PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024 TENTANG PENGGUNAAN FASILITAS APJII

DENGAN RAHMAT TUHAN YANG MAHA ESA

KETUA UMUM APJII

Menimbang:

a. bahwa dalam rangka melaksanakan keputusan Open Policy Meeting (OPM) tahun 2025, perlu disusun Standar Operasional Prosedur (SOP) Data Center APJII yang merujuk pada ISO 30414 dan standar internasional TIA/942 melalui pembahasan antara Badan Pengurus Pusat bersama Dewan Pengawas yang ditetapkan selambat-lambatnya 6 (enam) bulan sejak OPM;

b. bahwa Dewan Pengawas bersama dengan Badan Pengurus Pusat telah menyusun Standar Operasional Prosedur (SOP) Data Center dengan mendasarkan pada prinsip Kepastian Hukum, Tertib Pelaksanaan Tata Kelola, Transparansi, Proporsionalitas, Profesionalitas, Akuntabilitas, dan Interoperabilitas bagi Anggota;

c. bahwa Peraturan Asosiasi Penyelenggara Jasa Internet Indonesia Nomor 5 Tahun 2024 tentang Penggunaan Fasilitas APJII masih terdapat kekurangan dan belum menampung kebutuhan Anggota sehingga perlu diubah;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c perlu dibentuk Perubahan atas Peraturan Asosiasi Penyelenggara Jasa Internet Indonesia Nomor 5 Tahun 2024 tentang Penggunaan Fasilitas APJII;

Mengingat:

a. Pasal 14, Pasal 18, Pasal 41 angka 3, Pasal 42 Anggaran Dasar APJII dalam Akta Nomor 05 tanggal 26 September 2023;

b. Pasal 6 huruf c, Pasal 7 huruf e, Pasal 9 ayat (1), Pasal 66, Pasal 74, Pasal 76, Pasal 77 Anggaran Rumah Tangga APJII dalam Akta Nomor 06 tanggal 26 September 2023;

c. Peraturan Asosiasi Penyelenggara Jasa Internet Indonesia Nomor 5 Tahun 2024 tentang Penggunaan Fasilitas APJII;

Dengan Persetujuan Bersama
DEWAN PENGAWAS
dan
BADAN PENGURUS PUSAT

MEMUTUSKAN:

Menetapkan: **PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA TENTANG PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024 TENTANG PENGGUNAAN FASILITAS APJII.**

Pasal I

Ketentuan dalam Peraturan Asosiasi Penyelenggara Jasa Internet Indonesia Nomor 5 Tahun 2024 Tentang Penggunaan Fasilitas APJII diubah sebagai berikut:

I. Ketentuan Pasal 16 diubah sehingga berbunyi:

Pasal 16

(1) Tata cara pendaftaran dan penggunaan Fasilitas Data Center dituangkan dalam suatu Standar Operasional Prosedur (SOP) yang tercantum dalam Lampiran I sampai dengan Lampiran LIX yang merupakan bagian tidak terpisahkan dari Peraturan Asosiasi ini.
(2) Tata cara pendaftaran dan penggunaan Fasilitas Data Center sebagaimana dimaksud ayat (1) diumumkan secara terbuka kepada Anggota melalui media komunikasi resmi APJII.

II. Di antara BAB VI dan BAB VII disisipkan 1 (satu) bab, yakni BAB VIA sehingga berbunyi:

BAB VIA
KETENTUAN PERALIHAN

III. Di antara Pasal 29 dan Pasal 30 disisipkan 1 (satu) pasal, yakni Pasal 29A sehingga berbunyi sebagai berikut:

Pasal 29A

Standar Operasional Prosedur (SOP) yang telah ditetapkan pada Peraturan Asosiasi ini harus dilaksanakan dalam jangka waktu 6 (enam) bulan sejak tanggal ditetapkannya Peraturan Asosiasi ini.

Pasal II

Peraturan Asosiasi ini berlaku efektif sejak tanggal ditetapkan.

Disahkan di Jakarta
Pada tanggal 25 Maret 2026

Ketua Umum
Asosiasi Penyelenggara Jasa Internet Indonesia

Muhammad Arif

LAMPIRAN I
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

MASTER SOP LAYANAN DATA CENTER

1. Pendahuluan

1.1. Latar Belakang

Data Center merupakan fasilitas kritikal yang menyediakan infrastruktur teknologi informasi untuk mendukung operasional bisnis, penyimpanan data, layanan aplikasi, dan komunikasi. Keandalan Data Center sangat bergantung pada prosedur operasional yang standar dan terukur.

Untuk memastikan konsistensi, keamanan, serta ketersediaan layanan, maka diperlukan **Standard Operating Procedure (SOP) Layanan Data Center** yang menjadi acuan bagi seluruh personel operasional, mitra, dan pihak terkait. SOP ini juga bertujuan agar seluruh layanan yang diberikan dapat memenuhi **Service Level Agreement (SLA)** serta sesuai dengan standar internasional seperti **ISO/IEC 20000-1, ISO/IEC 27001, ISO 22301, TIA-942, dan ITIL v4 (IT Infrastructure Library v4)**.

1.2. Disclaimer: Walaupun adanya SOP Layanan Data Center ini, Pihak APJII tidak bertanggung jawab atas transaksi atau pertukaran data (informasi) yang dilakukan oleh Anggota/Tenant Data Center APJII terhadap perangkat miliknya.

1.3. Tujuan SOP

SOP ini dibuat untuk:

1.2.1. Memberikan panduan operasional yang jelas dan konsisten dalam pengelolaan layanan Data Center.
1.2.2. Memastikan kepatuhan terhadap standar internasional dan SLA dengan pelanggan.
1.2.3. Menjamin keamanan, ketersediaan, dan efisiensi infrastruktur Data Center.

1.4. Obyektif SOP

1.3.1. Meminimalisir risiko insiden akibat human error.
1.3.2. Menyediakan dasar acuan untuk pelatihan staf operasional.
1.3.3. Menjadi pedoman dalam audit internal maupun eksternal.

1.5. Dasar & Referensi Standar

1.5.1. ISO/IEC 20000-1: IT Service Management
1.5.2. ISO/IEC 27001: Information Security Management
1.5.3. ISO 22301: Business Continuity Management
1.5.4. ANSI/TIA-942-C: Data Center Infrastructure Standard
1.5.5. ITIL v4: IT Service Management Framework

1.6. Definisi & Istilah

1.6.1. SLA (Service Level Agreement): Perjanjian tingkat layanan antara penyedia layanan dan pelanggan.
1.6.2. Remote Hands: Layanan teknis jarak jauh yang dilakukan teknisi Data Center atas permintaan pelanggan.
1.6.3. Incident: Gangguan atau penurunan kualitas layanan yang tidak direncanakan.
1.6.4. Change: Perubahan terencana pada konfigurasi, sistem, atau layanan di Data Center.

2. Ruang Lingkup

SOP ini berlaku untuk:

2.1. Seluruh layanan Data Center termasuk interkoneksi, colocation, cloud, dan managed services.
2.2. Aktivitas operasional harian, pemeliharaan, keamanan, dan layanan pelanggan.
2.3. Seluruh staf operasional Data Center, vendor, serta pihak ketiga yang memiliki otorisasi.

3. Tanggung Jawab & Organisasi

3.1. Struktur Organisasi Operasional

3.1.1. Data Center Manager: Bertanggung jawab penuh atas kelancaran operasional.
3.1.2. Supervisor: Melaksanakan monitoring, pemeliharaan, laporan operasional dan memastikan kegiatan tim teknis dan noc berjalan sesuai prosedur.
3.1.3. Tim Teknis: Melaksanakan installasi, konfigurasi, troubleshooting (masalah teknis), pemeliharaan, dan laporan operasional.
3.1.4. Tim NOC: Melaksanakan monitoring, pendampingan, pemeliharaan, incident ticket dan laporan operasional.
3.1.5. Administrasi & Support: Membantu Tim Teknis dan Tim NOC dalam hal administrasi dan membuat laporan kegiatan operasional.

3.2 . Matriks RACI (contoh sederhana)

3.2.1. Responsible: Operation Engineer.
3.2.2. Accountable: Data Center Manager.
3.2.3. Consulted: Vendor / Subcontractor.
3.2.4. Informed: Customer / Management.

4. Kebijakan Layanan Data Center

4.1. Kebijakan Umum: Semua aktivitas operasional wajib terdokumentasi.
4.2. Keamanan Fisik: Hanya personel berwenang yang diperbolehkan masuk.
4.3. Keamanan Informasi: Akses ke sistem dikelola melalui prinsip “least privilege”.
4.4. Ketersediaan Layanan: Infrastruktur didesain minimal Rated-3 TIA-942-C (N+1 redundancy system).

5. Prosedur Operasional Utama

5.1. Prosedur Layanan

5.1.1. Permohonan, perubahan, dan pemutusan layanan interkoneksi.
5.1.2. Permohonan, perubahan, dan pemutusan layanan *colocation*.
5.1.3. Permohonan layanan *smarthand*.

5.2. Prosedur akses masuk dan keluar dari data center

5.2.1. Permohonan akses data center.
5.2.2. Prosedur pemutakhiran data akses.

5.3. Prosedur Interkoneksi

5.3.1. Prosedur penarikan interkoneksi baru.
5.3.2. Prosedur terminasi *fiber optic (FO)*.
5.3.3. Prosedur *dismantles* (pembongkaran) interkoneksi.
5.3.4. Prosedur perapihan kabel interkoneksi.
5.3.5. Prosedur penarikan kabel masuk dari luar data center.
5.3.6. SLG (*Service Level Guarantee*)/jaminan layanan interkoneksi.

5.4. Prosedur *Colocation*

5.4.1. Prosedur Masuk dan Keluar Barang.
5.4.1.1. Melakukan koordinasi dengan pihak Pengelola Gedung (*Building Management*).
5.4.2. Prosedur *Staging* barang masuk.
5.4.3. Prosedur instalasi perangkat.
5.4.4. Prosedur pembongkaran perangkat.
5.4.4.1. Tipe dan spesifikasi perangkat yang diizinkan untuk *colocation*.
a. Network Element (OTB).
b. Network Equipment (Router & Switch).
c. SLG (*Service Level Guanratee*)/jaminan *colocation*.

5.5. Prosedur *Smarthand*

5.5.1. Prosedur *request* untuk Smarthand.

5.6. Prosedur Penanganan Gangguan

5.6.1. Matriks eskalasi gangguan.

5.7. Prosedur perawatan berkala fasilitas data center

5.7.1. Manajemen fasilitas fisik & infrastruktur.

5.7.2. Sarana & Prasarana.
5.7.3. Prosedur perawatan dan pergantian perangkat atau komponen yang rusak.

5.8. Prosedur manajemen fasilitas (kebersihan & tata ruang) data center
5.8.1. Kebersihan Rack *Tenant*.
5.8.2. Kebersihan Rack MMR Bersama.
5.8.3. Kebersihan area Data Center secara umum.
5.8.4. Waste Management (Pengelolaan Limbah Kabel yang Berbahaya).

5.9. Prosedur keamanan fisik data center
5.9.1. Pengecekan *visitor* sebelum memasuki data center.
5.9.1.1. Pengecekan barang bawaan saat masuk & keluar dari data center.
5.9.1.2. Pemeriksaan Keamanan.
5.9.2. Pengecekan hak akses *visitor*.
5.9.2.1. *Visitor* wajib mengajukan hak akses (paling lambat H-1).
5.9.2.2. Memiliki konfirmasi hak akses.
5.9.2.3. Membawa identitas diri yang sesuai dengan hak akses.
5.9.2.4. Hak akses yang memiliki batas waktu kunjungan.
5.9.2.5. Kartu akses wajib dipakai selama berada di area data center.
5.9.2.6. *Visitor* wajib mengajukan hak akses (paling lambat H-1).
5.9.2.7. Dalam kondisi darurat, *Visitor* dapat mengajukan hak akses darurat dengan mengikuti prosedur untuk mendapatkan hak akses darurat.
5.9.2.8. Prosedur Mendapatkan hak akses darurat.
5.9.2.8.1. Membawa surat resmi dari Perusahaan.
5.9.2.8.2. Membawa identitas diri yang masih *valid* dan sesuai dengan identitas diri *Visitor*.
5.9.3. Patroli berkala di area Data Center
5.9.3.1. ***Visitor*** wajib menggunakan kartu hak akses.
5.9.3.2. ***Visitor*** wajib mematuhi batasan waktu berkunjung/kunjungannya.
5.9.3.3. **APJII &** ***Visitor*** wajib mematuhi Zona Akses (Color Card Coding).
- **Merah**: *Restricted Area*/*Critical Area*.
- **Biru**: Staff Operasional/*Engineer*.
- **Hijau**: *Tenant*/*Customer*/Klien.
- **Kuning**: *Vendor*/Kontraktor.
- **Putih/Abu-Abu**: *Visitor*/*Guest*/Tamu.
- **Hitam/Emas:** *Security/Emergency Access*.

5.9.3.4. Memastikan *Visitor* tidak melakukan tindakan-tindakan yang mencurigakan.

5.10. Prosedur Pelaporan & Monitoring
5.10.1. Jumlah anggota APJII yang menggunakan layanan data center.
5.10.1.1. Jumlah anggota APJII yang memiliki rack.
5.10.1.2. Jumlah anggota yang masuk dalam layanan *Colocation*.
5.10.2. Jumlah perangkat baru yang dipasang (*install*).
5.10.3. Jumlah perangkay yang dibongkar/dicopot (*dismantle*).
5.10.4. Jumlah interkoneksi yang baru.
5.10.5. Jumlah interkoneksi yang dibongkar/dicopot (*dismantle*).
5.10.6. Tipe perangkat yang dipasang / terpasang (ter-*Install*).

5.11. Prosedur Mitigasi Risiko Bencana atau Gangguan
5.11.1. Pengecekan berkala untuk mencegah terjadinya kerusakan yang disebabkan oleh:

5.11.1.1. Banjir.
5.11.1.2. Kebocoran Air.
5.11.1.3. Arus Pendek/Konsleting/Short Circuit.
5.11.2. Kerusuhan.
5.11.3. Pencegahan Kebakaran.
5.11.4. Prosedur Evakuasi.
5.11.5. Evaluasi Keberlangsungan Layanan.
5.11.6. Meminimalisir Terjadinya Risiko.
5.11.7. Prosedur Pemulihan Layanan.

5.12. Prosedur Publikasi Informasi & Sosialisasi (*Awareness*) di data center.
5.12.1. Berkoordinasi dengan bidang Humas.

5.13. Prosedur Pengalihan Kepemilikan Aset & Layanan
5.13.1. Prosedur pengalihan kepemilikan perangkat Anggota APJII yang tidak diambil setelah berakhirnya layanan.
5.13.2. Prosedur pengalihan kepemilikan aset antar Anggota APJII/Institusi lainnya (misal: akuisisi).
5.13.3. Prosedur pengalihan layanan.
5.13.4. Prosedur penerimaan hibah.

5.14. Prosedur Penyelesaian untuk Opened Ticket/Closed Ticket
5.14.1. Prioritas penyelesaian pekerjaan sesuai dengan antrian.
5.14.2. Prioritas penyelesaian pekerjaan sesuai dengan tingkat urgensi. (Penentuan Tingkat urgensi).

5.15. Desain dan Tata Ruang
5.15.1. Pemetaan posisi rack.
5.15.1.1. Standarisasi ukuran rack, ukuran ducting, ukuran cable tray, dan ketinggian raised floor.
5.15.1.2. Mengatur maksimal beban rack.
5.15.1.3. Mengatur maksimal jumlah device/perangkat pada rack.
5.15.2. Suhu dan Sirkulasi.
5.15.2.1. Menetapkan suhu ruangan yang ideal, suhu return-hot-air ke PAC, suhu supply udara dingin dari PAC ke setiap perangkat ICT.
5.15.2.2. Evaluasi cooling load secara berkala.
5.15.2.3. Perawatan perangkat PAC secara berkala.
5.15.2.4. Jalur Hot-Aisle & Jalur Cold-Aisle.
5.15.3. Desain dan Topologi Kelistrikan.
5.15.3.1. Pemetaan jalur kelistrikan.
5.15.3.2. Sistem Backup Kelistrikan.
5.15.3.3. Sistem Grounding Kelistrikan.
5.15.3.4. Mengatur pembagian beban kelistrikan untuk setiap rack.
5.15.3.5. Mengatur beban listrik untuk setiap rack.
5.15.4. Sistem Pencegahan Bahaya Kebakaran.
5.15.4.1. Sistem pendeteksi bahaya asap dan api.
5.15.4.2. Fire Alarm.
5.15.4.3. Fire Suppression System (FSS).
5.15.4.4. Prosedur Evakuasi.
5.15.4.5. Fire Drill Simulation.
5.15.5. Pemetaan jalur evakuasi.

5.16. Infrastruktur Jaringan

5.16.1. Struktur Kabel & Aksesoris Penunjang.
- Jalur *Cable Tray*.
- Jalur *Shaft*.
- Jalur *Raised-Floor*.

5.16.2. Desain/*Layout* Jaringan.

5.16.3. Jenis Kabel.
- *Backbone Cable*.
- *Cross-Connect Cable*.
- Tipe Kabel.
- Topologi Kabel.
- *Cable Management*.
  - *Fibre Patch Panel*.
  - *OTB*.
  - *Horizontal and Vertical Cable Management*.

5.16.4. *Testing & Maintenance*.

5.16.5. Prosedur penarikan, perapihan, dan *dismantle* kabel.

5.16.6. Prosedur penanganan kabel masuk dari luar data center

6. Prosedur Pendukung

- **Manajemen SLA:** Monitoring performa layanan sesuai kontrak.
- **Vendor Management:** Evaluasi kinerja vendor dilakukan minimal setiap 6 bulan.
- **Audit & Compliance:** Audit internal dilakukan setiap tahun.
- **Training:** Staf diwajibkan mengikuti pelatihan operasional & keamanan.

7. Health, Safety & Environment (HSE)

- Karyawan wajib menggunakan APD saat melakukan pekerjaan teknis.
- Bahan kimia/gas pemadam disimpan sesuai regulasi K3.
- Rute evakuasi dan assembly point wajib disosialisasikan kepada seluruh personel.

8. Evaluasi & Review SOP

- SOP ditinjau ulang minimal 1 kali dalam setahun.
- Update dilakukan jika ada perubahan standar internasional, regulasi, atau hasil audit.
- Continuous Improvement dijalankan melalui evaluasi insiden dan feedback pelanggan.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN II
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP LAYANAN DATA CENTER APJII

1. Pendahuluan

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) sebagai pengelola Data Center (DC) dan Internet Exchange Point (IIX) memiliki tanggung jawab untuk menyediakan layanan dengan tingkat ketersediaan tinggi, keamanan, dan keandalan bagi para anggota (tenant) dan penyelenggara layanan internet.

Layanan utama yang diberikan meliputi:

- **Layanan Interkoneksi (Interconnection Service)** – berupa konektivitas antar anggota/tenant untuk pertukaran trafik internet (peering).
- **Layanan Kolokasi (Colocation Service)** – berupa penyediaan ruang, daya, dan pendinginan bagi perangkat anggota.
- **Layanan Pendukung (Smart Hand Service)** – berupa dukungan teknis jarak jauh (remote support) oleh teknisi APJII.

SOP ini menjadi acuan operasional bagi seluruh personel teknis dan administrasi DC APJII agar proses pemberian layanan dilakukan secara terstandar, terdokumentasi, aman, dan konsisten.

2. Tujuan

Tujuan dari SOP ini adalah:

1. Menjamin setiap layanan Data Center (interkoneksi, kolokasi, dan smart hand) berjalan sesuai standar mutu dan keamanan.
2. Menetapkan prosedur layanan yang seragam, terdokumentasi, dan mudah diaudit.
3. Meminimalkan risiko operasional dan gangguan layanan melalui mekanisme kontrol dan eskalasi yang jelas.
4. Meningkatkan kepuasan anggota (tenant) melalui proses layanan yang cepat, transparan, dan terukur.
5. Mendukung kepatuhan terhadap standar **TIA-942-C Rated Facility**, **ISO/IEC 27001 (Information Security)**, **ISO/IEC 20000-1 (IT Service Management)**, dan **ISO 22301 (Business Continuity Management System)**.

3. Dasar dan Referensi Standar

SOP ini mengacu pada standar dan regulasi berikut:

No	Dokumen/Standar	Keterangan
1	**TIA-942-C**	Standar desain dan operasi Data Center terkait fasilitas fisik dan infrastruktur
2	**ISO/IEC 27001:2022**	Standar sistem manajemen keamanan informasi
3	**ISO/IEC 20000-1:2018**	Standar sistem manajemen layanan TI (Service Management System)
4	**ISO 22301:2019**	Standar sistem manajemen keberlangsungan bisnis
5	**ITIL v4 Framework**	Best practice manajemen layanan TI
6	**Peraturan APJII tentang Layanan IIX dan DC**	Pedoman internal APJII
7	**Peraturan Kominfo No. 9 Tahun 2023**	Tentang penyelenggaraan pusat data dan pertukaran internet
8	**SLA/SLO Layanan Data Center APJII**	Dokumen Service Level Agreement antar pihak

4. Definisi Istilah

Istilah	Definisi
Data Center (DC)	Fasilitas dengan sistem kelistrikan, pendinginan, keamanan, dan jaringan yang digunakan untuk menempatkan perangkat server dan jaringan milik Anggota/Tenant.
Interkoneksi / Peering	Layanan konektivitas antar tenant/anggota APJII dan pertukaran trafik internet melalui Internet Exchange Point (IIX).
Kolokasi (Colocation)	Penyediaan ruang rack, daya listrik, sistem pendingin, dan keamanan untuk perangkat milik Anggota/Tenant di fasilitas DC APJII.
Smart Hand Service	Layanan dukungan teknis jarak jauh oleh staf APJII atas permintaan tenant untuk melakukan tindakan fisik terhadap perangkat
Rack Unit (U)	Satuan tinggi peralatan di rack, setara dengan 1,75 inci.

Istilah	Definisi
SLA (Service Level Agreement)	Perjanjian tingkat layanan antara APJII dan tenant yang mendefinisikan ketersediaan, waktu respons, dan parameter mutu layanan.
Ticketing System	Sistem aplikasi untuk mencatat, melacak, dan mengelola permintaan layanan serta insiden dari tenant.
NOC (Network Operation Center)	Tim operasional yang memantau dan menangani operasional jaringan dan infrastruktur 24x7.

5. Ruang Lingkup

Ruang lingkup SOP ini mencakup seluruh kegiatan yang berhubungan dengan **layanan operasional Data Center APJII**, yang terbagi dalam tiga kategori utama:

A. Layanan Interkoneksi

1. **Proses Pendaftaran & Aktivasi**
    - Tenant/anggota mengajukan permohonan interkoneksi melalui portal DCIM APJII dan melengkapi persyaratan.
    - Tim NOC melakukan verifikasi kelayakan teknis (port availability, VLAN ID, kapasitas link).
    - Aktivasi dilakukan oleh teknisi jaringan dan diuji bersama tenant.
    - Tiket layanan dibuat dan ditutup setelah verifikasi berhasil.
2. **Konfigurasi & Monitoring**
    - Konfigurasi BGP peering, VLAN tagging, dan IP allocation sesuai kebijakan IIX.
    - Pemantauan trafik interkoneksi 24x7 melalui sistem monitoring.
3. **Maintenance & Troubleshooting**
    - Penanganan gangguan interkoneksi mengikuti SLA response time.
    - Eskalasi ke vendor atau backbone operator bila diperlukan.
4. **Dokumentasi**
    - Setiap perubahan jaringan didokumentasikan di Network Configuration Database (NCDB).

B. Layanan Kolokasi

1. **Proses Permintaan & Persiapan**
    - Tenant/anggota mengajukan permohonan interkoneksi melalui portal DCIM APJII dan melengkapi persyaratan.
    - Anggota/Tenant mengajukan permintaan space (per rack atau per U).
    - Tim NOC memverifikasi kapasitas daya, pendingin, dan ruang tersedia.
    - Persetujuan diberikan melalui surat kontrak dan SLA.
2. **Instalasi & Akses**
    - Jadwal instalasi dijadwalkan oleh Tim Teknis/NOC APJII dan dilaporkan ke PIC/Penanggung Jawab Operasional DC APJII.
    - Akses fisik tenant diverifikasi melalui sistem keamanan (access card).
    - Tim Teknis/NOC mendampingi selama proses pemasangan perangkat.

3. **Operasional & Pemeliharaan**
    - Pemantauan lingkungan (suhu, kelembapan, daya, keamanan) 24x7.
    - Preventive maintenance dilakukan sesuai jadwal harian, mingguan, bulanan, triwulan, dan tahunan.
4. **Reporting**
    - Anggota/Tenant menerima laporan log akses, Suhu dan Kelembaban Udara (Humadity) per bulan.

C. Layanan Pendukung (Smart Hand Service)

1. **Jenis Layanan**
    - Restart / Power Cycle perangkat Anggota/Tenant.
    - Pemeriksaan status perangkat (indikator LED, power, temperatur/suhu).
    - Plug / Unplug kabel / konektor.
2. **Prosedur Permintaan**
    - Anggota/Tenant mengajukan permintaan melalui portal DCIM
    - Tim teknis melaksanakan tindakan sesuai instruksi tertulis.
    - Hasil pekerjaan dan bukti foto dilaporkan ke tenant.
3. **Batasan Layanan**
    - Tidak termasuk konfigurasi software, perubahan sistem operasi, atau instalasi aplikasi.

7. Catatan dan Dokumentasi

Semua kegiatan operasional dicatat dalam:

- **Ticketing System (Incident)**
- **Portal DCIM (Request, Change)**
- **Logbook Akses Fisik Anggota/Tenant**
- **Daily Operation Checklist (Electrical, Cooling, Security)**
- **SLA Report & Monthly Performance Dashboard**
- **Incident Root Cause Analysis (RCA) Report**

8. Review dan Audit

- SOP ini ditinjau minimal **setiap 12 bulan sekali** atau ketika terjadi perubahan signifikan dalam kebijakan atau teknologi.
- Audit internal dilakukan sesuai ISO 27001 & 20000-1 untuk memastikan kepatuhan terhadap proses layanan.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.
MUHAMMAD ARIF

LAMPIRAN III
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP ALUR PROSES LAYANAN DATA CENTER APJII

1. Permohonan Layanan Baru

Tahapan Proses

1. **Pengajuan Permohonan**
   - Anggota APJII mengajukan **Permohonan Layanan** (Interkoneksi / Colocation / Smarthand) di Portal DCIM.
   - Dokumen pendukung: Surat resmi dari perusahaan anggota, spesifikasi kebutuhan teknis.
2. **Verifikasi Administrasi**
   - Tim Administrasi dan Support memverifikasi status keanggotaan APJII & kelengkapan dokumen serta status Outstanding dari Finance.
   - SLA: Maksimal **2 hari kerja**.
3. **Analisis Teknis & Ketersediaan Kapasitas**
   - Tim Operasional mengecek ketersediaan port, rack, power, dan sumber daya lainnya.
   - SLA: Maksimal **3 hari kerja**.
4. **Persetujuan Manajemen**
   - Jika lolos verifikasi, permohonan disetujui oleh **Manager**.
   - SLA: Maksimal **2 hari kerja**.
5. **Implementasi Layanan**
   - Tim Operasional melakukan instalasi/aktivasi layanan.
   - SLA: **5–10 hari kerja** tergantung kompleksitas.
6. **Uji Coba & Validasi**
   - Pengujian bersama anggota (User Acceptance Test).
   - Hasilnya dituangkan dalam **Berita Acara (BA) Aktivasi Layanan**.
7. **Serah Terima Layanan**
   - Layanan dinyatakan aktif & masuk dalam monitoring.
   - Pelanggan menerima **Service Activation Report**.

Eskalasi

- Jika ada kendala teknis → eskalasi ke **Supervisor**, Manager dan Kabid Terkait.
- Jika ada kendala administratif → eskalasi ke **Supervisor, Manager dan Kabid Terkait.**

2. Perubahan Layanan (Change Request)

Tahapan Proses

1. **Pengajuan Perubahan**
    - Anggota mengajukan **Change Request** ke Portal DCIM
    - Dokumen pendukung: surat resmi dan deskripsi perubahan.
2. **Evaluasi Administrasi & Kontrak**
    - Tim Administrasi dan Support mengecek kontrak dan konsekuensi biaya.
    - SLA: **2 hari kerja**.
3. **Analisis Teknis**
    - Tim Operasional mengevaluasi ketersediaan kapasitas (power, port, space).
    - Jika berisiko tinggi, perlu **Change Advisory Board (CAB)** approval.
    - SLA: **3 hari kerja**.
4. **Approval Manajemen**
    - Disetujui oleh **Data Center Manager**.
    - SLA: **2 hari kerja**.
5. **Implementasi Perubahan**
    - Tim Operasional melaksanakan perubahan sesuai jadwal (maintenance window jika diperlukan).
    - SLA: **3–7 hari kerja** tergantung kompleksitas.
6. **Uji Coba & Validasi**
    - Testing bersama anggota.
    - Dokumen: **Berita Acara Perubahan Layanan**.
7. **Update Dokumentasi & Billing**
    - Sistem monitoring & billing diperbarui sesuai perubahan layanan.

Eskalasi

- Perubahan kritikal → dilaporkan ke **Management APJII** sebelum implementasi.
- Kendala teknis → eskalasi ke **NOC/Operation Head**.

3. Pemutusan Layanan

Tahapan Proses

1. **Pengajuan Pemutusan**
    - Anggota mengajukan permohonan tertulis melalui Portal DCIM.
    - Minimal **30 hari kalender sebelum tanggal efektif** (mengacu ke kontrak).
2. **Verifikasi Administrasi**
    - Tim Administrasi dan Support memeriksa status kontrak, tagihan, dan kewajiban yang harus diselesaikan.
    - SLA: **2 hari kerja**.
3. **Koordinasi Teknis**
    - Tim Operasional menjadwalkan tanggal & jam pemutusan layanan.
    - Menyiapkan **escort untuk dismantle perangkat**.
    - SLA: **3 hari kerja**.
4. **Pelaksanaan Pemutusan**
    - Tim Operasional menonaktifkan layanan dan melakukan dismantle perangkat.
    - Dokumentasi foto/video jika diperlukan.

5. **Konfirmasi & Berita Acara**
    - Disusun **Berita Acara Pemutusan Layanan** ditandatangani kedua belah pihak.
6. **Update Sistem**
    - Layanan dinonaktifkan di monitoring system & billing system.
7. **Arsip & Dokumentasi**
    - Semua dokumen pemutusan diarsipkan minimal **3 tahun** untuk keperluan audit.

4. Ringkasan SLA Waktu >> **Revisi Timeline**

Jenis Proses	SLA Administrasi	SLA Teknis	SLA Implementasi
Permohonan Baru	1 hari kerja	3 hari kerja	3-5 hari kerja
Perubahan Layanan	2 hari kerja	3 hari kerja	3-5 hari kerja
Pemutusan Layanan	2 hari kerja	3 hari kerja	Sesuai jadwal

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN IV
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP AKSES MASUK DAN KELUAR DATA CENTER APJII

1. Pendahuluan

Data Center APJII merupakan fasilitas kritikal yang harus dijaga keamanan, integritas, dan ketersediaannya. Oleh karena itu, setiap individu yang masuk dan keluar area Data Center wajib mengikuti standar prosedur akses yang telah ditetapkan. SOP ini bertujuan memberikan panduan konsisten dalam pengelolaan akses fisik, baik untuk staf internal, tenant/anggota, maupun pihak ketiga.

2. Tujuan

- Menjamin keamanan fisik aset dan infrastruktur Data Center APJII.
- Mengatur mekanisme akses keluar-masuk sesuai otorisasi.
- Menyediakan standar prosedur permohonan dan pemuktahiran hak akses.
- Meminimalisir potensi risiko keamanan akibat akses tidak sah.

3. Dasar & Referensi Standar

- **ISO/IEC 27001** – Information Security Management.
- **ISO/IEC 27002** – Security Controls for Physical & Environmental Security.
- **TIA-942-C** – Data Center Telecommunications Infrastructure Standard (Facility & Security).
- **ISO 22301** – Business Continuity Management.
- Kebijakan Internal APJII tentang Pengelolaan Data Center.

4. Definisi Istilah

- **Hak Akses**: Hak untuk masuk ke area tertentu di dalam Data Center.
- **Tenant/Anggota**: Perusahaan anggota APJII yang menggunakan layanan Data Center.
- **Visitor/Tamu**: Individu yang melakukan kunjungan ke DC APJII.
- **Kartu Akses**: ID Card resmi yang diberikan APJII untuk otorisasi masuk.
- **Escort**: Pendampingan oleh staf APJII/Tenant Pemilik Rack.
- **Tenant Pemilik Rack**: Anggota APJII yang memiliki Rack di DC APJII.
- **Tenant Pengguna Rack Bersama**: Anggota APJII yang memiliki perangkat di Rack Bersama.

- **Vendor/Kontraktor**: Pihak Ketiga yang melakukan pekerjaan di area DC APJII atas permintaan dari APJII dan/atau dari Tenant.

5. Ruang Lingkup

SOP ini mencakup:

- Prosedur **akses masuk** dan **keluar** Data Center.
- Prosedur **permohonan akses** Data Center APJII.
- Prosedur **pemuktahiran data akses** secara berkala.
- Berlaku untuk staf APJII, anggota/tenant, kontraktor, vendor, dan tamu.

6. Prosedur Akses Masuk Data Center

6.1 Ketentuan Umum

- Hanya individu dengan otorisasi yang diizinkan masuk.
    - Klasifikasi Pengunjung:
        - Tenant pemilik Rack.
        - Tenant pengguna Rack Bersama.
        - Tamu/Visitor.
        - Vendor.
- Semua pengunjung wajib tercatat di **Visitor Management System (VMS)**.
- Tidak diperkenankan membawa makanan, minuman, mengambil gambar+kamera/video, atau perangkat elektronik tanpa izin.

6.2 Proses Akses Masuk

1. **Registrasi Awal**
    - Pengunjung melakukan permohonan akses ke DC APJII melalui Portal Pusat Layanan APJII
        - Informasikan tujuan permohonan akses.
        - Informasikan jumlah dan data identitas pengunjung.
        - Melampirkan surat resmi dengan berkepala surat, cap stempel perusahaan dan tanda tangan yang bertanggung jawab.
    - Melakukan penukaran/penyerahan identitas resmi (KTP/SIM/Passport) di pos keamanan/lobi Data Center.
    - Mengisi **Formulir Akses Data Center**.
2. **Verifikasi & Otorisasi**
    - Team Helpdesk/NOC memverifikasi permohonan dan memberikan respon tanggapan melalui email.
    - Petugas keamanan memverifikasi identitas dengan daftar akses yang disetujui.
    - Jika pengunjung adalah **tenant/anggota** → validasi terhadap daftar Authorized Personnel.
    - Jika pengunjung adalah **vendor/kontraktor** → harus ada surat tugas resmi dari tenant/anggota.
3. **Pemberian Kartu Akses/Tanda Visitor**
    - Kartu akses sementara atau visitor pass diberikan.
    - Akses hanya berlaku sesuai area yang diizinkan & durasi kunjungan.

4. **Pendampingan (Escort)**
    - Visitor/vendor wajib didampingi staf APJII atau tenant pemilik layanan.

7. Prosedur Akses Keluar Data Center

1. Pengunjung mengembalikan **kartu akses/visitor pass** kepada petugas keamanan.
2. Petugas keamanan memeriksa barang bawaan (cross-check dengan saat masuk).
3. Exit dicatat dalam **Visitor Management System**.
4. Jika ada insiden/kecurigaan → dilaporkan ke Data Center Manager.

8. Prosedur Permohonan Akses Data Center

8.1 Pengajuan

- Tenant/anggota mengajukan **Email Permohonan Akses** berisi:
    - Nama, jabatan, dan perusahaan.
    - Nomor identitas resmi (KTP/Passport).
    - Nomor kontak/HP.
    - Alasan dan area akses.
    - Periode/jangka waktu akses.
- Surat resmi dari perusahaan tenant sebagai lampiran wajib.

8.2 Persetujuan

- Permohonan diperiksa oleh **Helpdesk APJII**.
- Disetujui oleh **Data Center Manager**.
- SLA: maksimal **1 hari kerja**.

8.3 Penerbitan Akses

- Jika disetujui → penerbitan **ID Card/Kartu Akses Permanen**.
- Jika ditolak → tenant mendapat notifikasi resmi dalam format email dan berikut alasannya.

9. Prosedur Pemuktahiran Data Akses

9.1 Pemutakhiran Berkala

- Data akses diverifikasi **setiap 6 bulan sekali** oleh tim Helpdesk/NOC.
- Tenant wajib mengirimkan daftar terbaru Authorized Personnel.
- ID Card yang tidak aktif > 90 hari otomatis diblokir.

9.2 Perubahan Personel

- Tenant wajib melaporkan **penambahan, penggantian, atau penghapusan** PIC (*Person in Charge*) akses dalam waktu **1x24 jam** setelah terjadi perubahan.
- Permohonan diajukan melalui **Formulir Update Data Akses** + surat resmi tenant.

9.3 Penonaktifan

- Akses dinonaktifkan jika:
  - Masa berlaku kontrak tenant berakhir.
  - Ada permintaan resmi dari tenant.
  - Ditemukan penyalahgunaan akses.

10. Catatan & Dokumentasi

- Semua permohonan akses, log masuk/keluar, dan update data disimpan minimal **2 tahun** untuk audit.
- Sistem log diintegrasikan dengan **BMS/Security System** Data Center.

11. Kartu Akses & Color Coding

Untuk memudahkan identifikasi visual, setiap kategori pengguna Data Center APJII diberikan **kartu akses dengan warna berbeda** sebagai berikut:

Kategori Pengguna	Warna Kartu Akses	Keterangan
Staf APJII (Internal)	**Merah**	Kartu akses permanen untuk pegawai tetap APJII. Memberikan akses penuh sesuai otorisasi jabatan.
Tenant Pemilik Rack	**Hijau**	Diberikan kepada Authorized Personnel dari perusahaan tenant pemilik rack. Akses terbatas hanya pada rak/ruang yang dimiliki tenant.
Tenant Pengguna Rack Bersama	**Biru**	Diberikan kepada Authorized Personnel dari perusahaan pengguna rack bersama. Akses terbatas hanya untuk keluar/masuk DC APJII. Setiap pekerjaan teknis wajib didampingi (escort) staff APJII.
Vendor/Kontraktor	**Kuning**	Diberikan kepada pihak ketiga yang melakukan pekerjaan teknis/maintenance di DC APJII. Wajib didampingi (escort) kecuali ada otorisasi khusus.
Visitor/Tamu	**Abu-Abu**	Akses bersifat sementara dan wajib didampingi staf APJII serta tidak melakukan kegiatan teknis.

12. Aturan Umum Penggunaan Kartu Akses

1. ***Non-Transferable*** – Kartu akses hanya boleh digunakan oleh pemilik sah.
2. ***Always Visible*** – Kartu akses wajib dipakai dan terlihat jelas selama berada di area Data Center.
3. ***Return Policy*** – Kartu akses visitor/vendor wajib dikembalikan setelah keluar.

4. ***Lost Card*** – Kehilangan kartu harus segera dilaporkan, dan akses dinonaktifkan segera setelah laporan diterima.
5. ***Audit Periodik*** – Log penggunaan kartu diaudit minimal setiap bulan oleh pihak Team Security & Team Data Center Operation.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN V
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP INTERKONEKSI DATA CENTER APJII

1. Pendahuluan

Interkoneksi merupakan salah satu layanan utama Data Center APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) yang memungkinkan pertukaran data antar penyelenggara jaringan, penyedia konten, dan pelanggan co-location melalui media transmisi, yaitu kabel fiber optik (FO).

Untuk menjaga keandalan, keamanan, dan keteraturan infrastruktur fisik di lingkungan Data Center APJII, diperlukan prosedur baku (Standard Operating Procedure/SOP) yang mengatur pelaksanaan seluruh aktivitas interkoneksi mulai dari penarikan kabel baru, terminasi, perapihan, hingga pembongkaran kabel/tarik mundur.

2. Latar Belakang

Kegiatan interkoneksi di Data Center APJII melibatkan berbagai pihak seperti Anggota/Tenant, penyedia backbone, serta tim operasional data center.
Tanpa adanya tata kelola yang baik, kegiatan fisik seperti penarikan atau terminasi kabel berpotensi menyebabkan:

- Gangguan layanan (downtime) pada sistem lain,
- Ketidakteraturan jalur kabel (cable congestion),
- Risiko keamanan fisik dan kebakaran,
- Pelanggaran standar pengelolaan infrastruktur data center.
- Tidak tercapainya suhu ideal di lingkungan Data Center

SOP ini disusun agar semua kegiatan interkoneksi dilakukan secara **terencana, terdokumentasi, aman, dan sesuai standar internasional.**

3. Tujuan SOP

1. Menetapkan prosedur standar untuk setiap kegiatan interkoneksi di Data Center APJII.
2. Menjamin integritas layanan interkoneksi dan menghindari gangguan terhadap sistem yang telah beroperasi.
3. Menjaga keteraturan tata kelola kabel dan infrastruktur fisik data center.
4. Menjamin setiap pihak yang melakukan pekerjaan di area data center mengikuti ketentuan keselamatan dan keamanan kerja.

4. Obyektif SOP

- Menyediakan panduan terperinci bagi teknisi, pelanggan, dan pihak ketiga terkait pelaksanaan pekerjaan interkoneksi.
- Memastikan seluruh proses interkoneksi terdokumentasi melalui *Work Permit* dan laporan hasil pekerjaan.
- Menetapkan jaminan layanan (*Service Level Guarantee / SLG*) terhadap performa konektivitas antar-rak maupun antar-tenant.
- Mendukung keberlangsungan operasional data center dengan menghindari potensi downtime akibat aktivitas fisik kabel.

5. Dasar & Referensi Standar

1. **TIA-942-C** – Telecommunications Infrastructure Standard for Data Centers.
2. **ISO/IEC 11801** – Generic Cabling for Customer Premises.
3. **ISO/IEC 27001:2022** – Information Security Management System (ISMS).
4. **TIA-606-C** – Administration Standard for Telecommunications Infrastructure.
5. **ISO 9001:2015** – Quality Management System.
6. **APJII Data Center Policy Manual** dan **APJII Colocation Service Agreement**.
7. **Panduan Keselamatan & K3 Data Center APJII.**

6. Definisi & Istilah

Istilah	**Definisi**
Interkoneksi	Koneksi fisik antar-perangkat jaringan melalui media kabel di dalam data center APJII.
FO (Fiber Optic)	Media transmisi berbasis serat optik yang digunakan untuk koneksi antar-rak atau antar-data center.
Transceiver	Modul SFP dan QSFP
Network Element	Perangkat berupa OTB, Patch Panel
Network Equipment	Perangkat berupa Router dan Switch
Rack	Lemari server tempat perangkat tenant atau penyedia jaringan ditempatkan.
Work Permit (Izin Kerja)	Dokumen resmi yang wajib diperoleh sebelum melakukan pekerjaan fisik di area data center.
Labeling	Pemberian kode identitas unik pada kabel, panel, dan perangkat untuk memudahkan identifikasi.
SLG (Service Level Guarantee)	Jaminan performa dan keandalan layanan interkoneksi yang diberikan kepada pelanggan.

7. Ruang Lingkup

SOP ini berlaku untuk seluruh kegiatan **interkoneksi** yang dilakukan di lingkungan Data Center APJII oleh Tim Teknis/NOC APJI.

Ruang lingkup meliputi:

a. Prosedur Penarikan Kabel Interkoneksi Baru

- Anggota/Tenant wajib melakukan *request* interkoneksi melalui Portal Pusat Layanan APJII.
- Selanjutnya, pihak Destination (tujuan) interkoneksi harus memberikan persetujuan atas permohonan interkoneksi.
- Helpdesk/NOC APJII akan melakukan verifikasi status *outstanding* dari pihak Finance serta informasi status keanggotaannya **maksimal dalam 1 hari kerja**.
- Finance akan menerbitkan *proforma invoice* kepada *Initiator* Interkoneksi.
- Setelah Anggota/Tenant telah menyelesaikan administrasi pembayaran, maka Anggota/Tenant wajib melakukan Goods-In modul transceiver sesuai dengan kebutuhan interkoneksi.
- NOC APJII akan mengukur panjang kabel kebutuhan interkoneksi **maksimal dalam 1x24 jam**.
- NOC APJII melakukan penarikan kabel Cross Connect sesuai kebutuhan dan kabel disediakan oleh pihak APJII **maksimal dalam 3x24 jam**.
- Penarikan Kabel yang dilakukan harus melalui Tray (Horizontal dan Vertikal) dan masuk ke dalam Rak Anggota/Tenant.
- Setelah penarikan kabel Cross Connect selesai dilakukan, NOC APJII akan memberikan label diujung kabel disisi Source dan diujung kabel disisi Destination.
- NOC APJII memastikan kabel interkoneksinya terpasang dalam kondisi baik dan bisa digunakan, dilakukan *test laser & OPM*.
- NOC APJII akan melakukan pemasangan konektor SFP ke perangkat anggota segera setelah kabel interkoneksi selesai ditarik dan dinyatakan layak untuk digunakan.
- Seluruh aktivitas penarikan kabel dari Rak ke Rak di Data Center APJII ataupun aktivitas penarikan kabel dari perangkat ke perangkat di dalam Rak MMR bersama di Data Center APJII, hanya boleh dilakukan oleh NOC/Tim Teknis APJII.
- Seluruh aktivitas Interkoneksi dibuat Berita Acara disertai dokumentasi teknis yang dibutuhkan.

b. Prosedur Penggantian Kabel Interkoneksi Yang Bersifat Mendesak (Darurat/Urgent)

- Adapun yang termasuk dalam kategori Penggantian Kabel Yang Bersifat Mendesak, antara lain:
    1. Gangguan kabel interkoneksi atau perangkat di Data Center APJII;
    2. Penggantian maupun kerusakan kabel interkoneksi existing;
    3. atau gangguan lain di Data Center APJII yang memerlukan tindakan pemulihan segera;
- Tenant wajib melakukan request penggantian kabel melalui Portal Pusat Layanan APJII, kemudian Tenant mengajukan permohonan Interkoneksi Darurat melalui email: tiket@apjii.or.id, yang ditujukan kepada Ketua Bidang urusan terkait, dengan disertakan detail penjelasan atas urgensi yang dimaksud. Dengan

demikian, penarikan kabel dapat diprioritaskan sesuai kebutuhan pemulihan layanan.
- Penggantian kabel cross connect/interkoneksi termasuk dalam kategori yang harus didahulukan (darurat), maka pihak NOC/Staff APJII harus menyelesaikan penggantian kabel secepatnya, dan dimungkinkan untuk penggantian sementara.
- Setelah kabel interkoneksi pengganti selesai ditarik & dipergunakan, maka kabel interkoneksi yang lama akan dilakukan *dismantle* segera **dalam kurun waktu 1x24 jam**.
- Seluruh aktivitas penggantian kabel interkoneksi dibuat Berita Acara disertai dokumentasi teknis yang dibutuhkan.

2. **Pelaksanaan Penarikan Kabel Interkonesi:**
   - Pekerjaan dilakukan hanya oleh NOC/Teknisi APJII yang memiliki izin kerja aktif.
   - Kabel ditarik menggunakan jalur *overhead cable tray* atau *underfloor pathway* sesuai desain standar TIA-942.
   - Selain NOC/Teknisi APJII, maka Anggota/Tenant dilarang melakukan aktivitas penarikan kabel interkoneksi.

3. **Dokumentasi:**
   - Setiap kabel interkoneksi baru wajib diberi **label pada kedua ujungnya**.
     - Standard Labeling Data Center APJII:
       1. 4 huruf/angka untuk Tenant ID,
       2. 2 huruf/angka untuk Rack ID,
       3. 2 huruf/angka untuk Row (Rack Unit) ID,
       4. 2 huruf/angka untuk Port ID
     - Contoh: Tenant ID 0001 sebagai Source, Tenant ID 0002 sebagai Destination. Perangkat Tenant ID 0001 berada di Rak P2 Row 14 port 6. Perangkat Tenant ID 0002 berada di Rak C1 Row 10 port 12. Maka label: **0001P21406-0002C11012**.
   - Hasil pekerjaan diserahkan dalam bentuk **berita acara dokumentasi teknis**.

c. Prosedur Dismantle (Pembongkaran) Kabel Interkoneksi

- Tenant mengajukan permohonan *dismantle* interkoneksi melalui Portal Pusat Layanan APJII.
- Setelah NOC APJII menerima permohonan dismante tersebut, selanjutnya NOC APJII akan melakukan pemotongan kabel dikedua ujung sisi konektor.
- NOC APJII akan segera melakukan penarikan mundur kabel setelah pemotongan dilakukan.
- Seluruh aktivitas *dismantle* kabel interkoneksi dibuat Berita Acara disertai dokumentasi teknis yang dibutuhkan.
- Update database di Portal Pusat Layanan APJII.

d. Prosedur Perapihan Kabel Interkoneksi

1. **Tujuan:**
   - Menjaga kerapihan jalur kabel agar tidak mengganggu sirkulasi udara dan keamanan fisik.
2. **Langkah-langkah:**
   - Gunakan Tray khusus jalur Interkoneksi yang tersedia secara Horizontal dan Vertical dan langsung masuk ke dalam Rak. Tidak ada kabel di luar jalur Tray.

- Memastikan tidak ada sisa kabel di luar Rak atau Tray.
- Melakukan Capacity Planning untuk kapasitas Tray yang tersedia (maksimal 80% dari kapasitas maksimum Tray).
- Gunakan *Velcro strap* (bukan cable tie permanen).
- Pisahkan jalur FO, UTP, dan power cable sesuai tray-nya.
- Pastikan semua kabel memiliki label di kedua ujungnya.
- Lakukan audit visual kabel setiap **3 bulan** untuk memastikan keteraturan.

3. **Dokumentasi:**
   - Hasil audit dilaporkan ke Supervisor Data Center dengan foto sebelum/sesudah perapihan.

f. SLG (Service Level Guarantee) / Jaminan Layanan Interkoneksi

Parameter	**Nilai Jaminan**	**Keterangan**
Availability	99.982%	Mengacu pada SLA Data Center Rated-3.
Downtime Maksimum/Bulan	7.2 menit/bulan	Berdasarkan perhitungan waktu aktif 99.982%.
Response Time	≤ 15 menit	Waktu maksimal respons teknis sejak laporan gangguan.
Resolution Time	≤ 2 jam	Waktu maksimal penyelesaian gangguan interkoneksi minor.
Monitoring	24x7 by NOC APJII	Pemantauan menggunakan sistem DCIM/NMS.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

1. WORK PERMIT TEMPLATE (IZIN KERJA DATA CENTER APJII)

Dokumen No: _____
Tanggal Pengajuan: ____ / ____ / _____
Nomor Tiket/WO: _____
Departemen / Perusahaan Pemohon: _____
Nama Teknisi: _____
No. ID / KTP / Kartu Akses: _____
Nomor Kontak (HP): _____

A. Deskripsi Pekerjaan

Uraian	**Keterangan**
Jenis Pekerjaan	☐ Penarikan Kabel Baru ☐ Terminasi FO ☐ Dismantle ☐ Perapihan Kabel ☐ Lainnya: _____
Lokasi Pekerjaan	☐ Meet Me Room ☐ Rack Area ☐ Riser ☐ Manhole / Duct ☐ Lainnya: _____
Tujuan Pekerjaan	_____
Estimasi Waktu	Mulai: ____ / ____ / ____ □ Jam: _____ s.d. Selesai: ____ / ____ / ____ □ Jam: _____
Jumlah Personel	_____ Orang

B. Peralatan yang Digunakan

(centang yang sesuai)

- Ladder
- Fiber Fusion Splicer
- OTDR / Power Meter
- Label Printer
- Crimp Tool
- Laptop
- Lainnya: _____

C. Dampak Potensial

Jenis Dampak	**Deskripsi Mitigasi**
Risiko Gangguan Layanan	
Risiko Keselamatan	
Risiko Kebersihan / Kontaminasi	

D. Persetujuan & Otorisasi

Jabatan	**Nama**	**Tanda Tangan**	**Tanggal**
Pemohon			
Supervisor DC APJII			
Security / Access Control			
DC Operation Approval			

Catatan: Semua aktivitas hanya boleh dilakukan setelah Work Permit disetujui dan disahkan oleh pihak **DC Operation APJII**.

2. RFI TEMPLATE (REQUEST FOR INTERCONNECTION)

Nomor RFI: _____
Tanggal Pengajuan: ____ / ____ / _____
Nama Perusahaan: _____
Alamat Email Teknis: _____
Nomor Telepon: _____

A. Informasi Teknis Permintaan

Keterangan	**Detail**
Jenis Interkoneksi	☐ Fiber Optic ☐ UTP Cat6A ☐ Power ☐ Lainnya
Jumlah Core / Pair	_____
Tujuan Interkoneksi	☐ Rack ke Rack ☐ Rack ke MMR ☐ Rack ke Panel ODF ☐ ODF ke ODF
Lokasi Awal (A-End)	_____
Lokasi Tujuan (B-End)	_____
Panjang Kabel Perkiraan	_____ meter
Label yang Diminta	_____

B. Rencana Pelaksanaan

Uraian	**Keterangan**
Estimasi Jadwal Pelaksanaan	Tanggal: ____ / ____ / ____ □ Jam: _____
Kontraktor / Vendor Pelaksana	_____
Penanggung Jawab Teknis	_____

Uraian	Keterangan
Email PIC	_____

C. Persetujuan & Otorisasi

Jabatan	Nama Tanda Tangan Tanggal
Pemohon (Tenant/Member)	
Supervisor DC APJII	
Network Operation Center (NOC) APJII	

Catatan: RFI ini menjadi dasar penerbitan **Work Permit** dan tidak dapat diproses tanpa diagram interkoneksi dan rencana jalur kabel yang disetujui.

3. AS-BUILT REPORT TEMPLATE (LAPORAN PEKERJAAN SELESAI)

Nomor Referensi Work Permit: _____
Tanggal Pelaksanaan: ____ / ____ / _____
Perusahaan Pelaksana: _____
PIC Lapangan: _____
Nomor HP PIC: _____

A. Ruang Lingkup Pekerjaan

Jenis Aktivitas	**Deskripsi**
Penarikan Kabel	
Terminasi	
Labeling	
Dismantle / Re-route	
Dokumentasi Foto ☐ Tersedia ☐ Tidak Tersedia	

B. Detail Teknis Pekerjaan

Item	**Lokasi A**	**Lokasi B**	**Jenis Kabel**	**Panjang (m)**	**No. Label**	**Test Result (dB)**
1						
2						

C. Lampiran

- Foto Instalasi Sebelum
- Foto Instalasi Sesudah
- Diagram Jalur Aktual (Drawing)
- OTDR / Power Meter Test Report
- Checklist Kebersihan Area

D. Catatan Temuan

E. Pengesahan

Jabatan	Nama Tanda Tangan	Tanggal
Pelaksana Lapangan		
Supervisor DC APJII		
NOC Verification		

Catatan: Form ini wajib diserahkan maksimal **1x24 jam setelah pekerjaan selesai**, untuk validasi dan pembaruan **As-Built Drawing Master File**.

Lampiran Pendukung Tambahan (opsional)

1. **Fiber Route Drawing Template (.DWG/.PDF)** – menunjukkan jalur aktual penarikan dari MMR → ODF → Rack.
2. **Cable Labeling Standard Sheet** – format kode label kabel interkoneksi APJII (misal: DCJKT-MMR01-RK12A-FOC-02).
3. **Cable Routing Approval Stamp Area** – untuk divalidasi oleh tim DC Operation sebelum eksekusi lapangan.

LAMPIRAN VI
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP CO-LOCATION DATA CENTER APJII

1. Pendahuluan

Co-location merupakan layanan Data Center APJII yang memberikan ruang (*space*), sistem kelistrikan, sistem pendinginan, sistem telekomunikasi, serta keamanan fisik bagi perangkat anggota/tenant. Untuk menjamin kelancaran, keamanan, dan keseragaman dalam operasional, diperlukan SOP yang mengatur alur permohonan, masuk/keluar barang, staging, instalasi, hingga pembongkaran perangkat tenant di fasilitas Data Center APJII.

2. Tujuan

- Menyediakan prosedur standar dalam pengelolaan layanan co-location.
- Menjamin keamanan dan ketertiban dalam proses masuk/keluar perangkat tenant.
- Memastikan koordinasi yang jelas dengan pihak Pengelola Gedung dan internal APJII.
- Mengurangi risiko kerusakan, kehilangan, atau insiden pada perangkat dan fasilitas Data Center.

3. Dasar & Referensi Standar

- **ISO/IEC 27001**: Information Security Management – kontrol akses fisik.
- **ISO/IEC 27002**: Annex A.11 (Physical and Environmental Security).
- **TIA-942-C**: Data Center Telecommunications Infrastructure Standard.
- **ISO 22301**: Business Continuity Management – keberlangsungan layanan.
- Kebijakan Keamanan Fisik Data Center APJII.

4. Definisi Istilah

- **Co-location**: Layanan penyewaan ruang di Data Center APJII untuk menempatkan perangkat tenant.
- **Staging Area**: Area khusus yang disediakan untuk mempersiapkan perangkat agar ***Ready to Use*** sebelum instalasi di rak tenant.
- **Authorized Personnel**: Individu yang terdaftar dan disetujui untuk melakukan pekerjaan di area Data Center.
- **Work Permit**: Surat izin kerja yang dikeluarkan APJII untuk aktivitas instalasi/pembongkaran perangkat.

- **Building Management**: Pihak pengelola gedung tempat Data Center APJII berlokasi.
- **Suspended**: Pemutusan sementara layanan yang dikarenakan adanya tunggakan tagihan layanan yang tidak terbayarkan atau belum melengkapi dokumen administrasi.
- **Terminated:** Pemutusan layanan yang dikarenakan penyalahgunaan layanan.
- **Akses Logistik:** Area Akses Bongkar Muat yang disediakan oleh *Building Management*.
- **Dismantle:** Pembongkaran/Pencopotan perangkat yang terpasang di DC APJII.
- **Ketua Bidang Terkait:** Ketua bidang yang melaksanakan urusan bidang **IIX & Data Center**.

5. Ruang Lingkup

SOP ini mencakup seluruh aktivitas co-location tenant di Data Center APJII, yaitu:

- Proses permohonan layanan co-location.
- Prosedur masuk dan keluar barang.
- Koordinasi dengan Pengelola Gedung (*Building Management*).
- Prosedur staging barang masuk.
- Prosedur instalasi perangkat.
- Prosedur *dismantle* perangkat.
    - Dismantle Permintaan Pengguna.
    - Dismantle karena terhentinya layanan.
        - Suspended.
        - Terminated.

6. Prosedur Co-location

6.1 Permohonan Layanan Co-location

1. Anggota APJII mengajukan **Permohonan Layanan Co-location** melalui Portal Pusat Layanan APJII.
2. Anggota APJII wajib mendowload dan menandatangani SPK (Surat Perjanjian Kerjasama), rangkap 2 dan Tanda Tagan basah (disertai Stempel Perusahaan). Kemudian scan dan Upload dokumen tersebut ke Portal Pusat Layanan APJII.
3. Anggota APJII wajib mengirimkan Dokumen asli tersebut (pada poin no,2) ke Kantor Pusat APJII. Selama Dokumen Asli tersebut belum diterima pihak APJII, maka proses permohonan tidak dapat dilanjutkan.
4. Helpdesk/NOC APJII akan melakukan verifikasi kapasitas (ruangan, ketersediaan *size* rack, & kelistrikan) dan informasi status *outstanding* dari pihak Finance serta informasi status keanggotaannya **maksimal dalam 1 hari kerja**.
5. Selanjutnya, Finance APJII akan mengirimkan Proforma Invoice ke Anggota APJII **maksimal dalam 1 hari kerja setelah dinyatakan tidak ada *outstanding***.
6. Setelah Anggota APJII melakukan pembayaran, maka Anggota APJII dapat melakukan *request Goods-In* melalui Portal Pusat Layanan APJII.
7. Setelah *request Goods-In* dilaksanakan, maka merujuk pada poin SOP *Goods-In (poin 6.2)*

6.2 Prosedur *Goods-In/Goods-Out*

6.2.1. Prosedur *Goods-In*

1. Anggota APJII mengajukan permohonan *Goods-In*, minimal H-3 melalui Portal Pusat Layanan APJII dengan informasi berikut:
    - Berisi spesifikasi perangkat,
    - Jumlah perangkat yang akan dipasang.
    - Serial Number/MAC Address.
2. NOC APJII menindaklanjuti permohonan *Goods-In* dengan berkoordinasi ke **Building Management** terkait jadwal *Goods-In* dan akses logistik .
3. Pihak **Building Management** akan menerbitkan ijin untuk aktivitas *Goods-In*.
4. Saat perangkat telah tiba di Data Center APJII, maka barang akan diperiksa oleh **Security Data Center** & **Building Management**.
5. Jika perangkat tersebut sudah sesuai dengan informasi dokumen yang telah di-*submit* sebelumnya, maka perangkat bisa dilanjutkan ke proses *Staging*.
6. Semua barang yang masuk akan dicatat dalam **Log-Book *Goods-In***.

6.2.2. Prosedur *Goods-Out*

7. Anggota APJII mengajukan permohonan *Goods-Out*, minimal H-3 melalui Portal Pusa Layanan APJII dengan informasi berikut:
    - Berisi Detail Spesifikasi perangkat.
    - Lokasi Rack.
    - Serial Number/MAC Address.
8. NOC APJII berkoordinasi dengan pihak Finance APJII terkait status *outstanding* tagihan, jika tidak terdapat *outstanding* terhadap layanan tersebut*,* maka NOC APJII melakukan proses *dismantle* perangkat.
9. Jika perangkat yang telah dilakukan *dismantle* sudah sesuai dengan informasi dokumen yang telah di-*submit* sebelumnya, maka NOC APJII mengijinkan perangkat tersebut untuk dibawa keluar.
10. NOC APJII berkoordinasi dengan **Building Management** terkait jadwal *Goods-Out* dan akses logistik.
11. Pihak **Building Management** akan menerbitkan ijin untuk aktivitas *Goods-Out*.
12. Saat perangkat akan keluar dari Data Center APJII, maka barang akan diperiksa oleh **Security Data Center** & **Building Management**.
13. Semua barang yang keluar akan dicatat dalam **Log-Book *Goods-Out***.

6.2.3. Prosedur *Goods-In/Goods-Out Darurat (Replacement* Perangkat).

14. Anggota APJII mengajukan permohonan *Goods-In Darurat*, melalui Portal Pusat Layanan APJII dengan informasi berikut:
    - Berisi spesifikasi perangkat.
    - Jumlah perangkat yang akan dipasang.
    - Serial Number/MAC Address.
15. Anggota APJII mengirimkan email permohonan *Goods-In Darurat* untuk keperluan *Replacement* Perangkat yang ditujukan kepada Ketua Bidang terkait melalui email: tiket@apjii.or.id yang berisi detail penjelasan kronologi dan alasan dilakukannya *replacement* perangkat dengan memperhatikan ketentuan berikut:

- Menyertakan informasi lokasi dan spesifikasi Perangkat Lama yang akan dilakukan *dismantle*.
- Size “U” dari Perangkat yang baru tidak melebihi dari Size “U” dari Perangkat yang lama.

16. *NOC* APJII mengajukan approval kepada Ketua Bidang terkait.
17. Jika Permohonan tersebut sudah disetujui oleh Ketua Bidang terkait, maka NOC APJII akan melakukan tindak lanjut dengan berkoordinasi ke **Building Management** terkait jadwal *Goods-In*, akses logistik, dan status darurat.
18. NOC APJII selanjutnya akan melakukan proses *Staging* dan dilanjutkan dengan *Dismantle* Perangkat lama serta memasang Perangkat yang baru ditempat yang sama.
19. Perangkat lama yang sudah dilakukan dismantle akan dilakukan proses *Goods-Out* sesuai dengan prosedur *Goods-Out* pada poin 6.2.2.

6.3 Koordinasi dengan *Building Management*

- Setiap aktivitas *Goods-In/Goods-Out* perangkat wajib melalui persetujuan dari Building Management.
- Persetujuan dari Building Management hanya dapat dilakukan pada hari dan jam kerja.
- NOC APJII wajib menyerahkan:
  - *Goods-In/Goods-Out Document* ke *Building Management*.
- Building Management akan menyiapkan:
  - Jalur logistik (service lift/loading dock).
  - Security check point tambahan.

6.4 Prosedur Staging *Goods-In*

1. Setelah barang diterima di area Data Center, perangkat ditempatkan di **Staging Area**.
2. Tim APJII melakukan pengecekan fisik (kondisi, nomor seri, jumlah).
3. Tenant menyiapkan perangkat (konfigurasi awal, labeling, pengujian dasar).
4. Lama penempatan di staging area selambat-lambatnya **3x24 jam** sebelum dipindahkan ke rak tenant dengan metode prioritas FIFO (*First-In-First-Out*).
5. Semua bahan material seperti Box Kemasan, Plastik, Buble Wrap, Packaging, Kardus tidak diperkenankan untuk dibawa masuk ke dalam area Data Center APJII.
6. Pemasangan semua aksesoris perangkat, wajib dilakukan pemasangannya di area *Staging*.

6.5 Prosedur Instalasi Perangkat

1. NOC APJII akan segera melakukan pemasangan dari perangkat tersebut, selambat-lambatnya **1x24 jam** setelah proses *Staging* selesai.
2. Proses pemasangan perangkat hanya boleh dilakukan oleh NOC APJII.
3. Setelah perangkat terpasang, NOC APJII akan menambahkan informasi perangkat baru tersebut ke dalam Portal Pusat Layanan APJII dan NOC APJII akan menerbitkan **Berita Acara Instalasi**. Anggota APJII wajib mengunduh dokumen **Berita Acara Instalasi** untuk ditandatangani dan dibubuhi stempel perusahaan, kemudian diunggah kembali pada Portal Pusat Layanan APJII.
4. Jika dalam 7x24 jam, Anggota tidak melakukan penandatanganan dan unggahan **Berita Acara Instalasi** tersebut, maka perangkat yang telah terpasang akan dilakukan ***suspended*** oleh NOC APJII.

6.6 Prosedur Permohonan Penghentian Layanan

1. Anggota/Tenant mengajukan **Permohonan Penghentian Layanan** melalui Portal Pusat Layanan APJII, disertai dengan:
    - Detail informasi perangkat yang terkait pada layanan tersebut.
    - PIC yang akan menerima perangkat.
    - Tanggal layanan dihentikan dan tanggal perangkat yang akan diambil.
2. NOC APJII akan melakukan verifikasi administrasi (status layanan, status tagihan, dan status perangkat) dan akan memberikan respon kepada Anggota/Tenant, **maksimal 1 hari kerja**.
3. Jika tidak ada laporan outstanding dari pihak Finance APJII, maka proses penghentian layanan dapat dilanjutkan oleh NOC APJII.
4. NOC APJII akan melanjutkan dengan proses *Dismantle* dan dilanjutkan *Goods-Out* **maksimal 3 hari kerja** setelah dinyatakan ***clear-outstanding*** dari pihak Finance.

6.7 Prosedur Penggantian Perangkat Co-Location.

1. Anggota/Tenant mengajukan **Permohonan Penggantian Perangkat Co-Location** melalui Portal Pusat Layanan APJII, disertai dengan:
    - Detail informasi perangkat lama dan perangkat baru yang terkait dengan layanan tersebut.
    - PIC yang akan menyerahkan dan menerima perangkat.
    - Tanggal akan dilakukan penggantian perangkat.
2. NOC APJII akan melakukan verifikasi administrasi (status layanan, status tagihan, dan status perangkat) dan akan memberikan respon kepada Anggota/Tenant, **maksimal 1 hari kerja**.
3. Jika tidak ada laporan outstanding dari pihak Finance APJII, maka proses penggantian perangkat dapat dilanjutkan oleh NOC APJII.
4. NOC APJII akan melanjutkan dengan proses *Goods-In* dan dilanjutkan Instalasi **maksimal 3 hari kerja** setelah dinyatakan ***clear-outstanding*** dari pihak Finance.

6.7 Prosedur *Dismantle* Perangkat.

6.7.1. Prosedur Dismantle Permintaan Anggota/Tenant.

- Anggota/Tenant melakukan permohonan dismantle sesuai dengan poin 6.6.
- NOC APJII memastikan perangkat yang akan dilakukan sesuai dengan informasi yang diberikan oleh Anggota/Tenant.
- NOC APJII melakukan terminasi power (listrik).
- NOC APJII melakukan terminasi kabel interkoneksi dan menambahkan label pada kabel interkoneksi yang sudah tidak digunakan tersebut untuk keperluan perapihan kabel interkoneksi.
- NOC APJII melakukan dismantle perangkat dari Rack.
- NOC APJII memastikan perangkat dan aksesorisnya sudah sesuai,
- NOC APJII memastikan Berita Acara Serah Terima ditandatangani oleh kedua belah pihak.
- NOC APJII menyerahkan perangkat kepada PIC Anggota/Tenant di Data Center APJII.

6.7.2. Prosedur Dismantle karena Terhentinya Layanan.

- Jika Anggota/Tenant memiliki tunggakan melebihi batas waktu tertentu yang diatur sesuai dengan peraturan asosiasi keanggotaan dan/atau sesuai dengan peraturan asosiasi terkait fasilitas APJII yang mewajibkan NOC APJII untuk melakukan pemutusan layanan, maka perangkat akan dilakukan *dismantle* oleh NOC APJII segera.
- Jika ditemukan bukti pelanggaran / *abuse* / penyalahgunaan penggunaan perangkat milik Anggota/Tenant yang melanggar kebijakan APJII, maka NOC APJII berhak melakukan pemutusan layanan terhadap perangkat.
- NOC APJII akan terlebih dahulu menginformasikan tindakan dismantle kepada Anggota/Tenant terkait dengan pelanggaran dan/atau tunggakan kewajiban diatas.
- Perangkat yang telah dismantle oleh NOC APJII yang diakibatkan oleh pelanggaran dan/atau tunggakan kewajiban diatas akan disimpan oleh NOC APJII.
- Jika dalam 30 hari kerja Anggota/Tenant tidak menyelesaikan kewajiban tunggakan dan tidak mengambil perangkatnya, maka perangkat tersebut bukan menjadi tanggung jawab APJII.

7. Catatan & Dokumentasi

- Semua aktivitas dicatat dalam sistem: permohonan, Work Permit, berita acara, log barang.
- Dokumen disimpan minimal **2 tahun** untuk kepentingan audit & keamanan.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN VII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP SMARTHAND DATA CENTER APJII

1. Pendahuluan

Layanan **Smart Hand** merupakan layanan bantuan teknis fisik yang disediakan oleh tim operasional Data Center APJII untuk Anggota/Tenant colocation dan tenant lainnya yang membutuhkan dukungan onsite tanpa harus hadir di lokasi. SOP ini berfungsi sebagai acuan standar dalam melakukan permintaan, pelaksanaan, dan pelaporan kegiatan Smart Hand agar berjalan aman, terkendali, dan terdokumentasi sesuai dengan praktik terbaik manajemen layanan data center.

2. Latar Belakang

Data Center APJII beroperasi 24x7x365 untuk menjaga kesinambungan layanan internet nasional. Dalam operasionalnya, Anggota/Tenant sering memerlukan tindakan fisik terhadap perangkat seperti pengecekan, power cycle / restart perangkat, & plug/unplug kabel konektor. Untuk memastikan seluruh kegiatan dilakukan secara **terkendali, terotorisasi, dan terpantau**, maka diperlukan SOP Smart Hand sebagai pedoman resmi yang sesuai dengan standar **TIA-942-C** dan **ISO 20000-1** tentang pengelolaan layanan TI.

3. Tujuan SOP

1. Menetapkan prosedur standar Smart Hand mulai dari permintaan hingga pelaporan.
2. Menjamin keamanan, integritas, dan akuntabilitas setiap aktivitas yang dilakukan terhadap perangkat Anggota/Tenant.
3. Menjaga efisiensi dan kepatuhan terhadap SLA (Service Level Agreement).
4. Mendukung kesiapan audit sertifikasi operasional data center.

4. Obyektif SOP

- Menjamin seluruh aktivitas Smart Hand dilakukan hanya atas dasar permintaan resmi Anggota/Tenant.
- Memastikan pelaksanaan dilakukan oleh NOC APJII.
- Meningkatkan kecepatan layanan dan kepuasan Anggota/Tenant.

5. Dasar & Referensi Standar

1. **TIA-942-C** — Data Center Telecommunications Infrastructure Standard (Clause: Operations & Maintenance).
2. **ISO/IEC 20000-1:2018** — IT Service Management (Service Request Management).
3. **ISO/IEC 27001:2022** — Information Security Management System.
4. **ISO 22301:2019** — Business Continuity Management System.
5. **Kebijakan Internal APJII** — Manajemen Akses, Keamanan Fasilitas, dan Layanan Anggota/Tenant.

6. Definisi & Istilah

Istilah	Definisi
Smart Hand	Layanan bantuan teknis fisik oleh tim data center atas permintaan Anggota/Tenant.
Requestor	Anggota/Tenant yang mengajukan permintaan Smart Hand.
NOC APJII	Unit yang menerima, memverifikasi, dan mengoordinasikan aktivitas Smart Hand dan yang mengerjakan proses Smart Hand.
SLA (Service Level Agreement)	Waktu target untuk respons dan penyelesaian layanan.

7. Ruang Lingkup: Prosedur Smart Hand

SOP ini berlaku untuk seluruh aktivitas Smart Hand yang dilakukan oleh tim NOC APJII di lingkungan Data Center, meliputi:

- Restart / Power Cycle perangkat Anggota/Tenant.
- Pemeriksaan status perangkat (indikator LED, power, temperatur/suhu).
- Plug / Unplug kabel / konektor.

8. Maksimal Permintaan Layanan Smart Hand.

- Maksimal jumlah permintaan layanan Smart Hand dari Anggota/Tenant adalah sebanyak 2x per bulan dan dikerjakan dengan Prioritas-1.
- Apabila Anggota/Tenant telah melewati batas maksimal jumlah permintaan layanan Smart Hand, maka Anggota/Tenant masih dapat mengajukan permintaan Smart Hand, namun akan dikerjakan dengan Prioritas-2.

9. Prosedur Request Smart Hand

9.1 Alur Proses Umum

Berikut adalah tahapan alur utama layanan Smart Hand:

1 REQUEST → 2 RESPONSE → 3 ACTIONS → 4 REPORTING

9.2 Tahapan Detail Proses

Tahap 1: Request (Permintaan Layanan)

- **Pihak:** Anggota/Tenant / Requestor
- **Permohonan diajukan melalui:** Portal Pusat Layanan APJII
- **Informasi wajib disertakan:**
    - Nama Anggota/Tenant dan perusahaan
    - Nomor rak / lokasi perangkat
    - Jenis pekerjaan yang diminta
    - Waktu pelaksanaan yang diinginkan
    - Kontak yang dapat dihubungi
    - Surat/email otorisasi untuk tindakan sensitif (misal: reboot/power cycle)

Tahap 2: Execution (Pelaksanaan di Lokasi)

- **Pihak:** NOC APJII
- **Langkah-langkah:**
    1. Masuk ke area Anggota/Tenant sesuai izin akses.
    2. Lakukan tindakan sesuai permintaan Anggota/Tenant.
    3. Dokumentasikan seluruh langkah (foto/video, catatan).
    4. Melaporkan hasil pekerjaan Smarthand melalui email ke Anggota/Tenant bahwa setelah pekerjaan selesai.
    5. Melakukan update status pekerjaan Smarthand telah selesai di website: https://dc.apjii.or.id/ dan/atau email: tiket@apjii.or.id disertai dengan dokumentasi pekerjaan (foto & video yang diambil, wajib menggunakan ***Timestamp***).

Target:

- Response: ≤ 15 menit.
- Actions:
    - Prioritas-1: ≤ 30 menit, setelah direspon.
    - Prioritas-2: ≤ 120 menit, setelah direspon.

9.5 Pengendalian Keamanan

- Setiap tindakan hanya boleh dilakukan oleh personel **NOC APJII**.
- Dokumentasi yang dikirimkan ke Anggota/Tenant sebagai bukti rekam.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN VIII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENANGANAN GANGGUAN DATA CENTER APJII

1. Pendahuluan

Gangguan (incident/disruption) di Data Center dapat berdampak signifikan pada layanan interkoneksi, colocation, maupun layanan pendukung lain yang diberikan APJII kepada anggotanya. Oleh karena itu, diperlukan SOP yang sistematis agar setiap gangguan dapat ditangani dengan cepat, tepat, dan terdokumentasi sesuai standar manajemen layanan TI dan keamanan data center.

2. Tujuan

- Menetapkan prosedur standar dalam mendeteksi, melaporkan, dan menangani gangguan di Data Center APJII.
- Meminimalkan dampak gangguan terhadap layanan anggota/tenant.
- Menjamin komunikasi efektif antara tim teknis, manajemen, dan anggota.
- Menjadi dasar evaluasi untuk perbaikan berkelanjutan (continuous improvement).

3. Dasar & Referensi Standar

- **ISO/IEC 20000-1** – IT Service Management (Incident Management).
- **ISO/IEC 27001 & 27035** – Information Security Incident Management.
- **TIA-942-C** – Data Center Standard (Operation & Security).
- **ITIL v4 Framework** – Incident & Problem Management.
- Kebijakan Internal APJII terkait operasional Data Center.

4. Definisi Istilah

- **Gangguan (Incident):** Kejadian yang mengakibatkan penurunan kualitas layanan, unavailability, atau potensi risiko terhadap operasi Data Center.
- **Severity:** Tingkat keparahan gangguan berdasarkan dampak dan urgensinya.
- **Prioritas:** Urutan penanganan berdasarkan kombinasi severity dan urgensi.
- **Trouble Ticket:** Sistem pencatatan resmi gangguan untuk tracking & dokumentasi.

- **Escalation:** Proses peningkatan level penanganan jika gangguan tidak terselesaikan dalam SLA.
- **Mean Time To Response:** Rata-rata waktu untuk memberikan response.
- **Mean Time To Repair:** Rata-rata waktu untuk melayani perbaikan.
- **Official Channel:** Nomor kontak Helpdesk APJII/E-mail: tiket@apjii.or.id

5. Ruang Lingkup

- Berlaku untuk semua layanan Data Center APJII (interkoneksi, colocation, smarthand, dan supporting infrastructure).
- Meliputi:
    1. Gangguan layanan ICT (network, server, aplikasi monitoring).
    2. Gangguan infrastruktur pendukung (listrik, pendingin, sistem keamanan, fire suppression).
    3. Gangguan keamanan (akses tidak sah, cyber-attack yang berdampak fisik).

6. Tipe Gangguan & Penanganan

1. **Gangguan Kritis (Critical Incident)**
    - Dampak: Seluruh layanan utama tidak berfungsi (misalnya total listrik padam, interkoneksi nasional lumpuh, bencana alam/force major).
    - Penanganan:
        - Tim NOC APJII wajib siaga penuh.
        - PIC / Penanggung Jawab Operasional DC APJII wajib siaga penuh dan segera berada di lokasi insiden selambat-lambatnya dalam waktu 1 jam sejak insiden dilaporkan.
        - Informasi disampaikan ke manajemen APJII & seluruh tenant DC (kontak teknis & pimpinan perusahaan yang terdapat di MyAPJII) melalui jalur resmi, selambat-lambatnya dalam waktu 1 jam.
        - Eskalasi ke vendor/partner/building management jika penyebab berasal dari pihak eksternal, selambat-lambatnya dalam waktu 1 jam.

2. **Gangguan Mayor (Major Incident)**
    - Dampak: Sebagian besar tenant atau layanan utama terganggu (misalnya salah satu chiller PAC gagal, sebagian rack kehilangan daya listrik).
    - Penanganan:
        - Tim Teknis/NOC APJII wajib siaga penuh.
        - PIC / Penanggung Jawab Operasional DC APJII wajib siaga penuh dan segera berada di lokasi insiden selambat-lambatnya dalam waktu 1 jam sejak insiden dilaporkan.
        - Tim Teknis/NOC APJII segera melakukan *troubleshooting action*, selambat-lambatnya 30 menit sejak insiden dilaporkan.

- Tim Teknis/NOC APJII eskalasi ke vendor/partner/building management jika tidak dapat ditangani oleh tim Teknis/NOC APJII atau penyebab berasal dari pihak eksternal, selambat-lambatnya dalam waktu 1 jam.
- Informasi kendala/gangguan dan estimasi perbaikan disampaikan ke manajemen APJII & kepada tenant DC APJII yang terdampak (kontak teknis & pimpinan perusahaan yang terdapat di MyAPJII) melalui jalur resmi, selambat-lambatnya dalam waktu 3 jam.

3. **Gangguan Minor (Minor Incident)**
   - Dampak: Terbatas pada 1–2 tenant/layanan (misalnya 1 port interkoneksi down, 1 breaker trip).
   - Penanganan:
     - Ditangani langsung oleh Tim Teknis/NOC APJII selambat-lambatnya dalam waktu 1 jam sejak insiden dilaporkan.
     - Informasi kendala/gangguan dan estimasi perbaikan disampaikan ke manajemen APJII & kepada tenant DC APJII yang terdampak (kontak teknis & pimpinan perusahaan yang terdapat di MyAPJII) melalui jalur resmi, selambat-lambatnya dalam waktu 3 jam.

4. **Gangguan Predective (Potential/Warning)**
   - Dampak: Belum terjadi gangguan tetapi berpotensi (misalnya suhu rack meningkat, sensor smoke warning).
   - Penanganan:
     - Tim Teknis/NOC APJII melakukan monitoring intensif.
     - Tim Teknis/NOC APJII melakukan pengecekan fisik.
     - Tim Teknis/NOC APJII eskalasi ke vendor/partner/building management jika tidak dapat ditangani oleh tim Teknis/NOC APJII atau berpotensi menjadi gangguan yang lebih serius, selambat-lambatnya dalam waktu 1 jam.

7. Klasifikasi Severity

Severity	Kriteria	Contoh
Severity 1 (Critical)	Semua layanan utama tidak berfungsi, risiko tinggi terhadap SLA dan BCP	Total listrik padam, konektivitas interkoneksi nasional terputus
Severity 2 (High)	Layanan utama sebagian terganggu, dampak luas > 50% tenant	Pendingin CRAC mati, salah satu jalur listrik utama trip
Severity 3 (Medium)	Gangguan terbatas, dampak < 10% tenant	1 port interkoneksi down, 1 rack mati
Severity 4 (Low)	Tidak ada dampak langsung pada tenant, hanya potensi atau peringatan	Suhu meningkat, alert UPS overload, sensor smoke aktif

8. Penentuan Prioritas

Prioritas = **Severity x Urgensi**

Prioritas	Kriteria	Target SLA
P1 (Highest)	Severity 1 – Urgensi tinggi	Mean Time To Response ≤ 15 menit, Mean Time To Repair ≤ 4 jam (diluar dari bencana alam/force major)
P2	Severity 2 – Urgensi tinggi	Mean Time To Response ≤ 15 menit, Mean Time To Repair ≤ 12 jam
P3	Severity 3 – Urgensi sedang	Mean Time To Response ≤ 15 menit, Mean Time To Repair ≤ 24 jam
P4 (Lowest)	Severity 4 – Urgensi rendah	Mean Time To Response ≤ 15 menit, Mean Time To Repair ≤ 3 hari

9. Tahapan Penanganan Gangguan

1. **Deteksi**
    - Melalui sistem monitoring, temuan atau laporan tenant.
2. **Pencatatan**
    - Gangguan dicatat dalam **Trouble Ticketing System** dengan nomor tiket unik.
3. **Klasifikasi & Prioritas**
    - Ditentukan severity & prioritas oleh Tim NOC APJII.
4. **Respon Awal**
    - Tim Teknis/NOC APJII melakukan analisis cepat & memberikan estimasi waktu penyelesaian.
5. **Eskalasi (Jika Perlu)**
    - Jika tidak selesai dalam penanganan gangguan, maka Tim Teknis/NOC APJII maka akan melakukan eskalasi ke PIC/Penanggug Jawab Operasional DC APJII.
6. **Pemulihan (Recovery)**
    - Perbaikan dilakukan sesuai prosedur teknis.
    - Konfirmasi layanan normal kembali.
7. **Komunikasi**
    - Tim Teknis/NOC APJII akan melakukan update status ke Helpdesk APJII dan Helpdesk APJII akan mempublikasikan secara berkala kepada anggota/tenant yang terdampak via portal DCIM (per 30 menit) atau menginformasikan via e-mail/WA Group untuk kendala gangguan *Critical* dan/atau *Major Incident*.
    - Laporan insiden final disampaikan ke manajemen & anggota/tenant.

8. **Penutupan Tiket**
    - Setelah perbaikan selesai & konfirmasi dari anggota/tenant, maka tiket ditutup secara otomatis dalam waktu selambat-lambatnya 1 x 24 jam.
9. **Post-Incident Review**
    - Analisis akar penyebab (Root Cause Analysis – RCA).
    - Rekomendasi perbaikan / predective maintenance.

10. Rekomendasi

- Melakukan **drill penanganan gangguan** (simulasi BCP/DRP) minimal 1 kali per tahun.
- Menggunakan **dashboard monitoring terintegrasi (DCIM)** untuk mempercepat deteksi.
- Menyediakan **SOP komunikasi insiden** agar tenant selalu mendapat informasi tepat waktu.
- Menetapkan **Knowledge Base** internal sebagai referensi troubleshooting standar.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN IX
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENANGANAN GANGGUAN DARURAT / FORCE MAJEURE DATA CENTER APJII

1. Pendahuluan

Data Center APJII merupakan fasilitas kritikal yang menyediakan layanan infrastruktur internet nasional bagi anggota APJII dan pemangku kepentingan lain. Mengingat perannya yang vital dalam menjaga konektivitas nasional, diperlukan prosedur yang sistematis untuk menghadapi **gangguan darurat akibat bencana alam atau kondisi force majeure**, agar kelangsungan layanan tetap terjaga dan dampak operasional dapat diminimalkan.

SOP ini menjadi panduan utama bagi seluruh personel operasional, keamanan, teknis, dan manajemen dalam melaksanakan tindakan respons cepat, mitigasi, dan pemulihan terhadap berbagai bentuk bencana alam maupun peristiwa tak terduga yang dapat mengganggu keberlangsungan operasional Data Center APJII.

2. Tujuan

Tujuan dari SOP ini adalah:

1. Menetapkan langkah-langkah penanganan darurat yang **terencana, terkoordinasi, dan efektif** dalam menghadapi bencana alam atau kejadian force majeure.
2. Memastikan **keselamatan personel**, **perlindungan aset infrastruktur dan data**, serta **kelangsungan layanan utama** (availability & uptime) tetap terjaga.
3. Menentukan **mekanisme komunikasi, eskalasi, dan pelaporan** selama dan setelah kejadian darurat.
4. Menyediakan **kerangka pemulihan operasional** (disaster recovery & business continuity) sesuai dengan standar internasional.
5. Mendukung kepatuhan terhadap **persyaratan sertifikasi dan audit** TIA-942, ISO 22301, dan DCOS terkait kesiapsiagaan bencana.

3. Dasar dan Referensi Standar

SOP ini disusun dengan mengacu pada standar, peraturan, dan pedoman berikut:

3.1 Standar Internasional

- **ISO 22301:2019** – Business Continuity Management Systems (BCMS)
- **ISO 27001:2022** – Information Security Management Systems
- **ISO 31000:2018** – Risk Management Guidelines
- **TIA-942-C** – Telecommunications Infrastructure Standard for Data Centers (Clause 6.3 & 6.4: Risk Assessment, Availability, and Environmental Considerations)
- **DCOS (Data Centre Operations Standard)** – Domain: Emergency Preparedness and Incident Management

3.2 Regulasi Nasional

- **Peraturan Pemerintah No. 82 Tahun 2012** tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE)
- **Permen Kominfo No. 4 Tahun 2016** tentang Sistem Manajemen Keamanan Informasi
- **Peraturan Kepala BNPB No. 4 Tahun 2019** tentang Pedoman Penyusunan Rencana Kontinjensi

3.3 Dokumen Internal

- Kebijakan Business Continuity Plan (BCP) APJII
- Disaster Recovery Plan (DRP) APJII
- Prosedur Evakuasi dan Keselamatan Kerja Data Center APJII
- Risk Assessment Register dan Environmental Risk Matrix

4. Definisi Istilah

Istilah	Definisi
Force Majeure	Keadaan Kahar (Force Majeure) adalah suatu kejadian diluar kemampuan dan kendali manusia, tidak dapat dihindarkan, dan tidak terbatas pada bencana alam, kebakaran, banjir, pemogokan umum, perang (dinyatakan atau tidak dinyatakan), pemberontakan, revolusi, makar, huru-hara, terorisme, wabah (baik wilayah, epidemik maupun endemik) dan diketahui secara luas sehingga kegiatan operasional Data Center APJII tidak dapat dilaksanakan sebagaimana mestinya.
Insiden Darurat	Kejadian lain yang tak terduga yang berpotensi mengganggu kegiatan operasional DC APJII, sehingga kegiatannya tidak dapat dilaksanakan sebagaimana mestinya.
Disaster Recovery (DR)	Proses pemulihan sistem dan fasilitas fisik agar dapat kembali beroperasional sebagaimana mestinya.
Business Continuity (BC)	Upaya mempertahankan kelangsungan proses operasional DC APJII selama terjadinya insiden.

Istilah	Definisi
Incident Commanding Officer (ICO)	Personel yang bertanggungjawab untuk memimpin tanggap darurat saat kejadian berlangsung.
Emergency Response Team (ERT)	Tim khusus yang bertugas melaksanakan evakuasi, pengamanan, dan mitigasi dampak bencana di fasilitas.
Critical Systems	Sistem utama yang mempengaruhi ketersediaan layanan, seperti infrastruktur ME (Mechanical & Electrical) dan jaringan backbone.
***R*esponsible**	Orang atau tim yang melaksanakan pekerjaan langsung**.** Mereka bertanggung jawab untuk menyelesaikan tugas atau aktivitas yang dimaksud. Bisa lebih dari satu orang.
***A*ccountable**	Orang yang memiliki tanggung jawab penuh atas hasil akhir dari aktivitas tersebut. Hanya satu orang yang boleh ditetapkan sebagai “Accountable” untuk setiap tugas agar tidak terjadi kebingungan dalam tanggung jawab.
***C*onsulted**	Orang atau pihak yang memiliki keahlian atau informasi khusus dan diberi kesempatan untuk memberikan masukan sebelum keputusan diambil atau pekerjaan dilakukan. Biasanya komunikasi bersifat dua arah.
***I*nformed**	Orang atau pihak yang perlu mengetahui hasil atau perkembangan dari aktivitas, namun tidak terlibat langsung dalam pelaksanaan maupun pengambilan keputusan. Biasanya komunikasi bersifat satu arah.

5. Ruang Lingkup

SOP ini berlaku untuk seluruh area dan sistem di lingkungan **Data Center APJII**, mencakup:

5.1 Area Fasilitas

- Data Hall utama APJII

5.2 Jenis Gangguan/Bencana yang Dicakup

1. **Gempa bumi**
2. **Banjir atau genangan air**
3. **Kebakaran**
4. **Petir dan gangguan kelistrikan eksternal**
5. **Kegagalan daya dari PLN dan backup system**
6. **Gangguan jaringan komunikasi eksternal**
7. **Kerusuhan sosial atau tindakan sabotase**
8. **Pandemi atau kejadian kesehatan massal**
9. **Ledakan, kebocoran bahan kimia, atau gas beracun**
10. **Kegagalan besar sistem HVAC atau sistem pendinginan utama**

5.3 Personel yang Terlibat

- **Incident Commanding Officer (ICO)** – Koordinator utama penanganan
- **Penanggung Jawab Operasional DC APJII** – Pengambil keputusan akhir
- **Emergency Response Team (ERT)** – Pelaksana teknis dan evakuasi
- **Security Team** – Pengendalian akses dan keamanan perimeter
- **NOC Team** – Pengamanan server, jaringan, dan sistem kritikal
- **Technical Team** – Pemulihan infrastruktur listrik dan mekanikal
- **Sekretariat APJII** – Hubungan internal dan eksternal (APJII, vendor, dan pihak berwenang)

5.4 Lokasi dan Koordinasi Eksternal

SOP ini juga mencakup koordinasi dengan:

- **BNPB / BPBD** (Badan Penanggulangan Bencana Daerah/Nasional)
- **PLN**, **Provider Jaringan**, dan **Vendor Maintenance**
- **Pemadam Kebakaran**
- **Paramedis**
- **Polsek/Polres setempat**
- **Manajemen Gedung** (bila Data Center berada di gedung bersama)

6. Prosedur Umum

1. **Deteksi dan Aktivasi**
    - Sistem monitoring (BMS, Fire Panel, VESDA, WLDS, dsb.) mendeteksi kondisi abnormal.
    - **ICO** segera mengaktifkan status *Emergency Mode* dan menginformasikan kepada seluruh tim.
2. **Respon Awal dan Evakuasi**
    - Personel diarahkan ke titik kumpul aman sesuai denah evakuasi.
    - Sistem kritikal diamankan melalui prosedur *Emergency Shutdown* jika diperlukan.
3. **Koordinasi dan Eskalasi**
    - **ICO** berkoordinasi dengan pihak eksternal (BNPB/PLN/Vendor).
    - Komunikasi resmi dilakukan oleh **Sekretariat APJII**.
4. **Pemulihan dan Pemantauan**
    - Setelah situasi dinyatakan aman, tim melakukan inspeksi kerusakan.
    - DR Plan diaktifkan jika sistem utama tidak dapat segera pulih.
    - Laporan insiden disusun maksimal 24 jam pasca kejadian.

7. Langkah-Langkah Penanganan Per Jenis Bencana

Berikut panduan terperinci untuk setiap skenario bencana yang mungkin terjadi di Data Center APJII:

7.1 Gempa Bumi

Tahap 1 – Saat Gempa Terjadi

- Tetap tenang, jangan panik dan jangan berlari.
- Segera berlindung di bawah meja yang kokoh atau struktur pelindung.
- Hindari berdiri dekat rak server, kaca, panel listrik, dan benda gantung.
- Jangan gunakan lift.

Tahap 2 – Setelah Guncangan Mereda

- Incident Commanding Officer (ICO) mengaktifkan status darurat.
- ERT memeriksa seluruh area untuk mendeteksi potensi kebakaran, kebocoran bahan bakar, atau kerusakan struktural.
- Lakukan **shutdown bertahap sistem non-kritikal** bila ada indikasi kerusakan fisik.
- Evakuasi personel ke titik kumpul aman di area terbuka yang telah ditentukan.

Tahap 3 – Pemulihan Awal

- Lakukan inspeksi menyeluruh pada:
    - Struktur bangunan & raised floor.
    - Racks dan peralatan IT.
    - Power path (UPS, PDU, genset).
    - Cooling system (PAC/CRAC).
- Koordinasi dengan **BPBD setempat** dan **vendor safety building** sebelum re-entry.

7.2 Kebakaran

Tahap 1 – Deteksi Awal

- Alarm dari **VESDA / Smoke Detector / Fire Panel** aktif.
- ICO mengumumkan **Evakuasi Segera** melalui sistem PA (Public Address).
- ERT memastikan area sumber asap dikonfirmasi dan memverifikasi apakah sistem **Fire Suppression** telah aktif otomatis.

Tahap 2 – Penanganan

- Jika aman, ERT menggunakan **APAR CO_2 atau Dry Chemical** untuk titik api kecil.
- Jika api besar, **tinggalkan area dan tutup pintu ruang** untuk menahan penyebaran api.
- Sistem fire suppression otomatis aktif secara penuh.
- Pastikan semua personel keluar menuju titik kumpul (*assembly point*) yang aman.

Tahap 3 – Pemulihan

- Setelah api padam dan area dinyatakan aman oleh petugas Damkar:
    - Lakukan assessment kerusakan.
    - Aktifkan sistem cadangan bila diperlukan (mis. data hall sekunder).
    - Jalankan DR Plan jika sistem utama terdampak.

7.3 Banjir atau Genangan Air

Tahap 1 – Peringatan

- Deteksi oleh **WLDS (Water Leak Detection System)** atau laporan visual.
- Matikan peralatan listrik di area terdampak jika memungkinkan dan aman.

Tahap 2 – Penanganan

- ERT segera menutup aliran air (valve utama).
- Gunakan pompa cadangan atau penyedot air untuk mengeringkan area.
- Amankan peralatan sensitif dan kabel listrik dari kontak air.

Tahap 3 – Pemulihan

- Periksa kelembapan ruang dan sistem grounding.
- Lakukan inspeksi ulang pada **kabel daya dan komunikasi**.
- Jalankan sistem pendingin dan listrik secara bertahap setelah area benar-benar kering.

7.4 Gangguan Listrik / Blackout Total

Tahap 1 – Deteksi

- Sistem BMS atau alarm UPS mendeteksi kehilangan daya utama PLN.

Tahap 2 – Respons

- **UPS dan baterai** akan mengambil alih beban otomatis.
- **Genset** aktif otomatis dalam ≤30 detik.
- ERT memantau status beban listrik, suhu ruangan, dan fuel level.

Tahap 3 – Pemulihan

- Setelah daya PLN stabil dan diverifikasi aman, sistem dikembalikan ke mode normal (supply PLN).
- Semua log kejadian disimpan dan dikaji.

7.5 Kerusuhan, Sabotase, atau Ancaman Keamanan

- Security segera mengaktifkan **Lockdown Mode**.
- Semua akses dikontrol melalui **Access Control System**.
- Informasikan ke Polsek/Polres setempat dan Manajemen APJII.
- Personel non-esensial dievakuasi melalui jalur aman.
- Setelah situasi terkendali, lakukan audit keamanan dan recovery aset.

7.6 Pandemi atau Kejadian Kesehatan Massal

- Terapkan **protokol karantina dan pembatasan personel onsite**.
- Aktifkan **model operasi remote (remote NOC)** untuk tim monitoring.
- Lakukan disinfeksi rutin dan sediakan APD bagi staf onsite.
- Dokumentasikan daftar personel yang bertugas selama periode pandemi.

8. Alur Komunikasi dan Eskalasi Internal

8.1 Level Eskalasi

Level	Kriteria	Tindakan	Penanggung Jawab
Level 1 – Minor Incident	Gangguan tidak berdampak pada layanan utama	Penanganan oleh ERT lokal	Tim NOC APJII
Level 2 – Major Incident	Gangguan menyebabkan downtime < 4 jam	Aktivasi IC, notifikasi ke Manajer DC	PIC / Penanggung Jawab Operasional DC APJII
Level 3 – Disaster / Force Majeure	Gangguan masif, downtime > 4 jam, atau evakuasi total	Aktivasi BCP & DR Plan	PIC / Penanggungg Jawab Operasional DC APJII

8.2 Alur Komunikasi Darurat

1. **Deteksi Insiden** → Operator NOC / ERT mendeteksi dan melapor ke IC.
2. **Verifikasi** → IC melakukan validasi dan menentukan level insiden.
3. **Aktivasi** → Jika major/disaster, IC mengaktifkan BCP dan DR.
4. **Notifikasi Internal** → Ke Manajer DC, Direktur Teknis APJII, BCP Team, dan Komunikasi Publik.
5. **Koordinasi Eksternal** → Dengan pihak PLN, Damkar, BNPB, vendor terkait.
6. **Laporan Resmi** → Disusun maksimal 24 jam setelah kejadian.

9. Prosedur Pemulihan Sistem (DR & BCP)

9.1 Aktivasi DR Site

- Jika sistem utama DC APJII tidak dapat beroperasi dalam waktu > 4 jam, **DR Site** diaktifkan.
- Sinkronisasi terakhir (replication logs) digunakan untuk restore data.
- Prioritas pemulihan:
    1. Core Network Infrastructure (Router, Switch, Firewall)
    2. DNS, IX Router, dan NOC Systems
    3. Monitoring Tools dan Ticketing System
    4. Secondary Storage dan Backup Systems

9.2 Tahapan Pemulihan

1. **Assessment dan Isolasi** – identifikasi area terdampak.
2. **Stabilisasi** – pemulihan listrik, pendinginan, dan keamanan.
3. **Restorasi Sistem IT** – aktivasi backup server dan storage.
4. **Verifikasi dan Testing** – memastikan sistem berfungsi normal.
5. **Re-entry** – DC kembali beroperasi normal.

9.3 Koordinasi dan Dokumentasi

- Semua langkah dicatat dalam *Disaster Log Sheet*.
- Keputusan aktivasi DR disetujui oleh **BCP Coordinator** dan **Direktur Teknis APJII**.

10. Struktur Tanggung Jawab (RACI Chart)

Aktivitas	Incident Commander	ERT	Security	IT Ops	Facility	Manajemen APJII
Deteksi & Aktivasi Alarm	A	R	C	C	C	I
Evakuasi Personel	A	R	R	C	C	I
Koordinasi Eksternal (BNPB, PLN)	A	C	C	I	R	I
Pemulihan Infrastruktur	C	C	C	R	A	I
Aktivasi DR Site	C	C	I	A	I	R
Komunikasi Publik & Pelaporan	C	I	I	I	I	A
Audit & Evaluasi Pascakejadian	C	C	I	C	R	A

Keterangan:

- **R** = ***R***esponsible (Pelaksana).
- **A** = ***A***ccountable (Penanggung Jawab Akhir).
- **C** = ***C***onsulted (Konsultan/Dilibatkan untuk Masukan)
- **I** = ***I***nformed (Diberi Informasi).

11. Formulir & Checklist Pascakejadian

11.1 Formulir Laporan Insiden Darurat

Item	Keterangan
Tanggal & Waktu Kejadian	
Jenis Bencana	
Lokasi Area	
Personel Terlibat	
Dampak terhadap Operasional	
Tindakan yang Diambil	

Item	Keterangan
Sistem yang Terpengaruh	
Estimasi Downtime	
Koordinasi dengan Pihak Eksternal	
Status Pemulihan	
Catatan / Rekomendasi	

11.2 Checklist Evaluasi Pascakejadian

No	Aspek Evaluasi	Ya/Tidak	Catatan
1	Sistem alarm berfungsi dengan baik		
2	Evakuasi dilakukan sesuai prosedur		
3	Tidak ada korban cedera		
4	Sistem UPS dan genset berfungsi saat blackout		
5	Sistem pendingin kembali normal		
6	Komunikasi internal berjalan lancar		
7	DR site diaktifkan sesuai waktu RTO		
8	Laporan insiden diserahkan dalam 24 jam		

12. Mekanisme Evaluasi & Continuous Improvement

1. **Post-Incident Review (PIR)** dilakukan maksimal **7 hari setelah kejadian**, dipimpin oleh **Data Center Manager**.
2. Evaluasi mencakup:
    - Kecepatan respon dan efektivitas komunikasi.
    - Ketepatan pelaksanaan SOP dan evakuasi.
    - Kinerja sistem pendukung (UPS, genset, fire system).
    - Kepatuhan terhadap RTO (Recovery Time Objective) dan RPO (Recovery Point Objective).
3. **Temuan dan rekomendasi** PIR dituangkan dalam *Incident Improvement Report*.
4. **Tindakan korektif dan pencegahan (CAPA)** ditetapkan dan diverifikasi implementasinya dalam waktu maksimal 30 hari.
5. Hasil evaluasi dimasukkan ke dalam **agenda rapat tahunan BCMS review meeting** untuk memastikan perbaikan berkelanjutan.

13. Penutup

SOP ini berlaku untuk seluruh Data Center APJII dan harus ditinjau ulang minimal **setiap 12 bulan** atau setelah setiap kejadian besar.

Semua personel wajib mengikuti pelatihan simulasi tanggap darurat (**emergency drill**) minimal **dua kali dalam setahun**, mencakup skenario gempa, kebakaran, dan gangguan daya.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN X
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENANGANAN GANGGUAN DARURAT GEMPA BUMI, BANJIR/GENANGAN AIR DATA CENTER APJII

1. Pendahuluan

Data Center APJII merupakan fasilitas kritikal nasional yang berfungsi sebagai pusat interkoneksi jaringan Internet Indonesia (IIX), tempat beroperasinya server, router, dan infrastruktur backbone utama penyelenggara jasa internet (ISP). Keandalan operasional data center ini sangat vital untuk menjaga konektivitas nasional tetap berjalan tanpa gangguan.

Indonesia merupakan wilayah rawan bencana alam, khususnya **gempa bumi dan banjir**. Oleh karena itu, diperlukan prosedur standar yang komprehensif dalam **menangani kondisi darurat akibat gempa bumi dan banjir**, untuk memastikan:

- Keselamatan seluruh personel di dalam fasilitas.
- Perlindungan terhadap infrastruktur IT, power, dan sistem pendukung kritikal.
- Pemulihan operasi (recovery) secepat mungkin setelah kejadian.

SOP ini menjadi pedoman bagi seluruh personel operasional, teknisi, security, housekeeping, dan manajemen Data Center APJII dalam merespons situasi darurat secara cepat, tepat, dan terkoordinasi.

2. Tujuan

Tujuan dari SOP ini adalah untuk:

1. Menetapkan langkah-langkah terstruktur dalam menghadapi dan menangani gangguan darurat akibat **gempa bumi dan banjir/Genangan Air** di lingkungan Data Center APJII.
2. Melindungi keselamatan seluruh **personel/karyawan APJII, tamu, dan pengunjung** di dalam area fasilitas.
3. Menjamin keamanan dan keandalan sistem **critical infrastructure**, termasuk power supply, cooling, network equipment, dan fire protection.
4. Meminimalkan **downtime** operasional dan kerugian akibat gangguan fisik.
5. Mendukung kelancaran pelaksanaan **Business Continuity Plan (BCP)** dan **Disaster Recovery Plan (DRP)**.
6. Menjadi panduan dalam **koordinasi lintas tim** (Security, Facility, NOC, dan Manajemen) selama fase tanggap darurat hingga pemulihan.

3. Dasar dan Referensi Standar

SOP ini disusun berdasarkan dan merujuk pada standar, regulasi, serta pedoman teknis sebagai berikut:

3.1. Standar Internasional dan Nasional

- **ISO 22301:2019** — *Business Continuity Management Systems (BCMS)*
- **ISO 45001:2018** — *Occupational Health and Safety Management Systems*
- **TIA-942-C:2024** — *Telecommunications Infrastructure Standard for Data Centers*
- **NFPA 75** — *Standard for the Fire Protection of Information Technology Equipment*
- **NFPA 76** — *Telecommunications Facilities Standard*
- **IEC 60364-4-44** — *Protection against voltage disturbances and electromagnetic disturbances*
- **SNI 03-1733-2004** — *Tata Cara Perencanaan Lingkungan Kerja terhadap Kebisingan dan Getaran*
- **Peraturan Kepala BNPB No. 4 Tahun 2008** — *Pedoman Penyusunan Rencana Penanggulangan Bencana*
- **Peraturan Menteri Ketenagakerjaan No. 5 Tahun 2018** — *K3 Lingkungan Kerja Fisik*

4. Definisi Istilah

Istilah	Definisi
Gempa Bumi	Getaran atau guncangan pada permukaan bumi akibat pergerakan lapisan bumi (tektonik atau vulkanik) yang berpotensi menyebabkan kerusakan pada struktur bangunan dan peralatan.
Banjir/Genangan Air	Kondisi naiknya permukaan air akibat curah hujan ekstrem, saluran air tersumbat, atau limpasan dari luar area yang menyebabkan genangan di sekitar atau dalam fasilitas.
Incident Commanding Officer (ICO)	Personel yang ditunjuk sebagai penanggung jawab utama dalam penanganan kondisi darurat di fasilitas & Operasional Data Center APJII. Biasanya dijabat oleh PIC / Penanggung Jawab Operasional DC APJII.
Emergency Response Team (ERT)	Tim tanggap darurat yang terdiri dari personel dari berbagai fungsi bertugas menangani situasi darurat.
Titik Kumpul (Assembly Point)	Titik kumpul aman yang telah ditentukan di luar area gedung untuk berkumpul setelah evakuasi.
Critical Infrastructure	Infrastruktur vital seperti sistem UPS, sistem pendingin, sistem jaringan, sistem kebakaran, dan power distribution yang mendukung operasi data center.

Istilah	Definisi
Recovery Phase	Tahapan pemulihan operasional setelah keadaan darurat dinyatakan aman.

5. Ruang Lingkup

SOP ini mencakup seluruh kegiatan penanganan darurat di fasilitas Data Center APJII, meliputi:

5.1. Lokasi yang Dicakup

- Seluruh area Operasional Data Center APJII di Gedung Cyber-1.

5.2. Situasi yang Dicakup

1. **Gempa Bumi**
    - Getaran ringan hingga berat yang berpotensi menyebabkan kerusakan struktural atau kebakaran sekunder.
    - Risiko jatuhnya benda berat, pecahan kaca, dan gangguan listrik.
2. **Banjir atau Genangan Air**
    - Air masuk ke area ruang server, ruang listrik, atau basement akibat hujan deras atau drainase tidak berfungsi.
    - Kelembapan berlebih yang berpotensi menyebabkan kerusakan pada sistem kelistrikan dan pendingin.

5.3. Tahapan Penanganan yang Dicakup

- **Pra-Kejadian (Mitigasi dan Kesiapsiagaan)**
  Menetapkan langkah preventif seperti pemeriksaan pompa, drainase, deteksi kebocoran air (WLDS), dan simulasi evakuasi.
- **Saat Kejadian (Respons Darurat)**
  Langkah real-time yang harus dilakukan selama gempa atau banjir sedang terjadi untuk melindungi keselamatan jiwa dan infrastruktur.
- **Pasca-Kejadian (Pemulihan dan Evaluasi)**
  Prosedur pemeriksaan keamanan, pemulihan sistem, dokumentasi insiden, dan evaluasi perbaikan untuk peningkatan berkelanjutan.

5.4. Pihak yang Bertanggung Jawab

Peran / Jabatan	Tanggung Jawab Utama
Kabid DC & IIX (APJII Incident Commander)	Mengkoordinasikan seluruh tindakan darurat dan memastikan keselamatan fasilitas.
Tim NOC APJI	Mengamankan perangkat jaringan, sistem monitoring, dan dokumentasi insiden.

Peran / Jabatan	Tanggung Jawab Utama
Security Supervisor	Mengarahkan evakuasi, mengontrol akses keluar/masuk, dan memastikan area aman.
Tim Teknis APJII	Mematikan sistem power atau cooling jika diperlukan, memeriksa infrastruktur setelah kejadian.
Housekeeping	Membantu membersihkan area terdampak banjir dan memastikan jalur evakuasi bebas hambatan.
HR/Admin	Melakukan pendataan personel dan memastikan semua pegawai/tamu dalam kondisi aman.

6. Prosedur Operasional Lengkap

6.1. Mitigasi dan Kesiapsiagaan Pra-Kejadian

No.	Langkah / Aktivitas	Penanggung Jawab	Frekuensi / Waktu Pelaksanaan	Keterangan / Catatan
1	Melakukan **inspeksi struktural** bangunan dan rak server (pastikan baut pengikat, bracing, anti-seismic rack terpasang baik).	Facility Team	6 bulanan	Ikuti panduan TIA-942-C
2	Memastikan **jalur evakuasi dan titik kumpul (Muster Point)** bersih, tidak terhalang, dan papan petunjuk jelas.	Security & HSE	Bulanan	Wajib sesuai layout evakuasi yang diperbarui.
3	Melakukan **uji fungsi sistem WLDS (Water Leak Detection System)** dan **drainase/pompa air** untuk pencegahan banjir.	Facility Team	Bulanan	Catat hasil tes di log sheet.
4	Meninjau **rencana kontinuitas bisnis (BCP)** dan memastikan kontak darurat semua pihak tersedia dan diperbarui.	BCP Coordinator	Triwulanan	Sertakan kontak PLN, Pemadam, BNPB lokal.
5	Melakukan **simulasi evakuasi gempa dan banjir** minimal 2 kali per tahun.	HSE & ERT	6 bulanan	Dokumentasi simulasi wajib disimpan.

No.	Langkah / Aktivitas	Penanggung Jawab	Frekuensi / Waktu Pelaksanaan	Keterangan / Catatan
6	Menyediakan dan memeriksa **peralatan darurat** (P3K, helm, lampu emergency, pompa portable, sepatu boot anti air).	Security & Housekeeping	Bulanan	Pastikan lokasi storage diketahui semua personel.
7	Melakukan **backup data sistem kritikal** secara rutin (offsite dan cloud).	NOC Team	Harian	Pastikan sistem monitoring berfungsi 24/7.

6.2. Prosedur Saat Kejadian – Gempa Bumi

A. Tindakan Saat Gempa Terjadi

No.	Langkah / Aktivitas	Penanggung Jawab	Tujuan / Hasil Diharapkan
1	Tetap tenang dan **tidak panik**, segera berlindung di bawah meja atau area aman jauh dari kaca, lemari, atau rak tinggi.	Seluruh Personel	Mencegah cedera akibat jatuhan benda.
2	**Dilarang berlari atau menggunakan lift.**	Semua personel	Hindari kecelakaan.
3	NOC dan Facility Team menjaga posisi aman, hindari panel listrik atau UPS room selama getaran.	NOC, Facility	Hindari risiko sengatan listrik atau kebakaran sekunder.
4	Setelah getaran berhenti, **Incident Commander (IC)** segera aktifkan **Emergency Response Team (ERT)**.	IC / Facility Manager	Memulai fase penilaian bahaya.
5	IC memerintahkan evakuasi ke **Muster Point** sesuai rute evakuasi terdekat.	Security & ERT	Menjaga keselamatan personel.

B. Setelah Gempa Berhenti (Tahap Penilaian Awal)

No.	Langkah / Aktivitas	Penanggung Jawab	Catatan / Tindakan Lanjutan
1	Pastikan seluruh personel dievakuasi dan aman, lakukan **absensi dan pendataan** di titik kumpul.	HR / Security	Laporkan jumlah personel ke IC.

No.	Langkah / Aktivitas	Penanggung Jawab	Catatan / Tindakan Lanjutan
2	Lakukan **pemeriksaan visual** bangunan dari luar (retakan, kerusakan struktur, panel jatuh).	Facility & Security	Jangan masuk sebelum dinyatakan aman.
3	Jika aman, lakukan **inspeksi bertahap**: ruang genset, panel listrik, UPS, baterai, dan server hall.	Facility Team	Gunakan APD lengkap.
4	Periksa **kebocoran bahan bakar, kebakaran, atau pipa pecah.**	Facility Team	Isolasi area bahaya segera.
5	NOC memastikan **sistem monitoring dan power status** (UPS/battery runtime) tetap stabil.	NOC	Laporkan ke IC jika ada alarm kritikal.
6	Jika ditemukan kerusakan berat, IC aktifkan **Disaster Recovery Plan (DRP)** untuk alih beban ke site cadangan.	IC & NOC	Koordinasi dengan tim regional APJII.

6.3. Prosedur Saat Kejadian – Banjir / Genangan Air

A. Saat Deteksi Awal (Air Masuk atau WLDS Alarm Aktif)

No.	Langkah / Aktivitas	Penanggung Jawab	Tujuan / Catatan
1	Segera konfirmasi sumber air (drainase, hujan, AC condensate, pipa bocor).	Facility Team	Identifikasi tingkat bahaya.
2	**Matikan power supply** pada area terdampak jika air mendekati perangkat listrik rendah.	Facility Team	Hindari risiko arus pendek.
3	NOC melakukan **monitoring suhu dan kelembapan** ruang server untuk mendeteksi potensi gangguan.	NOC	Pastikan lingkungan masih dalam batas aman.
4	Aktifkan **pompa air otomatis/manual** dan arahkan jalur drainase.	Facility / Housekeeping	Minimalisir genangan.
5	Pindahkan perangkat/asset penting ke area aman yang lebih tinggi.	Semua tim	Prioritaskan server, PDU, battery, dokumen.
6	Jika kondisi memburuk, **IC perintahkan evakuasi** ke area aman sesuai rencana.	IC / Security	Keselamatan personel utama.

B. Saat Banjir Meluas atau Masuk ke Area Kritis

No.	Langkah / Aktivitas	Penanggung Jawab	Catatan / Tindakan Lanjutan
1	Facility menutup jalur listrik utama (MCB/ACB Panel) di area terdampak.	Facility Manager	Catat status shutdown.
2	Koordinasikan dengan **PLN / genset operator** untuk pemutusan sementara suplai.	IC & Facility	Hindari backfeed berbahaya.
3	Dokumentasikan lokasi genangan dengan foto/video.	Security / Admin	Bukti laporan insiden.
4	Pastikan jalur evakuasi bebas air dan aman dilewati.	Security	Gunakan sepatu boot isolator.
5	Setelah air surut, lakukan **pengeringan & disinfeksi area**.	Housekeeping	Gunakan dehumidifier jika tersedia.

6.4. Tahap Pemulihan (Recovery Phase)

No.	Langkah / Aktivitas	Penanggung Jawab	Tujuan / Output
1	Lakukan **pemeriksaan keamanan struktur dan kelistrikan** oleh tim teknis dan pihak ketiga tersertifikasi.	Facility Manager	Pastikan aman sebelum power-up.
2	Lakukan **power-on bertahap** untuk sistem UPS, PDU, dan server.	NOC & Facility	Hindari lonjakan arus.
3	Verifikasi **fungsi sistem pendingin, deteksi kebocoran, dan alarm**.	Facility	Pastikan kondisi normal.
4	Aktifkan **sistem monitoring (BMS/DCIM)** untuk memastikan parameter kembali stabil.	NOC	Rekam semua log sistem.
5	Pastikan **backup data** dari DR site sudah sinkron kembali.	NOC	Validasi integritas data.
6	Lakukan **pelaporan insiden resmi** kepada Manajemen APJII dan pihak terkait (mis. PLN, pemadam, BNPB).	IC / Admin	Wajib diselesaikan dalam 48 jam.

6.5. Dokumentasi dan Evaluasi Pasca-Kejadian

No.	Langkah / Aktivitas	Penanggung Jawab	Catatan / Output
1	Mengisi **Incident Report Form** lengkap dengan kronologi, waktu, area terdampak, dan tindakan yang diambil.	IC / Admin	Diserahkan ke manajemen.
2	Melakukan **evaluasi pasca-insiden (After Action Review)** untuk identifikasi penyebab dan pelajaran.	BCP Committee	Jadwal maksimal 7 hari setelah kejadian.
3	Menyusun **Corrective and Preventive Action (CAPA)** untuk mencegah kejadian serupa.	Facility & HSE	Revisi SOP jika diperlukan.
4	Melakukan **update rencana BCP/DRP** berdasarkan hasil evaluasi.	BCP Coordinator	Pastikan versi terbaru terdokumentasi.
5	Arsipkan semua laporan (foto, form, log, checklist, laporan pihak ketiga) di repository BCP.	Admin	Retensi minimal 3 tahun.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XI
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENANGANAN GANGGUAN DARURAT KEBAKARAN DATA CENTER APJII

1. Pendahuluan

Kebakaran merupakan salah satu ancaman paling serius terhadap kelangsungan operasional data center karena dapat menyebabkan kerusakan fisik pada infrastruktur IT, gangguan layanan jaringan nasional, dan potensi kehilangan data kritikal.
Data Center APJII yang berlokasi di Gedung Cyber-1 merupakan salah satu hub utama pertukaran internet nasional (IIX), di mana operasionalnya bergantung pada ketersediaan sistem listrik, pendingin, dan konektivitas secara terus-menerus (24x7x365).

Sebagai fasilitas berisiko tinggi, diperlukan prosedur standar yang sistematis dan terkoordinasi untuk menangani situasi darurat akibat kebakaran agar dampak terhadap keselamatan personel, peralatan, dan layanan dapat diminimalkan.

SOP ini menetapkan langkah-langkah preventif, deteksi dini, komunikasi darurat, evakuasi, dan pemulihan pasca insiden kebakaran di lingkungan Data Center APJII yang berlokasi di Gedung Cyber-1.

2. Tujuan

Tujuan dari SOP ini adalah untuk:

1. Menetapkan tata cara penanganan keadaan darurat akibat kebakaran di lingkungan Data Center APJII atau tenant di Gedung Cyber-1.
2. Menjamin keselamatan seluruh personel, pengunjung, dan aset perusahaan selama terjadinya kebakaran.
3. Memastikan seluruh perangkat kritikal (server, UPS, PAC, panel listrik, kabel data, dan fasilitas lainnya) terlindungi secara optimal.
4. Menstandarkan mekanisme komunikasi dan koordinasi antara tim internal APJII, pengelola Gedung Cyber-1, serta pihak eksternal (Pemadam Kebakaran, PLN, dan Kepolisian).
5. Memastikan pemulihan layanan dan infrastruktur dapat dilakukan secara aman dan cepat setelah kondisi dinyatakan terkendali.

3. Dasar dan Referensi Standar

SOP ini disusun dengan mengacu pada peraturan, pedoman, dan standar nasional maupun internasional berikut:

3.1 Regulasi Nasional

- Undang-Undang No. 1 Tahun 1970 tentang Keselamatan Kerja
- Undang-Undang No. 24 Tahun 2007 tentang Penanggulangan Bencana
- Peraturan Menteri Tenaga Kerja No. PER.04/MEN/1980 tentang Syarat-syarat Pemasangan dan Pemeliharaan Alat Pemadam Api Ringan (APAR)
- Peraturan Menteri PUPR No. 26/PRT/M/2008 tentang Persyaratan Teknis Sistem Proteksi Kebakaran pada Bangunan Gedung dan Lingkungan
- SNI 03-1745-2000 tentang Tata Cara Perencanaan Proteksi Kebakaran untuk Bangunan Gedung

3.2 Standar dan Best Practice Internasional

- **TIA-942-C**: Telecommunications Infrastructure Standard for Data Centers (Bab Fire Protection & Safety)
- **ISO 22301:2019** – Business Continuity Management Systems (BCMS)
- **ISO 45001:2018** – Occupational Health and Safety Management Systems
- **NFPA 75** – Standard for the Fire Protection of Information Technology Equipment
- **NFPA 76** – Standard for the Fire Protection of Telecommunications Facilities
- **NFPA 101** – Life Safety Code
- **ASHRAE TC 9.9** – Mission Critical Facilities, Data Centers, Technology Spaces, and Electronic Equipment

4. Definisi Istilah

Istilah	Definisi
Data Center	Fasilitas yang digunakan untuk menempatkan sistem komputer dan komponen terkait seperti sistem telekomunikasi dan penyimpanan data dengan tingkat ketersediaan tinggi.
Gangguan Darurat (Emergency Incident)	Kondisi tidak normal yang mengancam keselamatan personel, merusak fasilitas, atau mengganggu operasional layanan secara signifikan.
Kebakaran (Fire Incident)	Suatu kejadian di mana terjadi pembakaran yang tidak terkendali pada area tertentu yang dapat menimbulkan bahaya bagi manusia, peralatan, dan lingkungan.
APAR (Alat Pemadam Api Ringan)	Peralatan yang digunakan untuk memadamkan api pada tahap awal kebakaran.

Istilah	Definisi
HSSD / VESDA	High-Sensitivity Smoke Detection System / Very Early Smoke Detection Apparatus — sistem deteksi asap dini dengan sensitivitas tinggi.
Novec 1230 / FM-200	Tabung gas pemadam kebakaran non-konduktif yang digunakan untuk melindungi peralatan elektronik tanpa merusak perangkat IT.
Fire Alarm Panel (FAP)	Sistem utama pengendali alarm kebakaran yang menerima sinyal dari sensor deteksi dan mengaktifkan alarm serta notifikasi.
EPO (Emergency Power Off)	Tombol darurat untuk memutus suplai listrik utama guna mencegah eskalasi kebakaran akibat arus listrik.
Evakuasi	Proses pemindahan orang secara aman dari area berisiko menuju titik kumpul (assembly point) yang telah ditetapkan.
Tim Tanggap Darurat (TTD)	Tim terlatih yang bertugas menangani situasi darurat kebakaran dan melakukan koordinasi dengan pihak eksternal.

5. Ruang Lingkup

5.1 Cakupan Fasilitas

SOP ini berlaku untuk seluruh area operasional Data Center APJII di Gedung Cyber-1.

5.2 Jenis Kegiatan

SOP ini mencakup kegiatan berikut:

1. **Pencegahan Kebakaran**
    - Pemeriksaan rutin sistem deteksi dan pemadam otomatis (HSSD/VESDA, Fire Alarm, Novec 1230, APAR).
    - Pemeliharaan sistem listrik dan HVAC agar tidak menjadi sumber potensi kebakaran.
    - Pelatihan dan simulasi kebakaran minimal 1 kali per tahun.
2. **Tindakan Saat Kebakaran Terjadi**
    - Identifikasi sumber kebakaran berdasarkan alarm atau visual.
    - Aktivasi sistem alarm dan pemadaman otomatis.
    - Evakuasi seluruh personel menuju assembly point.
    - Komunikasi cepat ke Security, Tim Tanggap Darurat, dan pengelola Gedung Cyber-1.
    - Pelaporan ke Pemadam Kebakaran dan otoritas terkait.
3. **Penanganan Pasca Kebakaran**
    - Isolasi area terdampak untuk investigasi dan pemulihan.
    - Pemeriksaan ulang sistem listrik dan pendingin sebelum reaktifasi.
    - Analisis akar penyebab (Root Cause Analysis).

- Penyusunan laporan insiden resmi (Incident Report) dan rencana perbaikan (Corrective Action Plan).

4. **Koordinasi dan Komunikasi**
   - Mekanisme komunikasi internal antar-tim APJII dan dengan pengelola Gedung Cyber-1.
   - Prosedur pemberitahuan kepada penyewa, anggota APJII, dan otoritas publik jika diperlukan.

6. Struktur Tanggung Jawab

Jabatan / Tim	Tanggung Jawab Utama
Incident Commander (IC) – *PIC / Penangggung Jawab Operasional DC APJII*	Memimpin dan mengoordinasikan seluruh tindakan darurat, mengambil keputusan strategis termasuk aktivasi evakuasi total.
Fire Warden / Koordinator Keamanan Gedung	Memantau sistem alarm kebakaran gedung, menghubungi pemadam kebakaran dan pihak pengelola Cyber-1.
Tim Tanggap Darurat (TTD)	Melakukan penilaian awal, memadamkan api dengan APAR jika aman, memastikan aktivasi sistem pemadam otomatis (Novec 1230/FM-200).
Tim Evakuasi	Membimbing seluruh personel keluar menuju titik kumpul aman (assembly point).
Tim Teknis APJII	Mematikan daya listrik non-kritikal melalui EPO jika diperlukan, memastikan sistem UPS, genset, dan pendingin aman dari eskalasi.
Tim NOC APJII	Melakukan shutdown aman terhadap server kritikal sesuai instruksi IC, dan menjaga integritas data.
Tim Dokumentasi & Komunikasi	Mencatat kronologi insiden, waktu kejadian, tindakan yang dilakukan, dan berkoordinasi dengan pihak eksternal.
Tim Pemulihan (Recovery Team)	Melakukan asesmen pasca insiden, analisis akar penyebab, dan pemulihan layanan operasional.

7. Prosedur Penanganan per Fase

7.1. Fase Deteksi Awal (0–2 menit)

Tujuan: Mengidentifikasi secara dini adanya indikasi kebakaran dan mengaktifkan sistem peringatan.

Langkah-langkah:

1. Sistem **HSSD/VESDA** atau **detektor asap panas** memberikan sinyal ke **Fire Alarm Panel (FAP)**.
2. Alarm visual dan audio aktif di seluruh area terkait.
3. **Security / Operator NOC** segera memverifikasi lokasi asal alarm melalui panel FAP atau kamera CCTV.
4. Jika ditemukan asap/percikan api kecil:
    - Tim TTD segera membawa **APAR** Kelas C untuk pemadaman awal.
    - Catat waktu pertama kali alarm aktif.
5. **Jika asap terus meningkat atau api tidak terkendali dalam 1 menit**, segera lanjut ke Fase Respon Darurat.

Komunikasi:

- Tim NOC APJII → Incident Commander: “Alarm kebakaran aktif di ruang server Hall-1 pukul 09:35am WIB, asap terdeteksi di area Rak 5B.”
- IC → Security: “Aktifkan protokol darurat kebakaran, siapkan tim evakuasi dan hubungi pengelola Gedung Cyber-1.”

7.2. Fase Respon Darurat (2–5 menit)

Tujuan: Menahan eskalasi api dan meminimalkan risiko terhadap manusia dan aset.

Langkah-langkah:

1. **Tim TTD** segera menuju lokasi dengan APAR dan memastikan area aman dari bahaya listrik.
2. **Tim Teknis APJII** siaga untuk memutus suplai listrik **non-kritikal** jika diminta IC.
3. Jika api tidak dapat dikendalikan dalam **2 menit**, sistem **Novec 1230/FM-200** akan aktif otomatis.
4. **Semua personel wajib segera meninggalkan ruang server sebelum sistem gas aktif.**
5. **IC** memastikan bahwa Fire Alarm utama sudah mengirim sinyal ke:
    - **Security Gedung Cyber-1**
    - **Pemadam Kebakaran (Dinas Damkar Jakarta Selatan)**
    - **Manajemen APJII / Pengelola Lantai**
6. Pintu ruang data center dikunci untuk menjaga tekanan gas tetap efektif.

Komunikasi Eksternal:

- Fire Warden → Gedung Cyber-1: “Telah terjadi kebakaran di ruang DC APJII Lantai X, sistem Novec aktif otomatis, mohon dukungan Damkar.”
- Gedung Cyber-1 → Damkar: “Alarm kebakaran aktif di tenant APJII, Gedung Cyber-1, Jl. Kuningan Barat 8, mohon segera ditangani.”

7.3. Fase Evakuasi (5–10 menit)

Tujuan: Memastikan semua personel meninggalkan area berbahaya secara aman.

Langkah-langkah:

1. **Tim Evakuasi** membimbing seluruh personel menuju **tangga darurat** dan **titik kumpul (assembly point)** di area luar Gedung Cyber-1.
2. **Security** memastikan tidak ada orang tertinggal di toilet, ruang UPS, atau ruang NOC.
3. **IC** melakukan absensi di assembly point.
4. Pastikan **tidak ada yang kembali ke dalam gedung** tanpa izin resmi dari pihak berwenang.
5. **Petugas medis / P3K** siaga jika ada korban luka ringan akibat asap atau kepanikan.

Target Waktu Evakuasi Total:
Maksimum **5–7 menit** sejak alarm kebakaran aktif.

7.4. Fase Pemulihan dan Investigasi (10 menit – 48 jam)

Tujuan: Memastikan area aman, menilai kerusakan, dan memulihkan operasi secara terkendali.

Langkah-langkah:

1. Setelah api padam, **Tim Pemadam Kebakaran** dan **Pengelola Gedung Cyber-1** memberikan *clearance* area.
2. **Tim Teknis APJII** melakukan pemeriksaan ulang terhadap sistem listrik, UPS, PAC, dan integritas grounding.
3. **Tim NOC APJII** melakukan pengecekan visual peralatan server, patch panel, dan jaringan optik.
4. **Incident Commander** mengisi dan menandatangani **Laporan Insiden Kebakaran (Fire Incident Report)**.
5. **Analisis Akar Penyebab (Root Cause Analysis – RCA)** dilakukan dalam waktu maksimal **24 jam** setelah kejadian.
6. **Rencana Pemulihan Layanan (Service Restoration Plan)** disusun dan dieksekusi setelah area dinyatakan aman.
7. **Rapat Evaluasi Internal** dilaksanakan untuk pembelajaran (*lesson learned*).

8. Checklist Tanggap Darurat Kebakaran

No	Aktivitas	Dilakukan oleh	Status (✓/✗)
1	Alarm kebakaran terdeteksi dan diverifikasi	Tim NOC	
2	Lokasi kebakaran diidentifikasi	Tim TTD	
3	APAR digunakan jika aman	Tim TTD	
4	Pemberitahuan ke IC dan Gedung Cyber-1	Security	

No	Aktivitas	Dilakukan oleh	Status (✓/✗)
5	Aktivasi sistem pemadam otomatis (Novec 1230)	Otomatis / Tim Teknis	
6	EPO (Emergency Power Off) dilakukan jika perlu	Tim Teknis	
7	Evakuasi seluruh personel ke assembly point	Tim Evakuasi	
8	Absensi personel dilakukan di assembly point	IC / HR	
9	Area dinyatakan aman oleh Damkar	Fire Warden	
10	Pemeriksaan ulang sistem M&E dan IT	Tim Teknis & NOC	
11	Penyusunan laporan dan RCA	IC / Dokumentasi	

9. Contoh Formulir Laporan Insiden Kebakaran

Form: FIRE INCIDENT REPORT
Data Center APJII – Gedung Cyber-1

Informasi Umum	Keterangan
Tanggal / Waktu Kejadian	……
Lokasi Area Terbakar	……
Ditemukan oleh	……
Jenis Alarm yang Aktif	HSSD / Smoke / Heat / Manual
Sumber Dugaan Api	( ) Listrik ( ) Pendingin ( ) Lainnya
Sistem Pemadam Aktif	( ) Novec 1230 ( ) APAR ( ) Manual
Waktu Pemadaman Selesai	……

Dampak & Tindakan	Keterangan
Personel Terluka	( ) Ya ( ) Tidak
Jumlah Korban	……
Kerusakan Peralatan	( ) Ringan ( ) Sedang ( ) Berat
Layanan yang Terdampak	……

Dampak & Tindakan	Keterangan
Tindakan Sementara	……
Tim yang Terlibat	……
Persetujuan & Tanda Tangan	
Incident Commander	……
Tim M&E	……
Tim IT Operations	……
Fire Warden Gedung Cyber-1	……
Tanggal Pelaporan	……

10. Peninjauan dan Pemutakhiran SOP

SOP ini wajib ditinjau dan diuji melalui **simulasi darurat (fire drill)** minimal **1 kali per tahun**, serta diperbarui bila terdapat:

- Perubahan layout ruang / sistem pemadam.
- Hasil audit internal atau eksternal.
- Pembelajaran dari insiden aktual.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENANGANAN GANGGUAN DARURAT KEGAGALAN DAYA PLN DAN SISTEM CADANGAN (BACKUP SYSTEM) DATA CENTER APJII

1. Pendahuluan

Ketersediaan daya listrik yang stabil merupakan faktor kritikal dalam menjamin kelangsungan operasional Data Center APJII yang melayani anggota ISP di seluruh Indonesia. Gangguan pada pasokan daya utama dari PLN berpotensi menyebabkan downtime, kerusakan peralatan IT, serta gangguan layanan bagi pelanggan.

Untuk itu, Data Center APJII telah dilengkapi dengan sistem cadangan daya (backup system) berupa **Uninterruptible Power Supply (UPS)**, **Battery Bank**, **Automatic Transfer Switch (ATS)**, dan **Genset (Diesel Generator Set)** yang beroperasi secara otomatis dan berlapis untuk menjaga kontinuitas suplai listrik.

SOP ini disusun untuk memberikan panduan terperinci mengenai langkah-langkah penanganan darurat saat terjadi **kegagalan daya PLN**, termasuk prosedur pemindahan beban ke sistem cadangan dan pemulihan kembali ke kondisi normal setelah pasokan PLN pulih.

2. Tujuan

Tujuan dari SOP ini adalah untuk:

1. Menjamin keberlangsungan layanan Data Center APJII saat terjadi gangguan daya dari PLN.
2. Memastikan semua personel operasional memahami dan melaksanakan langkah penanganan darurat dengan aman dan efisien.
3. Meminimalkan risiko downtime, kehilangan data, dan kerusakan peralatan akibat transisi daya.
4. Menetapkan mekanisme komunikasi, koordinasi, dan pelaporan selama dan setelah kejadian gangguan daya.
5. Memastikan pemulihan daya berjalan sesuai dengan prosedur yang aman, terkendali, dan terdokumentasi.

3. Dasar dan Referensi Standar

SOP ini mengacu pada standar dan panduan internasional serta regulasi nasional berikut:

No	Referensi Standar / Dokumen	Deskripsi
1	**TIA-942-C**	Telecommunications Infrastructure Standard for Data Centers – Bab Power & Redundancy
2	**ISO 22301:2019**	Business Continuity Management System (BCMS)
3	**ISO/IEC 27001:2022**	Information Security Management System – A.11.2 (Power & Environmental Controls)
4	**DCOS (Data Centre Operations Standard)**	Bab 6.2 – Emergency Power and Failover Procedures
5	**Permen ESDM No. 12 Tahun 2021**	Ketentuan Pemanfaatan Tenaga Listrik dan Pengoperasian Genset
6	**SOP Operasional Sistem Kelistrikan DC APJII**	Dokumen internal pendukung teknis
7	**Manual Book UPS dan Genset APJII**	Spesifikasi teknis sistem cadangan daya

4. Definisi Istilah

Istilah	Definisi
PLN (Perusahaan Listrik Negara)	Penyedia utama tenaga listrik nasional.
UPS (Uninterruptible Power Supply)	Sistem penyimpan daya sementara yang menjaga beban IT tetap hidup selama perpindahan sumber daya ke genset.
Battery Bank	Kumpulan baterai yang menjadi sumber energi sementara bagi UPS.
ATS (Automatic Transfer Switch)	Panel otomatis yang memindahkan suplai daya dari PLN ke Genset atau sebaliknya.
Genset (Generator Set)	Mesin pembangkit listrik darurat berbahan bakar diesel untuk menyuplai daya cadangan.
Load Bank	Perangkat untuk pengujian performa genset dengan simulasi beban listrik.

Istilah	Definisi
Failover	Proses otomatis pemindahan sumber daya dari sistem utama ke sistem cadangan saat terjadi gangguan.
Recovery (Failback)	Proses pengembalian suplai daya dari sistem cadangan ke sumber utama (PLN).
Alarm BMS (Building Management System)	Sistem monitoring yang memberikan peringatan dini terhadap status kelistrikan.
MCR (Main Control Room)	Ruang pusat kendali operasional Data Center.

5. Ruang Lingkup

SOP ini berlaku untuk seluruh area Data Center APJII, meliputi:

- **Area Daya dan Infrastruktur:**
  - Panel LVMDP, SDP, UPS, Battery Room, ATS, dan Genset Area.
- **Area IT Load:**
  - Server Hall, Network Room, NOC, dan sistem pendukung (PAC, fire suppression, access control).
- **Personel yang Terlibat:**
  - Duty Engineer / Power Technician
  - NOC (Network Operations Center) Officer
  - Facility Manager
  - Security Team
  - External Vendor (Genset & UPS Maintenance)
  - Building Management / PLN Contact Point

6. Prosedur Penanganan Darurat

6.1 Kondisi Normal (Standby Mode)

- Pasokan daya berasal dari PLN utama.
- UPS berada dalam kondisi online mode, menstabilkan dan menyaring daya ke beban kritikal.
- Genset dalam posisi **standby**, ATS pada posisi **PLN mode**.
- Sistem BMS aktif melakukan monitoring parameter tegangan, frekuensi, dan arus.

6.2 Kegagalan Daya PLN (Power Failure Event)

Deteksi Awal:

1. BMS menampilkan alarm **“Loss of PLN Input”**.
2. UPS beralih ke **battery mode**, menyuplai daya tanpa gangguan ke beban IT.
3. Duty Engineer segera mengonfirmasi di panel LVMDP dan mencatat waktu kejadian (T0).

Tindakan Otomatis:

1. ATS mendeteksi kehilangan daya dan mengirim sinyal auto-start ke Genset.
2. Genset mulai hidup dalam waktu **≤15 detik** dan mencapai tegangan stabil.
3. ATS berpindah otomatis ke **Genset mode** dan menyuplai daya ke UPS input.
4. UPS kembali ke mode normal (on-line with Genset).

Tindakan Manual:

- Duty Engineer memverifikasi kestabilan frekuensi dan tegangan output genset (±5%).
- Catat semua parameter ke **Log Gangguan Daya**.
- Laporan segera disampaikan ke Facility Manager & NOC melalui kanal darurat.

6.3 Pemantauan Saat Operasi Genset

1. Pastikan suhu, tekanan oli, level bahan bakar, dan indikator alarm genset normal.
2. Pastikan beban tidak melebihi 80% kapasitas genset.
3. Lakukan komunikasi rutin setiap 30 menit ke NOC dan manajemen fasilitas.
4. Apabila durasi pemadaman PLN melebihi **4 jam**, lakukan pengisian bahan bakar tambahan sesuai SOP pengisian bahan bakar darurat.

6.4 Pemulihan Daya dari PLN (Power Recovery)

Langkah-langkah:

1. Setelah PLN kembali normal, ATS mendeteksi kestabilan daya minimal **5 menit** tanpa fluktuasi.
2. Duty Engineer memverifikasi kondisi tegangan PLN (R-S-T = 380/220V, ±5%).
3. ATS berpindah otomatis dari **Genset Mode** ke **PLN Mode**.
4. UPS beralih kembali ke **on-line mode dengan PLN input**.
5. Genset menjalani **cooling down** selama 5 menit sebelum otomatis berhenti.
6. Catat waktu pemulihan dan lakukan pemeriksaan visual pasca-transisi.

6.5 Pasca-Kejadian (Post Incident Activities)

1. Duty Engineer menyusun **Incident Report Form (IRF)** maksimal 2 jam setelah kejadian.
2. Facility Manager melakukan **Root Cause Analysis (RCA)** jika ada anomali dalam proses failover.
3. Semua data dicatat dalam **Power Failure Logbook** dan diunggah ke sistem dokumentasi elektronik.
4. Lakukan **simulasi ulang** (dry-run test) dalam waktu 1 minggu jika terjadi kegagalan sistem otomatis.
5. Evaluasi prosedur ini setiap 6 bulan atau setelah insiden besar.

7. Dokumentasi dan Rekaman

- Log Book Gangguan Listrik (PLN Fail Log)
- Power Alarm Report dari BMS
- Form Insiden & Tindakan Korektif

- Checklist Harian UPS & Genset
- Bukti komunikasi dengan PLN/Vendor

8. Tanggung Jawab

Jabatan	Tanggung Jawab
Duty Engineer	Melaksanakan langkah darurat sesuai SOP dan mencatat semua kejadian.
Facility Manager	Koordinasi internal & eksternal, verifikasi laporan insiden, dan memastikan pemulihan sistem.
NOC Team	Memantau dampak layanan terhadap jaringan dan melaporkan status ke pelanggan internal.
Security	Menjaga akses area genset dan panel kelistrikan selama insiden berlangsung.
Vendor Maintenance	Memberikan dukungan teknis jika terjadi kegagalan sistem otomatis.

9. Evaluasi dan Revisi SOP

- Evaluasi SOP dilakukan minimal **setiap 12 bulan**.
- Revisi dilakukan jika terdapat perubahan konfigurasi sistem daya, penambahan genset, atau pembaruan regulasi/standar.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XIII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENANGANAN GANGGUAN DARURAT KERUSUHAN SOSIAL DAN TINDAKAN SABOTASE DATA CENTER APJII

1. Pendahuluan

Kerusuhan sosial, demonstrasi, dan tindakan sabotase merupakan ancaman eksternal yang berpotensi mengganggu kelangsungan operasional Data Center APJII. Situasi tersebut dapat berdampak pada keselamatan personel, kerusakan aset fisik, gangguan jaringan komunikasi, atau bahkan menghentikan layanan Internet Exchange (IX) yang dikelola oleh APJII.

Untuk menjamin **keamanan fisik, kesinambungan layanan, dan keselamatan personel**, perlu disusun **SOP Penanganan Gangguan Darurat Kerusuhan Sosial atau Sabotase** ini sebagai bagian dari sistem **Business Continuity Management System (BCMS)** dan **Emergency Response Plan (ERP)** APJII.

Dokumen ini menjadi panduan operasional bagi seluruh personel yang bertugas di Data Center APJII untuk merespons secara cepat, aman, terkoordinasi, dan efektif terhadap ancaman kerusuhan atau sabotase yang terjadi di sekitar maupun di dalam fasilitas data center.

2. Tujuan

Tujuan utama SOP ini adalah untuk:

1. Menjamin **keselamatan seluruh personel dan pengunjung** yang berada di lingkungan Data Center APJII.
2. Melindungi **infrastruktur kritikal** seperti sistem kelistrikan, pendingin (cooling system), sistem keamanan (CCTV, access control), dan perangkat jaringan utama IX.
3. Menetapkan **tata cara penanganan cepat dan sistematis** dalam menghadapi kondisi darurat akibat kerusuhan atau sabotase.
4. Memastikan **komunikasi internal dan eksternal yang terkoordinasi**, termasuk dengan pihak keamanan (TNI/POLRI), manajemen pusat, dan pihak penyewa/anggota APJII.
5. Meminimalkan **downtime operasional** serta mempercepat proses **recovery** menuju kondisi normal.
6. Mematuhi ketentuan dan standar keamanan serta keberlangsungan layanan sebagaimana diatur dalam **ISO 22301**, **ISO 27001**, dan **TIA-942-C**.

3. Dasar dan Referensi Standar

SOP ini disusun berdasarkan dan mengacu pada standar serta regulasi berikut:

1. **ISO 22301:2019** – *Security and resilience — Business continuity management systems — Requirements.*
2. **ISO/IEC 27001:2022** – *Information Security Management Systems (ISMS).*
3. **TIA-942-C:2024** – *Telecommunications Infrastructure Standard for Data Centers*, bagian *Physical Security & Safety.*
4. **Data Centre Operations Standard (DCOS)** – EPI Global Standard, Bab *Crisis Management & Incident Response.*
5. **Undang-Undang No. 11 Tahun 2008** jo. **UU No. 19 Tahun 2016** – *Informasi dan Transaksi Elektronik (ITE).*
6. **Peraturan Pemerintah No. 71 Tahun 2019** – *Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE).*
7. **Pedoman Keamanan dan Keselamatan Gedung Data Center APJII**.
8. **Kebijakan Keamanan Fasilitas (Facility Security Policy)** dan **Kebijakan Kesinambungan Layanan APJII (Business Continuity Policy).**

4. Definisi Istilah

Istilah	Definisi
Kerusuhan Sosial	Peristiwa gangguan keamanan yang melibatkan massa di sekitar lokasi Data Center yang berpotensi mengancam keselamatan personel dan aset fisik.
Tindakan Sabotase	Upaya disengaja oleh pihak internal atau eksternal untuk merusak, mengganggu, atau menghentikan sistem dan infrastruktur data center.
Incident Commander (IC)	Personel senior yang bertanggung jawab mengendalikan situasi darurat dan mengoordinasikan seluruh tim tanggap darurat.
ERT (Emergency Response Team)	Tim yang ditunjuk untuk melakukan penanganan langsung terhadap situasi darurat termasuk evakuasi, pengamanan, dan pelaporan.
BCR (Business Continuity Representative)	Penanggung jawab penerapan rencana kesinambungan bisnis dan pemulihan layanan.
Command Post (Posko Komando)	Lokasi yang ditetapkan sebagai pusat koordinasi selama keadaan darurat.
Evakuasi Aman	Proses pemindahan personel dari area berisiko menuju titik kumpul aman yang telah ditentukan.

Istilah	Definisi
Lockdown Mode	Prosedur pengamanan di mana seluruh akses ke dalam gedung Data Center ditutup sementara untuk mencegah ancaman eksternal masuk.
Sabotase Fisik	Aksi merusak fasilitas seperti genset, UPS, kabel daya, pendingin, atau sistem keamanan.
Sabotase Digital	Aksi meretas atau mengganggu sistem kontrol (BMS, DCIM, SCADA, atau sistem jaringan).

5. Ruang Lingkup

SOP ini mencakup seluruh kegiatan yang berkaitan dengan penanganan kondisi darurat **akibat kerusuhan sosial atau tindakan sabotase**, baik **di dalam** maupun **di sekitar area Data Center APJII**, meliputi:

5.1. Cakupan Fasilitas

- Seluruh area operasional Data Center APJII yang berlokasi di Gedung Cyber-1.

5.2. Jenis Gangguan yang Dicakup

1. **Kerusuhan sosial di luar kompleks** yang berpotensi meluas ke area Data Center.
2. **Kerusuhan atau perusakan fasilitas** oleh massa di dalam atau sekitar lokasi.
3. **Aksi sabotase internal** (oleh pegawai/kontraktor/visitor) terhadap infrastruktur.
4. **Aksi sabotase eksternal** melalui akses fisik atau digital.
5. **Ancaman bom atau bahan peledak.**
6. **Pemblokiran akses jalan** menuju/keluar dari lokasi DC oleh massa.

5.3. Tahapan Penanganan

Ruang lingkup penanganan mencakup seluruh siklus tanggap darurat:

- Peringatan dini (Early Warning)
- Aktivasi rencana darurat
- Koordinasi dengan pihak berwenang
- Evakuasi dan lockdown
- Komunikasi dan pelaporan ke manajemen
- Pemulihan dan normalisasi operasional
- Evaluasi pasca-insiden (Post-Incident Review)

Peringatan Dini (Early Warning Stage)

Tujuan:

Mendeteksi secara cepat setiap potensi ancaman kerusuhan sosial atau tindakan sabotase sebelum berkembang menjadi situasi darurat yang mengganggu keamanan personel dan operasional data center.

Indikator Aktivasi:

- Terdapat laporan dari satpam kawasan, aparat, atau warga sekitar mengenai kerumunan massa, demonstrasi, atau ancaman keamanan di radius 1–3 km dari data center.
- Sistem keamanan (CCTV, perimeter sensor, panic alarm) mendeteksi aktivitas mencurigakan di area luar.
- Adanya informasi intelijen, media sosial, atau pemberitahuan resmi dari instansi pemerintah terkait potensi aksi massa.

Langkah Operasional:

1. **Security Supervisor** melakukan verifikasi cepat terhadap informasi melalui kamera perimeter dan personel lapangan.
2. Jika ancaman dinilai **valid atau berpotensi meningkat**, Security melaporkan ke **Incident Commander (IC)** melalui saluran komunikasi darurat.
3. IC mengeluarkan **"Warning Notification"** ke seluruh staf operasional dan menyiapkan **ERT (Emergency Response Team)** untuk siaga tahap awal.
4. Semua staf diminta menahan tamu atau vendor baru hingga ada perintah lebih lanjut.
5. Semua data aktivitas dicatat dalam **Incident Logbook – Stage 1: Early Warning**.

Penanggung Jawab:
Security Supervisor & Incident Commander

Output:

- Laporan peringatan dini (Early Warning Report)
- Aktivasi status "Siaga Darurat Level 1"

2. Aktivasi Rencana Darurat (Emergency Activation Stage)

Tujuan:

Menetapkan status darurat secara resmi dan mengaktifkan protokol tanggap darurat yang melibatkan seluruh tim operasional, keamanan, dan komunikasi APJII.

Indikator Aktivasi:

- Situasi eksternal memburuk (massa bergerak mendekati area gedung, aksi perusakan, pemblokiran akses jalan).
- Terdapat indikasi sabotase fisik atau digital terhadap sistem infrastruktur.
- Arahan dari manajemen atau otoritas keamanan untuk melakukan pengamanan penuh.

Langkah Operasional:

1. IC menetapkan **Status "Emergency Condition – Civil Unrest / Sabotage"**.
2. **Command Post** (posko komando) dibentuk di ruang NOC atau area aman di dalam DC.
3. **ERT** dan **Security** menempati posisi siaga di area penting (perimeter, genset, ruang daya).
4. Pengaktifan **Emergency Notification System (ENS)** untuk memberi tahu seluruh staf dan tenant.
5. Semua aktivitas operasional non-esensial dihentikan sementara.

Penanggung Jawab:

Incident Commander (IC)

Output:

- Status darurat aktif
- Aktivasi Command Post
- Catatan aktivasi dalam *Emergency Activation Log*

Koordinasi dengan Pihak Keamanan (Security Coordination Stage)

Tujuan:

Memastikan sinergi cepat dengan aparat keamanan (Polsek, Koramil, Satpam kawasan) guna mengendalikan situasi dan melindungi fasilitas data center.

Indikator Aktivasi:

- Situasi eksternal telah berdampak langsung pada akses data center atau keselamatan staf.
- Diperlukan pengamanan tambahan atau evakuasi terkoordinasi.

Langkah Operasional:

1. **IC atau Security Supervisor** segera menghubungi Polsek/Koramil setempat dan menyampaikan:
    - Lokasi dan situasi terkini.
    - Jumlah personel di dalam gedung.
    - Permintaan bantuan pengamanan atau pengawalan evakuasi.
2. Informasikan ke **Manajemen APJII Pusat** terkait eskalasi status keamanan.
3. Siapkan area parkir belakang sebagai **temporary access** untuk aparat keamanan.
4. Catat seluruh komunikasi eksternal (nama petugas, waktu, hasil koordinasi) ke *Security Communication Log*.

Penanggung Jawab:

Incident Commander & Security Supervisor

Output:

- Koordinasi resmi dengan aparat keamanan
- Bukti komunikasi dan log dokumentasi

Evakuasi dan Lockdown (Evacuation & Lockdown Stage)

Tujuan:

Melindungi keselamatan personel dengan mengevakuasi ke area aman atau mengamankan fasilitas dengan sistem lockdown untuk mencegah ancaman eksternal masuk.

Indikator Aktivasi:

- Massa telah mencapai perimeter gedung atau terjadi kerusuhan di sekitar lokasi.
- Terdapat ancaman langsung ke keselamatan personel atau infrastruktur.

Langkah Operasional:

A. Lockdown

1. Security menutup seluruh akses keluar/masuk, mengunci pintu utama dan belakang, serta menonaktifkan **visitor entry system**.
2. Access control diatur ke **manual lockdown mode** – hanya IC yang berwenang membuka akses.
3. CCTV perimeter dipantau terus-menerus di Command Post.

B. Evakuasi

1. IC memerintahkan **ERT** untuk memulai evakuasi personel ke **Titik Kumpul Aman (Assembly Point)**.
2. Rute evakuasi alternatif digunakan bila area depan tidak aman.
3. ERT mencatat jumlah personel (headcount) menggunakan *Evacuation Sheet*.
4. IC memastikan tidak ada personel tertinggal melalui pengecekan ulang setiap ruang.

Penanggung Jawab:

Incident Commander & ERT Leader

Output:

- Laporan lockdown aktif
- Headcount personel di titik kumpul
- Form *Evacuation Record* tersimpan

Komunikasi dan Pelaporan ke Manajemen (Communication & Reporting Stage)

Tujuan:

Menjamin adanya komunikasi cepat, akurat, dan terkoordinasi dengan manajemen pusat APJII, pihak tenant, dan otoritas eksternal selama keadaan darurat.

Indikator Aktivasi:

- Status darurat telah aktif atau evakuasi telah dilaksanakan.
- Diperlukan keputusan strategis dari manajemen pusat (misal: aktivasi BCP site).

Langkah Operasional:

1. **ICO** melaporkan status terkini ke **PIC/Penanggung Jawab Operasional Data Center APJII** melalui hotline darurat.
2. **BCR (Business Continuity Representative)** mengirimkan *Situation Report (SitRep)* berkala setiap 30 menit.
3. **Manajemen APJII** menyiapkan *holding statement* untuk komunikasi publik bila situasi mencuat ke media.
4. **Tenant/anggota APJII** dihubungi secara resmi melalui jalur komunikasi yang telah disepakati (email resmi, grup Telegram IX, dll).
5. Semua log komunikasi disimpan dalam *Incident Communication Register*.

Penanggung Jawab:

Incident Commander & Business Continuity Representative

Output:

- Laporan situasi berkala ke manajemen
- Log komunikasi internal & eksternal
- Notifikasi resmi ke tenant

Pemulihan dan Normalisasi Operasional (Recovery & Normalization Stage)

Tujuan:

Memulihkan layanan operasional data center ke kondisi normal secara terkontrol setelah situasi keamanan dinyatakan aman oleh otoritas setempat.

Indikator Aktivasi:

- Kepolisian atau aparat keamanan menyatakan area aman.
- Tidak ada lagi ancaman terhadap keselamatan personel dan fasilitas.
- Infrastruktur fisik dan jaringan siap diuji kembali.

Langkah Operasional:

1. **ICO** memberikan instruksi “Return-to-Operation” secara bertahap.
2. **Tim Teknis** melakukan inspeksi menyeluruh: daya, pendingin, sistem keamanan, BMS, dan jaringan.
3. **NOC** memastikan konektivitas IX berfungsi normal, melakukan monitoring intensif selama 4 jam pertama.
4. Bila ditemukan kerusakan, aktifkan *Corrective Maintenance Procedure*.
5. Semua hasil verifikasi dicatat dalam *Post-Incident Restoration Log*.

Penanggung Jawab:

Facility Manager, BCR, dan NOC Team

Output:

- Formulir *Return-to-Operation Approval*
- Log pemulihan sistem
- Validasi kesiapan layanan

Evaluasi Pasca-Insiden (Post-Incident Review Stage)

Tujuan:

Melakukan evaluasi menyeluruh untuk menilai efektivitas tanggap darurat, menemukan akar penyebab, serta menetapkan tindakan korektif dan pencegahan (CAPA) untuk masa depan.

Indikator Aktivasi:

- Situasi darurat telah berakhir dan semua sistem kembali normal.
- Data insiden telah terkumpul lengkap dari seluruh tim terkait.

Langkah Operasional:

1. IC dan BCR menyelenggarakan **Post-Incident Review Meeting** maksimal **24 jam setelah insiden berakhir**.
2. Setiap unit (Security, Facility, NOC, IT, BCR) menyampaikan laporan singkat (chronology, tindakan, kendala, dan rekomendasi).
3. Tim BCR menyusun **Laporan Akhir Insiden (Final Incident Report)** yang mencakup:
    - Kronologi lengkap
    - Dampak dan durasi downtime
    - Respons dan hasil koordinasi
    - Pelajaran yang dipetik (*lessons learned*)
    - Rencana perbaikan (CAPA – Corrective and Preventive Action)
4. Dokumen hasil review menjadi bagian dari **BCMS Record** dan digunakan untuk memperbarui SOP serta rencana latihan simulasi.

Penanggung Jawab:

Incident Commander & Business Continuity Representative

Output:

- *Post-Incident Review Report*
- *Corrective and Preventive Action Plan*
- *Updated SOP & Training Plan*

5.4. Pihak yang Terlibat

- **Incident Commander (IC)** – Kepala Operasional Data Center.
- **Security Supervisor** – Pengendali lapangan keamanan.
- **ERT (Emergency Response Team)** – Melaksanakan tindakan cepat dan evakuasi.
- **BCR (Business Continuity Representative)** – Mengaktifkan prosedur pemulihan layanan.
- **NOC/APJII Operation Center** – Menjaga kestabilan layanan IIX/IX.
- **Facility Management** – Melindungi aset infrastruktur fisik.
- **Pihak eksternal:** Kepolisian, TNI, Pemadam Kebakaran, dan BPBD setempat.

6. Prosedur Penanganan Gangguan (Langkah Demi Langkah)

Tahap	Langkah-Langkah Operasional	Penanggung Jawab	Waktu Respons Maksimal
Deteksi Awal / Early Warning	- Menerima laporan dari petugas keamanan, CCTV, atau pihak eksternal mengenai potensi kerusuhan atau kerumunan massa di sekitar DC. - Security segera melakukan verifikasi visual melalui kamera perimeter dan pos jaga. - Catat waktu dan sumber laporan di *Incident Logbook*. - Laporan segera disampaikan ke Incident Commander (IC).	Security Supervisor	≤ 5 menit
Aktivasi Prosedur Darurat	- IC menilai tingkat ancaman (minor / moderate / severe). - Jika ancaman signifikan, IC mengaktifkan status “**Emergency Condition – Civil Unrest/Sabotage**”. - Alarm internal atau pesan broadcast dikirim melalui radio komunikasi / BMS notification.	Incident Commander	≤ 10 menit

Tahap	Langkah-Langkah Operasional	Penanggung Jawab	Waktu Respons Maksimal
	- ERT dan BCR segera siaga di Command Post.		
Lockdown dan Pengamanan Akses	- Tutup semua akses keluar/masuk gedung dengan sistem **lockdown mode** (Access Control disabled, manual override via Security). - Pastikan pintu server room dan ruang kritikal dikunci ganda. - Non-personnel (visitor, vendor) diarahkan ke ruang aman. - Security menempatkan petugas di titik strategis tanpa konfrontasi fisik.	Security Team	≤ 10 menit
Koordinasi dengan Pihak Eksternal	- IC segera menghubungi Kepolisian (Polsek/Polres setempat), Satpam kawasan, dan manajemen gedung (jika multi-tenant). - Laporkan kondisi terkini, jumlah personel di lokasi, serta kebutuhan bantuan keamanan. - Pastikan komunikasi tercatat dalam *Incident Logbook*.	Incident Commander	≤ 15 menit
Evakuasi Aman (jika diperlukan)	- Jika kerusuhan menjalar ke area DC atau terdapat ancaman langsung, lakukan evakuasi menuju **Titik Kumpul Aman (Assembly Point)** yang telah ditetapkan. - Gunakan rute evakuasi alternatif yang tidak menghadap jalan utama. - ERT memandu personel dan memastikan headcount di titik kumpul.	ERT Leader	≤ 20 menit
Penanganan Sabotase (Fisik/Digital)	- Jika terdapat indikasi sabotase fisik (perusakan genset, UPS, kabel, CCTV), segera hentikan aktivitas area terdampak dan amankan barang bukti. - Jika terdapat indikasi serangan digital (BMS/DCIM/Network intrusion), aktifkan *Cybersecurity Incident SOP* paralel. - Koordinasi dengan tim IT Security dan Network Operation Center (NOC).	Tim Teknis/NOC APJII	Segera

Tahap	Langkah-Langkah Operasional	Penanggung Jawab	Waktu Respons Maksimal
Komunikasi Internal & Eksternal	- IC memberikan laporan kondisi ke **Manajemen APJII Nasional** melalui kanal resmi (email, grup darurat, hotline). - Manajemen menyiapkan *press holding statement* jika ada potensi media coverage. - Komunikasi dengan tenant/anggota APJII dilakukan oleh BCR sesuai *Communication Tree*.	IC & BCR	≤ 30 menit
Pemulihan dan Normalisasi	- Setelah situasi aman dan dinyatakan kondusif oleh aparat keamanan, IC menginstruksikan pembukaan akses bertahap. - Lakukan inspeksi kondisi fisik, fungsi sistem listrik, pendingin, jaringan, dan keamanan. - Dokumentasikan seluruh temuan, kerusakan, dan langkah pemulihan.	PIC/Penanggung Jawab Operasional DC APJII	≤ 2 jam setelah aman
Evaluasi dan Pelaporan Akhir	- Setelah operasi normal kembali, IC dan BCR mengadakan *Post-Incident Review Meeting* maksimal 24 jam setelah kejadian. - Menyusun **Laporan Insiden Resmi (Incident Report)** lengkap dengan kronologi, dampak, dan rekomendasi perbaikan. - Simpan dokumen sebagai bukti audit ISO 22301/DCOS.	IC & BCR	≤ 24 jam

7. Tanggung Jawab dan Koordinasi Tim

Peran / Jabatan	Tanggung Jawab Utama
Incident Commander (IC)	- Mengambil keputusan aktivasi status darurat. - Mengkoordinasikan semua tim selama kejadian. - Menjadi penghubung utama dengan manajemen APJII dan pihak eksternal.

Peran / Jabatan	Tanggung Jawab Utama
Security Supervisor	- Memantau situasi keamanan. - Melakukan lockdown dan mengamankan perimeter. - Memberikan laporan situasi real-time ke IC.
Emergency Response Team (ERT)	- Melaksanakan evakuasi, penyelamatan, dan bantuan darurat. - Mengatur headcount dan memastikan tidak ada korban. - Melakukan first aid jika diperlukan.
Tim Teknis	- Memastikan perlindungan dan kelangsungan sistem listrik, cooling, dan infrastruktur utama. - Menonaktifkan sistem yang berisiko meledak atau terbakar (panel-panel listrik).
NOC / IT Operations	- Memastikan jaringan tetap aktif atau dialihkan ke sistem redundan (failover site). - Memonitor IX traffic dan sistem kontrol jaringan.
Business Continuity Representative (BCR)	- Mengaktifkan *Business Continuity Plan (BCP)* bila diperlukan. - Menangani komunikasi dengan tenant/anggota. - Mengkoordinasikan proses pemulihan dan dokumentasi pasca-insiden.
Manajemen APJII Pusat	- Memberikan dukungan kebijakan dan sumber daya. - Melakukan komunikasi publik dan koordinasi tingkat nasional.

8. Prosedur Komunikasi dan Eskalasi

8.1. Jalur Eskalasi Internal

Tingkat Insiden	Kriteria	Eskalasi ke	Mode Komunikasi
Level 1 – Minor	Massa di sekitar area, belum berdampak ke DC	Security → IC	Radio / Telepon
Level 2 – Moderate	Potensi masuk ke area DC, gangguan layanan ringan	IC → Facility Manager / BCR	Radio + WhatsApp Group Darurat
Level 3 – Severe	Kerusuhan/sabotase langsung mempengaruhi operasional	IC → Ketum & Dewas	Hotline + Email + Rapat Virtual

8.2. Jalur Komunikasi Eksternal

- **Polsek/Polres setempat** – Koordinasi keamanan lapangan.
- **TNI Koramil** – Bantuan pengamanan perimeter.
- **BPBD / Pemadam** – Jika terdapat potensi kebakaran.
- **Vendor Maintenance** – Untuk inspeksi pasca-kerusakan.
- **Media** – Hanya melalui pernyataan resmi dari Humas APJII.

9. Rencana Evakuasi dan Lockdown

Kegiatan	Langkah Detail	Tanggung Jawab
Evakuasi Aman	- Aktifkan alarm evakuasi. - Pemandu evakuasi (ERT) memimpin jalur keluar. - Hindari area depan gedung jika massa berkumpul. - Kumpulkan seluruh personel di **Assembly Point 1 (belakang gedung)** atau **Assembly Point 2 (lokasi alternatif)**. - Lakukan headcount.	ERT Leader
Lockdown Mode	- Tutup seluruh akses pintu luar menggunakan access control system dan kunci manual. - Matikan sistem visitor entry. - Pantau seluruh CCTV perimeter. - Laporkan situasi ke IC setiap 10 menit.	Security Supervisor
Evakuasi Aset Kritis (jika diperlukan)	- Backup data segera dilakukan melalui DRC (Disaster Recovery Center). - Lepaskan perangkat portable penting (tape backup, media) dan simpan di ruang aman tahan api.	NOC / IT Ops

10. Langkah Pemulihan Pasca-Insiden (Recovery Plan)

Fase	Aktivitas Pemulihan	Penanggung Jawab	Output yang Dihasilkan
Assessment Awal	- Pemeriksaan fisik area dan sistem. - Identifikasi kerusakan infrastruktur. - Penilaian risiko lanjutan.	Facility Engineer	*Damage Assessment Report*
Pemulihan Layanan	- Reaktifasi sistem pendingin, daya, dan jaringan secara bertahap. - Monitoring kestabilan sistem selama 4 jam pertama. - Validasi dengan checklist BCP.	BCR & NOC	*Service Restoration Log*

Fase	Aktivitas Pemulihan	Penanggung Jawab	Output yang Dihasilkan
Validasi Keamanan	- Pemeriksaan ulang akses kontrol, CCTV, alarm. - Reset semua kredensial akses jika dicurigai bocor.	Security & IT Security	*Post-Security Validation Report*
Re-entry Approval	- IC menandatangani *Return-to-Operation Approval Form* setelah area dinyatakan aman.	IC & Manajemen APJII	*Re-entry Authorization*
Review dan Pembelajaran	- Evaluasi respon, kendala, dan area perbaikan. - Update SOP jika diperlukan. - Lakukan pelatihan ulang personel.	IC & BCR	*Post-Incident Review Report*

11. Dokumentasi, Pelaporan, dan Evaluasi

Dokumen	Isi Pokok	Penanggung Jawab	Retensi Arsip
Incident Logbook	Catatan waktu, kronologi, dan tindakan lapangan.	Security	3 tahun
Incident Report Form	Laporan resmi insiden (kerusuhan/sabotase).	IC / BCR	5 tahun
Damage Assessment Report	Rincian kerusakan fisik dan estimasi perbaikan.	Facility Manager	5 tahun
Post-Incident Review	Analisis penyebab, efektivitas respon, rekomendasi.	BCR & IC	5 tahun
BCP Activation Log	Waktu aktivasi, pihak terlibat, dan hasil pemulihan.	BCR	5 tahun

12. Lampiran

12.1. Denah Titik Kumpul Aman

- **Assembly Point 1:** Gedung Cyber-1, area parkir staf (radius aman ≥ 100 m dari perimeter).
- **Assembly Point 2:** Gedung M-Ten (lokasi alternatif bila area utama tidak aman).

12.2. Daftar Kontak Darurat

Unit / Instansi	Kontak	Nomor Telepon / Hotline
Polsek Setempat	Ka. SPKT	110 / (021) XXXXXXXX
Koramil Setempat	Danramil	(021) XXXXXXXX
BPBD / Pemadam	Posko Darurat	113 / (021) XXXXXXXX
Manajemen APJII Pusat	Direktur Operasional	+62 812-XXXX-XXXX
Facility Manager APJII DC	Bapak [Nama]	+62 813-XXXX-XXXX
NOC / Operation Center	On-duty Engineer	+62 21-XXXX-XXXX
ERT Leader	[Nama]	+62 8XX-XXXX-XXXX

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XIV
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENANGANAN GANGGUAN DARURAT PANDEMI ATAU KEJADIAN KESEHATAN MASSAL DATA CENTER APJII

1. Pendahuluan

Data Center APJII merupakan fasilitas kritikal nasional yang menyediakan layanan interkoneksi internet dan infrastruktur digital yang harus tetap beroperasi secara kontinu 24x7x365. Dalam situasi **pandemi global**, **wabah menular**, atau **kejadian kesehatan massal** lainnya (seperti paparan bahan kimia biologis atau epidemi lokal), keberlangsungan operasional dan keselamatan personel menjadi sangat terganggu.

SOP ini disusun untuk memastikan bahwa Data Center APJII memiliki mekanisme **tanggap darurat** yang terstruktur, terkoordinasi, dan selaras dengan prinsip **business continuity** serta **keselamatan kerja**, sehingga dampak terhadap operasional, personel, dan layanan terhadap anggota maupun pelanggan dapat diminimalisasi.

2. Tujuan

Tujuan utama dari SOP ini adalah untuk:

1. Menetapkan **prosedur standar tanggap darurat** terhadap pandemi atau kejadian kesehatan massal di lingkungan Data Center APJII.
2. Memastikan **keselamatan dan kesehatan seluruh personel**, termasuk staf operasional, penyewa (tenant), kontraktor, dan tamu yang berada di dalam area fasilitas.
3. Menjamin **kelangsungan layanan kritikal** Data Center melalui penerapan langkah-langkah pencegahan, mitigasi, dan pengendalian risiko.
4. Mengatur **koordinasi antar tim** (Operation, Security, Engineering, IT Support, dan Management) dalam menghadapi kondisi kesehatan darurat.
5. Menyediakan **mekanisme komunikasi internal dan eksternal** selama masa pandemi atau wabah, agar keputusan dapat diambil cepat, akurat, dan terverifikasi.
6. Menjamin **pemenuhan regulasi nasional dan standar internasional** yang relevan dengan keselamatan kerja, keamanan informasi, dan keberlangsungan bisnis.

3. Dasar dan Referensi Standar

SOP ini mengacu dan disusun berdasarkan standar dan regulasi berikut:

3.1. Standar Internasional

- **ISO 22301:2019** – *Business Continuity Management Systems (BCMS)*
- **ISO 45001:2018** – *Occupational Health and Safety Management Systems*
- **ISO/IEC 27001:2022** – *Information Security Management System (ISMS)*
- **TIA-942-C:2024** – *Telecommunications Infrastructure Standard for Data Centers* (clause 6.4 & 6.6 on Environmental & Safety considerations)
- **WHO Guidelines** – *Operational considerations for COVID-19 management and similar pandemics in critical facilities*

3.2. Regulasi Nasional

- **Undang-Undang No. 36 Tahun 2009** tentang Kesehatan
- **Undang-Undang No. 1 Tahun 1970** tentang Keselamatan Kerja
- **Peraturan Menteri Ketenagakerjaan No. 5 Tahun 2018** tentang K3 Lingkungan Kerja
- **Keputusan Menteri Kesehatan RI** tentang Penanggulangan Kejadian Luar Biasa (KLB) Penyakit Menular
- **Surat Edaran Kemenkes & BNPB** terkait Protokol Kesehatan dan Penanggulangan Pandemi

4. Definisi Istilah

Istilah	Definisi
Pandemi	Wabah penyakit menular yang menyebar secara global dan berdampak pada banyak negara serta wilayah.
Kejadian Kesehatan Massal	Situasi darurat di mana sejumlah besar orang mengalami gangguan kesehatan secara bersamaan akibat paparan penyakit, bahan kimia, biologis, atau sebab lingkungan lainnya.
Isolasi	Pemisahan individu yang telah terinfeksi penyakit menular dari orang yang sehat untuk mencegah penyebaran.
Karantina	Pembatasan pergerakan orang yang diduga telah terpapar penyakit menular namun belum menunjukkan gejala.
Screening Kesehatan	Pemeriksaan kondisi kesehatan personel dan tamu untuk mendeteksi gejala awal penyakit menular (misalnya pengukuran suhu tubuh, observasi gejala).
PPE (Personal Protective Equipment)	Peralatan pelindung diri seperti masker, sarung tangan, pelindung wajah, dan hazmat suit yang digunakan untuk melindungi diri dari paparan penyakit atau bahan berbahaya.
Incident Commander (IC)	Personel yang ditunjuk untuk memimpin dan mengkoordinasikan seluruh aktivitas tanggap darurat pada situasi pandemi di Data Center.

Istilah	Definisi
Critical Staff	Karyawan yang memiliki peran penting dan harus tetap bekerja di fasilitas meskipun dalam kondisi darurat (misalnya NOC, Facility Operations, Security).
Remote Work rrangement	Pengaturan kerja jarak jauh yang diterapkan untuk non-critical staff selama masa pandemi.

5. Ruang Lingkup

Ruang lingkup SOP ini mencakup seluruh kegiatan, pihak, dan fasilitas di lingkungan Data Center APJII yang terlibat dalam penanganan pandemi atau kejadian kesehatan massal, meliputi:

5.1. Lingkup Fasilitas

- Seluruh area operasional Data Center APJII yang berlokasi di Gedung Cyber-1.

5.2. Lingkup Personel

- Seluruh staf internal APJII yang bekerja di fasilitas Data Center
- Kontraktor pihak ketiga (maintenance, cleaning, security, vendor sistem pendingin, dan power)
- Pengunjung, auditor, tenant, dan tamu resmi
- Pihak eksternal terkait (tim medis, satgas kesehatan, petugas pemadam, BPBD, atau instansi pemerintah)

5.3. Lingkup Tahapan Kegiatan

Ruang lingkup penanganan mencakup **seluruh siklus tanggap darurat pandemi atau kejadian kesehatan massal**, yaitu:

1. **Peringatan Dini (Early Warning)**
    - Pemantauan status kesehatan global/nasional dari WHO, Kemenkes, dan BNPB.
    - Aktivasi status siaga internal apabila terdapat potensi wabah.
2. **Aktivasi Rencana Darurat (Emergency Activation)**
    - Penetapan *Incident Commander* dan *Emergency Response Team*.
    - Pemberlakuan protokol masuk dan keluar area yang diperketat (health check, sanitizer, physical distancing).
3. **Koordinasi dengan Pihak Keamanan dan Medis**
    - Pengaturan akses keluar-masuk dengan Security dan pelaporan ke instansi terkait.
    - Aktivasi fasilitas isolasi sementara bila ditemukan personel dengan gejala.
4. **Evakuasi dan Lockdown**
    - Mekanisme pembatasan akses area terdampak (zoning red/yellow/green).
    - Penutupan area publik atau ruangan yang terkontaminasi sementara untuk desinfeksi.

5. **Komunikasi dan Pelaporan ke Manajemen**
    - Laporan harian kesehatan personel dan aktivitas mitigasi ke Crisis Management Team (CMT).
    - Komunikasi resmi kepada seluruh tenant dan pelanggan.
6. **Pemulihan dan Normalisasi Operasional**
    - Proses disinfeksi, verifikasi keamanan area, dan *fit-to-work clearance*.
    - Penilaian kesiapan tim operasional untuk kembali bertugas secara normal.
7. **Evaluasi Pasca-Inisiden (Post-Incident Review)**
    - Analisis efektivitas tindakan yang diambil.
    - Revisi terhadap BCP, ERP, dan SOP bila diperlukan.
    - Dokumentasi laporan akhir dan rekomendasi perbaikan.

6. Struktur Organisasi Tanggap Darurat

Untuk memastikan pelaksanaan penanganan pandemi atau kejadian kesehatan massal berjalan efektif dan terkoordinasi, dibentuk **Struktur Organisasi Tanggap Darurat (Emergency Response Organization – ERO)** sebagai berikut:

6.1. Struktur Organisasi

1. **Incident Commander (IC)**
   Bertanggung jawab penuh atas pengambilan keputusan strategis selama masa darurat dan mengoordinasikan seluruh unit kerja.
   Biasanya dijabat oleh **Head of Data Center Operations** atau **Facility Manager**.
2. **Deputy Incident Commander (DIC)**
   Membantu IC dan menggantikan peran IC bila berhalangan.
   Bertanggung jawab terhadap pelaksanaan teknis harian dan koordinasi lapangan.
3. **Crisis Management Team (CMT)**
   Terdiri dari perwakilan manajemen, IT Operations, HR, Security, Engineering, dan HSE Officer.
   Fungsi utama: koordinasi strategis, komunikasi internal/eksternal, dan pengambilan kebijakan.
4. **Health and Safety Team (HST)**
   Dipimpin oleh HSE Officer, bertugas melakukan penilaian risiko kesehatan, penerapan protokol pencegahan, serta penyediaan fasilitas medis dasar dan PPE.
5. **Security and Access Control Team (SACT)**
   Bertanggung jawab atas kontrol akses keluar/masuk, penerapan physical distancing, serta pengawasan area karantina/isolation zone.
6. **Operations Continuity Team (OCT)**
   Menjaga keberlangsungan layanan data center, termasuk NOC, sistem kelistrikan, pendinginan, dan jaringan.
7. **Communication and Documentation Team (CDT)**
   Bertugas menyusun laporan kejadian, dokumentasi foto/video, serta menyampaikan komunikasi resmi ke tenant, vendor, dan otoritas terkait.

7. Tanggung Jawab dan Wewenang

Jabatan/Tim	Tanggung Jawab Utama
Incident Commander (IC)	- Menetapkan status darurat dan mengaktifkan SOP. - Mengkoordinasikan seluruh tim tanggap darurat. - Menyetujui langkah isolasi, lockdown, atau evakuasi. - Melaporkan kondisi ke Direksi APJII.
Deputy IC	- Mengimplementasikan keputusan IC di lapangan. - Mengatur rotasi personel dan jadwal kerja darurat. - Melakukan koordinasi dengan pihak eksternal (BNPB, Dinkes).
Crisis Management Team (CMT)	- Mengawasi kebijakan operasional dan komunikasi publik. - Memastikan kepatuhan terhadap BCP dan regulasi pemerintah. - Melakukan evaluasi pasca-insiden.
Health and Safety Team (HST)	- Melakukan screening kesehatan harian. - Menyiapkan dan mengelola area isolasi. - Menyediakan dan mengawasi penggunaan PPE. - Menangani prosedur desinfeksi dan waste management medis.
Security & Access Control Team (SACT)	- Mengatur protokol keluar/masuk dengan pemeriksaan suhu dan daftar kunjungan. - Menjaga keamanan area karantina dan membatasi mobilitas personel.
Operations Continuity Team (OCT)	- Memastikan infrastruktur IT & MEP tetap beroperasi aman. - Menjalankan shift rotation system untuk menghindari paparan massal. - Melakukan remote monitoring bila memungkinkan.
Communication & Documentation Team (CDT)	- Menyusun laporan insiden dan notifikasi resmi. - Menjaga konsistensi pesan ke tenant dan regulator. - Mengarsipkan seluruh dokumen dan hasil evaluasi.

8. Prosedur Penanganan

Prosedur ini mencakup **tahapan operasional lengkap** mulai dari pencegahan hingga pemulihan:

8.1. Tahap 1 – Pencegahan dan Kesiapsiagaan

1. Melakukan **monitoring harian** atas status kesehatan global/nasional dari WHO, Kemenkes, dan BNPB.
2. Menetapkan **status kesiagaan internal** (Level 0–3):
    - Level 0: Normal Operation
    - Level 1: Waspada (kasus nasional terdeteksi)
    - Level 2: Siaga (kasus di wilayah Jabodetabek)
    - Level 3: Darurat (kasus di area fasilitas atau staf terpapar)
3. Menerapkan **kebijakan kerja bergilir dan remote work** untuk staf non-kritis.
4. Menyediakan **alat pelindung diri (PPE)** bagi seluruh personel.
5. Menetapkan **zona sanitasi wajib** di setiap pintu masuk (temperature check, hand sanitizer, UV cabinet).

8.2. Tahap 2 – Respon Darurat

1. Aktivasi SOP oleh Incident Commander bila terdapat personel dengan gejala menular.
2. Personel dengan gejala segera **dipisahkan dan dibawa ke area isolasi** sementara.
3. Koordinasi dengan fasilitas kesehatan terdekat untuk pemeriksaan lanjutan.
4. SACT menutup sementara area terdampak dan membatasi akses.
5. HST melakukan **disinfeksi menyeluruh** dengan bahan disinfektan sesuai standar WHO.
6. Semua personel yang kontak langsung di-*trace* dan diarahkan ke karantina mandiri.
7. CDT mengirim **notifikasi internal dan eksternal** terkait situasi terkini.

8.3. Tahap 3 – Pemulihan Operasional

1. Area yang terkontaminasi dinyatakan aman setelah hasil desinfeksi dan clearance dari HST.
2. Personel yang terpapar kembali bekerja hanya setelah dinyatakan **fit-to-work** oleh pihak medis.
3. Re-entry dilakukan bertahap sesuai prioritas fungsional.
4. Normalisasi sistem dilakukan dengan **monitoring intensif selama 14 hari**.
5. CMT melakukan **review efektivitas penanganan** dan update terhadap BCP serta ERP.

8.4. Tahap 4 – Evaluasi Pasca-Inisiden

1. Mengumpulkan seluruh laporan dari tim terkait.
2. Melakukan *Root Cause Analysis (RCA)* terhadap penyebab paparan dan hambatan operasional.
3. Menyusun **Post-Incident Report (PIR)** berisi:
    - Kronologi kejadian
    - Dampak operasional
    - Tindakan yang diambil
    - Rekomendasi perbaikan
4. Melakukan **briefing pembelajaran (lesson learned)** kepada seluruh personel.

9. Komunikasi dan Pelaporan

9.1. Jalur Komunikasi Internal

- IC → CMT → Semua Tim Pendukung
- CMT → Direksi APJII
- HST → Personel dan Security (status kesehatan & area aman)
- CDT → Tenant dan pengguna layanan

9.2. Komunikasi Eksternal

- Dinas Kesehatan setempat / Satgas COVID-19
- BPBD / BNPB
- Vendor dan kontraktor yang beroperasi di fasilitas
- Tenant / pelanggan data center

9.3. Format Laporan Darurat

Setiap kejadian wajib dilaporkan menggunakan format berikut:

- Tanggal dan waktu kejadian
- Jenis insiden (pandemi/wabah/paparan)
- Lokasi area terdampak
- Jumlah personel terlibat
- Tindakan yang dilakukan
- Status pemulihan
- Catatan/temuan tambahan

11. Pelatihan dan Simulasi

Untuk menjaga kesiapsiagaan, APJII wajib melaksanakan:

1. **Simulasi Tanggap Darurat Kesehatan** minimal **2 kali per tahun**, mencakup:
    - Evakuasi medis
    - Isolasi dan lockdown area
    - Koordinasi antar-tim dan komunikasi
2. **Pelatihan PPE dan Desinfeksi Mandiri** untuk seluruh staf dan kontraktor.
3. **Briefing Awareness** setiap 6 bulan tentang protokol kesehatan.
4. **Audit Internal** oleh Tim HSE & BCP untuk memastikan efektivitas SOP.

Catatan pelatihan disimpan oleh HR & HSE Department sebagai bukti kepatuhan terhadap ISO 45001 dan ISO 22301.

12. Penutup

SOP ini menjadi pedoman resmi bagi seluruh personel Data Center APJII dalam menghadapi situasi pandemi atau kejadian kesehatan massal. Semua pihak wajib mematuhi prosedur yang telah ditetapkan untuk menjamin **keselamatan personel**, **keberlangsungan layanan**, serta **perlindungan reputasi organisasi**.

SOP ini bersifat **living document**, yang harus dievaluasi secara berkala minimal **setiap 12 bulan** atau setiap kali terjadi perubahan signifikan dalam peraturan pemerintah, standar internasional, maupun kondisi epidemiologis nasional.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XV
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENANGANAN GANGGUAN DARURAT YANG DISEBABKAN OLEH PETIR DAN KELISTRIKAN EKSTERNAL DATA CENTER APJII

1. PENDAHULUAN

Data center APJII yang berlokasi di Gedung Cyber-1 merupakan fasilitas kritikal nasional yang menyediakan layanan interkoneksi dan internet exchange utama di Indonesia. Dalam operasionalnya, keandalan sistem kelistrikan dan keamanan terhadap gangguan elektromagnetik serta petir menjadi prioritas utama untuk menjaga **availability**, **integrity**, dan **continuity** layanan data center.

Indonesia, sebagai wilayah tropis dengan tingkat aktivitas petir yang tinggi, sangat berpotensi mengalami gangguan eksternal akibat sambaran langsung maupun induksi petir, serta gangguan suplai listrik dari jaringan PLN. Oleh karena itu, diperlukan **Standard Operating Procedure (SOP)** khusus yang mengatur tata cara penanganan darurat apabila terjadi gangguan akibat petir atau kelistrikan eksternal agar kerusakan peralatan, downtime, dan risiko keselamatan dapat diminimalkan.

2. TUJUAN

Tujuan dari SOP ini adalah untuk:

1. Menetapkan langkah-langkah sistematis dalam penanganan kejadian darurat akibat petir atau gangguan kelistrikan eksternal di lingkungan data center APJII atau Gedung Cyber-1.
2. Menjamin keselamatan personel, perlindungan peralatan, dan kontinuitas layanan IT serta telekomunikasi.
3. Memastikan koordinasi yang cepat, tepat, dan terukur antara tim operasional, keamanan, dan pihak eksternal (PLN, manajemen gedung, vendor UPS/Genset, dsb).
4. Menjadi pedoman dalam investigasi, pelaporan, dan pencegahan kejadian berulang.

3. DASAR DAN REFERENSI STANDAR

SOP ini disusun dengan mengacu pada standar nasional dan internasional berikut:

3.1 Standar Nasional dan Internasional

- **TIA-942-C**: Telecommunications Infrastructure Standard for Data Centers (Bab: Electrical System & Site Space Consideration)
- **NFPA 70 (NEC)**: National Electrical Code (Lightning & Surge Protection)
- **NFPA 780**: Standard for the Installation of Lightning Protection Systems
- **IEC 62305 Series**: Protection Against Lightning (Parts 1–4)
- **IEEE Std 142 (Green Book)**: Recommended Practice for Grounding of Industrial and Commercial Power Systems
- **ISO 22301:2019**: Business Continuity Management System (BCMS)
- **ISO 45001:2018**: Occupational Health and Safety Management System
- **SNI 03-7015-2004**: Sistem Proteksi Petir
- **SNI IEC 60364-4-44:2011**: Proteksi terhadap Gangguan Tegangan Lebih dan Transien

3.2 Dokumen Internal dan Acuan Operasional

- Kebijakan K3L Data Center APJII
- SOP Penanganan Gangguan Listrik Internal (SOP-DC-ELEC-002)
- SOP Eskalasi Insiden Kritis (SOP-DC-ESC-001)
- Logbook Operasional dan Incident Register
- Data Sheet UPS, Genset, ATS/AMF, SPD, dan Grounding System

4. DEFINISI ISTILAH

Istilah	Definisi
Petir (Lightning)	Discharge listrik atmosferik yang terjadi antara awan dan bumi atau antar awan, menghasilkan lonjakan tegangan tinggi.
Surge/Transient Voltage	Lonjakan tegangan sesaat akibat induksi elektromagnetik dari sambaran petir atau switching listrik eksternal.
SPD (Surge Protection Device)	Perangkat proteksi yang membatasi lonjakan tegangan berlebih akibat petir atau gangguan eksternal.
Genset (Generator Set)	Perangkat pembangkit listrik cadangan yang berfungsi otomatis ketika sumber listrik utama (PLN) padam.
ATS/AMF Panel	Panel otomatis untuk memindahkan beban listrik dari sumber utama (PLN) ke genset, dan sebaliknya.
Grounding System	Sistem pentanahan yang mengalirkan energi petir atau arus bocor ke bumi dengan aman.
BMS (Building Management System)	Sistem otomatisasi untuk monitoring dan kontrol fasilitas (listrik, pendingin, alarm, dll).
Incident Commander (IC)	Personel yang ditunjuk untuk memimpin dan mengkoordinasikan penanganan insiden darurat.

Istilah	Definisi
Failover	Proses otomatis pemindahan beban operasional ke sistem cadangan untuk menjaga layanan tetap aktif.

5. RUANG LINGKUP

5.1 Lokasi Berlaku

SOP ini berlaku di seluruh area operasional **Data Center APJII** yang berada di **Gedung Cyber-1.**

5.2 Jenis Gangguan yang Dicakup

1. **Gangguan akibat sambaran petir langsung**, yang menyebabkan kerusakan fisik pada sistem proteksi atau lonjakan arus ke instalasi listrik.
2. **Gangguan akibat induksi petir tidak langsung**, seperti lonjakan tegangan pada jalur kabel listrik atau data.
3. **Gangguan akibat kelistrikan eksternal dari PLN**, seperti overvoltage, undervoltage, brownout, atau pemadaman total.
4. **Gangguan kombinasi**, yaitu gangguan petir yang memicu kerusakan peralatan kelistrikan eksternal dan internal sekaligus.

5.3 Batasan

- SOP ini **tidak mencakup** penanganan kebakaran (diatur dalam SOP Emergency Fire Handling).
- SOP ini **tidak mencakup** perbaikan teknis jangka panjang pasca-insiden (diatur dalam SOP Preventive & Corrective Maintenance).

6. PROSEDUR PENANGANAN

6.1 Tahap 1 – Deteksi dan Identifikasi Awal

1. Sistem BMS atau alarm SPD akan mengirim notifikasi lonjakan tegangan atau gangguan suplai PLN.
2. Operator NOC mencatat waktu kejadian, indikator peringatan, dan area terdampak.
3. Apabila terlihat flash petir di area rooftop atau grounding bar menunjukkan arus berlebih, aktifkan **status siaga petir**.

6.2 Tahap 2 – Respon Awal

1. Incident Commander (IC) segera diberitahu oleh Operator NOC.
2. Lakukan pengecekan kondisi sumber listrik:
    - **PLN**: status breaker, incoming voltage.
    - **UPS**: beban, alarm, mode bypass atau on-battery.
    - **Genset**: status AMF/ATS dan tegangan output.
3. Jika terdapat **tegangan abnormal atau shutdown mendadak**, segera isolasi sumber daya yang rusak (open circuit breaker sesuai SOP isolasi listrik).

6.3 Tahap 3 – Aktivasi Mode Darurat

1. Jika suplai PLN gagal > 10 detik, sistem **ATS otomatis memindahkan** beban ke **genset**.
2. Pastikan sistem pendingin (PAC/CRAC) dan UPS tetap aktif.
3. Operator melaporkan status ke:
    - Supervisor Operasional
    - Manajemen Gedung Cyber-1
    - Tim K3L dan Security

6.4 Tahap 4 – Mitigasi Teknis

1. Periksa semua SPD di panel utama dan sub-panel. Jika **indikator SPD rusak (merah)**, segera ganti unit cadangan.
2. Lakukan pemeriksaan visual terhadap grounding bar, konektor, dan kabel.
3. Pastikan **potensial grounding < 1 ohm** (untuk data center Tier-3 ke atas).
4. Jika ditemukan **bau terbakar** atau suara abnormal, lakukan shutdown selektif terhadap peralatan non-kritis.

6.5 Tahap 5 – Pemulihan dan Normalisasi

1. Setelah suplai PLN stabil minimal 15 menit, kembalikan beban dari genset ke PLN secara bertahap melalui ATS.
2. Verifikasi kestabilan tegangan, arus, dan frekuensi sebelum memulihkan semua sistem.
3. Pastikan semua alarm di BMS dalam status “Normal/Green”.
4. Update logbook insiden dan kirim laporan sementara (Incident Preliminary Report) dalam waktu maksimal 1 jam.

6.6 Tahap 6 – Evaluasi dan Pelaporan

1. Tim teknis melakukan **root cause analysis (RCA)** untuk menentukan sumber gangguan.
2. Buat **Incident Report Final** lengkap dengan:
    - Kronologi kejadian
    - Waktu dan durasi gangguan
    - Dampak layanan
    - Komponen yang terdampak
    - Langkah perbaikan & pencegahan
3. Laporan disampaikan kepada:
    - Manajemen APJII
    - Pengelola Gedung Cyber-1
    - Vendor sistem listrik terkait

7. KESELAMATAN DAN K3L

- Dilarang melakukan pemeriksaan panel listrik tanpa APD lengkap (sarung tangan isolasi, sepatu safety, face shield).
- Pastikan area kerja aman dari potensi induksi petir atau kabel basah.
- Selalu pasang **Lock-Out Tag-Out (LOTO)** saat isolasi panel.
- Pastikan komunikasi aktif melalui radio/HT antar personel selama penanganan.

8. DOKUMENTASI DAN RECORD

Semua dokumen berikut harus disimpan minimal 3 tahun:

- Incident Log (waktu kejadian, tindakan, personel, hasil)
- SPD & Grounding Test Report
- Laporan PLN/Genset Monitoring
- RCA dan Preventive Action Record

9. PENUTUP

SOP ini bertujuan menjaga keandalan operasional dan keamanan data center APJII terhadap ancaman alamiah (petir) dan eksternal (PLN). Seluruh personel wajib memahami prosedur ini dan mengikuti simulasi darurat minimal **dua kali dalam setahun** untuk memastikan kesiapan menghadapi insiden nyata.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XVI
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENANGANAN GANGGUAN DARURAT JARINGAN KOMUNIKASI EKSTERNAL DATA CENTER APJII

1. Pendahuluan

Jaringan komunikasi eksternal di Data Center APJII merupakan infrastruktur vital yang menghubungkan sistem internal Data Center dengan jaringan publik Internet Exchange (IX), jaringan anggota ISP, upstream provider, dan mitra strategis lainnya. Ketersediaan dan stabilitas jaringan eksternal ini menjadi faktor kritis dalam menjamin kontinuitas layanan bagi seluruh anggota APJII dan pelanggan colocation.

Gangguan pada jaringan komunikasi eksternal — baik akibat **kegagalan fisik (hardware failure)**, **konfigurasi salah (misconfiguration)**, **serangan siber (DDoS, BGP hijacking)**, maupun **force majeure (kebakaran, banjir, gempa)** — dapat berdampak serius terhadap performa dan ketersediaan layanan Data Center APJII.

Oleh karena itu, diperlukan **SOP (Standard Operating Procedure)** yang komprehensif untuk memastikan bahwa setiap insiden atau gangguan darurat pada jaringan komunikasi eksternal dapat ditangani dengan cepat, terkoordinasi, aman, dan terdokumentasi dengan baik.

2. Tujuan

SOP ini bertujuan untuk:

1. Menetapkan langkah-langkah terstruktur dalam menangani gangguan darurat jaringan komunikasi eksternal pada Data Center APJII.
2. Memastikan waktu pemulihan (recovery time) seoptimal mungkin dan meminimalkan dampak terhadap layanan dan anggota.
3. Menjamin koordinasi efektif antara tim internal APJII (NOC, Infrastruktur, Keamanan, dan Manajemen) serta pihak eksternal (ISP anggota, vendor, dan regulator).
4. Mendukung implementasi standar **Business Continuity Plan (BCP)** dan **Disaster Recovery Plan (DRP)** pada operasional Data Center APJII.
5. Memenuhi persyaratan kepatuhan terhadap **standar internasional dan nasional** terkait manajemen insiden dan keandalan infrastruktur komunikasi.

3. Dasar dan Referensi Standar

SOP ini disusun berdasarkan acuan dan referensi sebagai berikut:

3.1 Standar Internasional

- **ISO/IEC 27035:2016** — Information Security Incident Management
- **ISO/IEC 22301:2019** — Business Continuity Management Systems
- **ISO/IEC 20000-1:2018** — IT Service Management
- **TIA-942-C:2024** — Telecommunications Infrastructure Standard for Data Centers
- **ITIL v4** — Incident, Problem, and Change Management Framework
- **RFC 7454** — BGP Operations and Security Best Practices
- **NIST SP 800-61 Rev.2** — Computer Security Incident Handling Guide

3.2 Regulasi dan Pedoman Nasional

- **Peraturan Menteri Kominfo No. 7 Tahun 2021** tentang Penyelenggaraan Telekomunikasi
- **Pedoman Operasional IX APJII**
- **Dokumen BCP & DRP APJII**
- **Kebijakan Keamanan Informasi dan Jaringan APJII (Information Security Policy)**

4. Definisi Istilah

Istilah	Definisi
Gangguan Darurat Jaringan Komunikasi Eksternal	Kondisi tidak normal yang menyebabkan degradasi atau penghentian total layanan komunikasi antara Data Center APJII dan jaringan eksternal (IX, ISP anggota, atau upstream).
NOC (Network Operation Center)	Unit teknis yang bertanggung jawab memantau, mengidentifikasi, dan menangani insiden jaringan 24x7.
Incident Severity Level	Klasifikasi tingkat keparahan insiden berdasarkan dampak dan urgensi: Level 1 (Minor), Level 2 (Major), Level 3 (Critical/Emergency).
Root Cause Analysis (RCA)	Analisis penyebab utama yang dilakukan setelah insiden untuk mencegah kejadian serupa.
Failover Link	Jalur komunikasi cadangan yang otomatis mengambil alih fungsi utama saat jalur utama gagal.
External Communication Network	Infrastruktur komunikasi eksternal yang mencakup peering link, upstream connection, IX fabric, dan interkoneksi ISP.
Incident Commander (IC)	Personel yang ditunjuk oleh APJII untuk mengoordinasikan penanganan insiden hingga pemulihan selesai.

5. Ruang Lingkup

SOP ini mencakup seluruh aktivitas yang terkait dengan **identifikasi, eskalasi, mitigasi, pemulihan, komunikasi, dan dokumentasi** atas gangguan darurat jaringan komunikasi eksternal di lingkungan Data Center APJII.

5.1 Ruang Lingkup Teknis

- Sistem dan perangkat jaringan eksternal (router, switch core, border gateway, firewall edge, DDoS mitigation system).
- Koneksi antar data center (DC-to-DC interconnect, IX backbone, MPLS link).
- Koneksi eksternal ke ISP anggota dan upstream global provider.
- Jalur redundansi dan failover yang terhubung ke perangkat komunikasi eksternal.
- Infrastruktur monitoring dan alerting (NMS/APM tools).

5.2 Ruang Lingkup Organisasi

- **Tim Internal:**
  - **Helpdesk (Single Point of Contact/SPOC: Primary Responder)**
  - **Tim Teknis/NOC**
  - **Tim Manajemen APJII dan Komunikasi Publik**
- **Pihak Eksternal:**
  - ISP anggota APJII
  - Vendor perangkat dan penyedia layanan (Cisco, Juniper, Mikrotik, dll.)
  - Provider upstream Internet global
  - Regulator (KOMDIGI) jika insiden berdampak signifikan nasional

5.3 Ruang Lingkup Tahapan Penanganan

1. **Deteksi dan Validasi Gangguan** — Identifikasi awal melalui monitoring system, alarm, atau laporan anggota.
2. **Eskalasi Insiden** — Penetapan level keparahan dan penunjukan Incident Commander.
3. **Analisis Awal dan Isolasi** — Menentukan penyebab awal dan menahan dampak lebih luas (misal, menutup sesi BGP tertentu).
4. **Mitigasi dan Pemulihan Layanan** — Aktivasi jalur cadangan, konfigurasi ulang, atau tindakan teknis lain untuk mengembalikan konektivitas.
5. **Komunikasi dan Koordinasi** — Informasi internal, pemberitahuan anggota, dan update status.
6. **RCA dan Post-Incident Review** — Analisis akar penyebab, rekomendasi perbaikan, serta laporan insiden resmi.

6. Prosedur Detail Penanganan Gangguan Darurat

Prosedur ini menggambarkan langkah-langkah sistematis mulai dari deteksi awal hingga pemulihan layanan dan evaluasi pascainsiden.

6.1 Tahap 1 – Deteksi dan Validasi Awal

Tujuan: Mengidentifikasi gangguan sesegera mungkin dan memastikan kebenaran kejadian.

Langkah-langkah:

1. **Monitoring otomatis:** Sistem NMS/APM (seperti Zabbix, PRTG, atau LibreNMS) mendeteksi anomali (packet loss, latency tinggi, link down, BGP session drop).
2. **Pemberitahuan otomatis:** Alarm dikirim ke tim NOC melalui email, SMS, atau aplikasi insiden (misal PagerDuty/WhatsApp Group NOC).
3. **Verifikasi awal:**
    - Cek status perangkat (ping/traceroute, SNMP check).
    - Bandingkan dengan status di router lain untuk memastikan bukan false alarm.
4. **Klasifikasi awal:** Tentukan apakah gangguan bersifat **internal** (perangkat DC APJII) atau **eksternal** (provider atau ISP anggota).
5. **Pencatatan awal:** NOC membuat entri pada sistem log/incident ticket dengan timestamp deteksi pertama.

6.2 Tahap 2 – Penetapan Tingkat Keparahan dan Eskalasi

Level	Deskripsi	Contoh Kasus	Waktu Respon
Level 1 (Minor)	Gangguan kecil tanpa dampak signifikan pada layanan utama.	Fluktuasi latency pada 1 link upstream.	< 30 menit
Level 2 (Major)	Gangguan berdampak pada sebagian pengguna/anggota, namun masih ada jalur cadangan.	Down salah satu link IX atau core router.	< 15 menit
Level 3 (Critical/Emergency)	Seluruh konektivitas eksternal terganggu atau layanan utama lumpuh total.	Semua koneksi eksternal putus, DDoS besar-besaran, atau kerusakan fisik perangkat utama.	**< 5 menit (respon langsung)**

Langkah-langkah:

1. NOC menentukan tingkat keparahan berdasarkan dampak aktual.
2. Jika Level 2 atau 3, **Incident Commander (IC)** ditunjuk oleh Kepala NOC atau Manager Infrastruktur.
3. IC bertanggung jawab mengoordinasikan seluruh tindakan teknis, komunikasi, dan dokumentasi.
4. NOC segera **melakukan eskalasi** ke pihak terkait (lihat Bagian 8: Alur Eskalasi).

6.3 Tahap 3 – Isolasi dan Analisis Awal

Tujuan: Mengidentifikasi sumber masalah dan mencegah meluasnya dampak.

Langkah-langkah:

1. IC memerintahkan tim NOC melakukan langkah teknis seperti:
    - Isolasi router/switch bermasalah (shutdown port, disable interface, hold BGP session).
    - Cek konfigurasi BGP, OSPF, dan VRRP untuk kemungkinan route flap.
    - Analisis log (syslog, SNMP trap, flow data) untuk identifikasi penyebab.
2. Jika terindikasi serangan DDoS, segera aktifkan **DDoS mitigation system atau blackhole routing**.
3. Jika disebabkan oleh provider eksternal, lakukan **konfirmasi langsung ke NOC provider** melalui jalur komunikasi resmi.
4. Catat hasil analisis sementara pada log insiden.

Tujuan: Mengidentifikasi sumber masalah dan mencegah meluasnya dampak.

Langkah-langkah:

1. IC memerintahkan tim NOC melakukan langkah teknis seperti:
    - Isolasi router/switch bermasalah (shutdown port, disable interface, hold BGP session).
    - Cek konfigurasi BGP, OSPF, dan VRRP untuk kemungkinan route flap.
    - Analisis log (syslog, SNMP trap, flow data) untuk identifikasi penyebab.
2. Jika terindikasi serangan DDoS, segera aktifkan **DDoS mitigation system atau blackhole routing**.
3. Jika disebabkan oleh provider eksternal, lakukan **konfirmasi langsung ke NOC provider** melalui jalur komunikasi resmi.
4. Catat hasil analisis sementara pada log insiden

6.4 Tahap 4 – Mitigasi dan Pemulihan

Tujuan: Mengembalikan layanan secepat mungkin dengan risiko minimal.

Langkah-langkah:

1. Aktifkan **jalur redundan (failover)** jika tersedia:
    - Backup IX path / alternate upstream link.
    - Route adjustment melalui BGP prepend atau traffic engineering.
2. Lakukan tindakan perbaikan perangkat keras jika diperlukan (hot-swap PSU, replace module, reload device).
3. Verifikasi stabilitas layanan setelah pemulihan dilakukan (monitoring latency, route visibility, throughput).
4. Konfirmasi kepada semua pihak terkait bahwa layanan telah kembali normal.
5. Tandai status insiden sebagai **“Resolved”** di sistem ticketing.

6.5 Tahap 5 – Komunikasi dan Koordinasi

Tujuan: Menjamin transparansi dan koordinasi informasi selama insiden.

Langkah-langkah:

1. **Internal Communication:**
    - NOC memberikan update berkala setiap 30 menit ke IC dan Manajemen APJII.
    - SOC diinformasikan jika ada indikasi serangan keamanan.
2. **External Communication:**
    - IC atau Public Information Officer menginformasikan status insiden kepada ISP anggota melalui email atau portal anggota APJII.
    - Komunikasi dengan vendor dan regulator jika insiden berpotensi berdampak nasional.
3. Semua komunikasi harus terdokumentasi dalam log insiden dan laporan resmi.

6.6 Tahap 6 – RCA dan Evaluasi Pascainsiden

Tujuan: Menemukan akar penyebab dan mencegah insiden serupa.

Langkah-langkah:

1. Dalam waktu **maksimal 24 jam setelah insiden ditutup**, IC memimpin **Root Cause Analysis (RCA)**.
2. Identifikasi: penyebab utama, kronologi, sistem terdampak, waktu pemulihan, dan efektivitas tindakan.
3. Hasil RCA dituangkan dalam **Post-Incident Report (PIR)**.
4. Jika ditemukan kelemahan sistemik, buat rekomendasi tindakan korektif (Corrective Action Plan).
5. Laporan diserahkan kepada Manajemen dan dijadikan dasar update SOP/BCP/DRP.

7. Tanggung Jawab dan Peran

Peran / Unit	Tanggung Jawab Utama
NOC Engineer	Melakukan monitoring, validasi gangguan, tindakan teknis awal, dan pelaporan status.
Incident Commander (IC)	Mengkoordinasikan respon teknis dan komunikasi selama insiden darurat.
Network Infrastructure Team	Menangani eskalasi teknis lanjutan dan pemulihan perangkat atau konfigurasi.
SOC (Security Operation Center)	Mengidentifikasi dan menanggulangi insiden yang bersifat serangan siber.
Facility Management	Memastikan dukungan infrastruktur fisik (daya, suhu, UPS, genset) jika gangguan terkait daya.
Vendor/Provider	Memberikan dukungan teknis sesuai SLA, termasuk penggantian perangkat atau link.

Peran / Unit	Tanggung Jawab Utama
Manajemen APJII	Menyetujui komunikasi eksternal resmi dan menerima laporan akhir insiden.
Public Information Officer (PIO)	Mengatur komunikasi eksternal kepada anggota, mitra, dan regulator.

8. Alur Eskalasi Insiden

8.1 Alur Umum:

1. **Deteksi** oleh NOC
2. **Validasi dan Klasifikasi** (Minor / Major / Critical)
3. **Eskalasi Internal:**
    - Minor → ditangani langsung oleh NOC
    - Major → ke IC dan Network Infrastructure Team
    - Critical → ke IC, SOC, Facility, dan Manajemen APJII
4. **Eskalasi Eksternal (jika diperlukan):**
    - Vendor perangkat (SLA support call)
    - Provider upstream / IX peer
    - Regulator (Kominfo) bila insiden berdampak luas
5. **Koordinasi Pemulihan → Validasi → RCA → Laporan**

8.2 Waktu Eskalasi Maksimal:

Level Insiden	Waktu Eskalasi Internal	Waktu Eskalasi ke Eksternal
Level 1	30 menit	Tidak perlu
Level 2	15 menit	30 menit
Level 3	5 menit	Segera (< 10 menit)

9. Format Pelaporan Insiden (Post-Incident Report Template)

Judul Laporan: Laporan Gangguan Darurat Jaringan Komunikasi Eksternal DC APJII
Tanggal Insiden: ……
Waktu Mulai: …… | **Waktu Pulih:** ……
Durasi Gangguan: …… menit

A. Informasi Umum

- Pelapor: ……
- Unit Pelapor: ……

- Lokasi: ……
- Tipe Gangguan: (Link Down / BGP Flap / DDoS / Hardware Failure / Lainnya)
- Level Insiden: (1 / 2 / 3)

B. Kronologi Kejadian

Tuliskan urutan peristiwa dari deteksi hingga pemulihan layanan dengan timestamp.

C. Dampak

- Layanan terdampak: ……
- Jumlah pelanggan/anggota terdampak: ……
- Estimasi kerugian operasional: ……

D. Analisis Penyebab (RCA)

- Penyebab langsung: ……
- Penyebab akar (root cause): ……
- Faktor pendukung: (misconfig, kegagalan hardware, human error, serangan eksternal, dll.)

E. Tindakan Perbaikan

- Langkah mitigasi yang dilakukan: ……
- Tindakan korektif yang direkomendasikan: ……
- Personel penanggung jawab tindak lanjut: ……

F. Status Akhir

- Status layanan: Pulih / Dalam perbaikan / Monitoring lanjut
- Catatan tambahan: ……

Disusun oleh:
NOC Engineer / Incident Commander
Disetujui oleh:
Manager Infrastruktur / Head of Data Center

10. Lampiran

Lampiran A – Daftar Kontak Penting

Nama/Unit	Jabatan	No. Telepon / WA	Email
NOC APJII	24x7 Monitoring	xxx-xxxxxxx	noc@apjii.or.id
Incident Commander	—	xxx-xxxxxxx	—
SOC APJII	Security Operation	xxx-xxxxxxx	soc@apjii.or.id

Nama/Unit	Jabatan	No. Telepon / WA	Email
Vendor Cisco	TAC Support	—	—
Vendor Juniper	JTAC Support	—	—
ISP Member Contact Center	—	—	—
KOMDIGI / Regulator Contact	—	—	—

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XVII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENANGANAN GANGGUAN DARURAT LEDAKAN, KEBOCORAN BAHAN KIMIA ATAU GAS BERACUN DATA CENTER APJII

1. Pendahuluan

Data Center APJII merupakan fasilitas kritikal yang berfungsi sebagai pusat pengelolaan dan pertukaran data nasional bagi penyelenggara layanan internet di Indonesia. Sebagai infrastruktur vital, keberlangsungan operasional Data Center harus dijaga agar tetap aman, andal, dan memenuhi standar keselamatan kerja serta keamanan lingkungan.

Dalam operasionalnya, potensi gangguan darurat seperti **ledakan, kebocoran bahan kimia, atau gas beracun** dapat terjadi akibat:

- Kegagalan sistem mekanikal atau elektrikal (misalnya sistem UPS, genset, atau sistem pendingin).
- Kebocoran dari bahan pendingin (seperti refrigerant R410A, R407C, atau gas CO_2 suppression system).
- Reaksi kimia dari cairan pembersih atau bahan perawatan peralatan.
- Kegagalan tangki bahan bakar genset (fuel tank) yang dapat menimbulkan uap berbahaya atau ledakan.

SOP ini disusun untuk memastikan setiap personel Data Center APJII memahami dan dapat melakukan tindakan cepat, tepat, dan terkoordinasi dalam menghadapi kondisi darurat yang berpotensi menimbulkan bahaya terhadap keselamatan manusia, aset, dan kontinuitas layanan operasional.

2. Tujuan

Tujuan dari SOP ini adalah untuk:

1. Memberikan **pedoman langkah-langkah preventif dan responsif** terhadap kondisi darurat berupa ledakan, kebocoran bahan kimia, atau gas beracun.
2. Meminimalkan **risiko terhadap keselamatan personel, peralatan IT, dan fasilitas Data Center**.
3. Menjamin **kelangsungan operasional dan layanan kritikal** APJII tetap terjaga setelah insiden.

4. Menetapkan **mekanisme komunikasi, koordinasi, dan pelaporan** antar tim internal, pihak keamanan, penyedia layanan darurat, serta manajemen APJII.
5. Mendukung penerapan **sistem manajemen keselamatan kerja dan lingkungan (HSE)** serta **Business Continuity Management (BCM)** dalam lingkup operasional Data Center.

3. Dasar dan Referensi Standar

SOP ini disusun berdasarkan dan mengacu kepada standar, regulasi, dan panduan berikut:

a. Standar Nasional & Regulasi

1. **Peraturan Menteri Ketenagakerjaan No. 5 Tahun 2018** tentang Keselamatan dan Kesehatan Kerja Lingkungan Kerja.
2. **Peraturan Menteri Lingkungan Hidup No. 13 Tahun 2010** tentang Kualitas Udara dan Emisi Gas Beracun.
3. **Peraturan Pemerintah No. 50 Tahun 2012** tentang Penerapan Sistem Manajemen Keselamatan dan Kesehatan Kerja (SMK3).
4. **Undang-Undang No. 1 Tahun 1970** tentang Keselamatan Kerja.
5. **Peraturan Menteri Komunikasi dan Informatika** tentang Penyelenggaraan Pusat Data dan/atau Disaster Recovery Center.

b. Standar Internasional dan Teknis

1. **TIA-942-C** – *Telecommunications Infrastructure Standard for Data Centers* (khususnya klausul Facility & Safety).
2. **ISO 22301:2019** – *Security and Resilience – Business Continuity Management Systems (BCMS)*.
3. **ISO 45001:2018** – *Occupational Health and Safety Management Systems*.
4. **NFPA 75 dan NFPA 76** – *Fire Protection of Information Technology Equipment*.
5. **ASHRAE Standard 15 & 34** – *Safety Standard for Refrigeration Systems and Designation of Refrigerants*.
6. **ISO 14001:2015** – *Environmental Management System*.
7. **NFPA 68 & 69** – *Explosion Protection by Deflagration Venting & Explosion Prevention Systems*.

4. Definisi Istilah

Untuk kejelasan dan keseragaman pemahaman, istilah-istilah berikut digunakan dalam SOP ini:

1. **Ledakan (Explosion)**
   Suatu peristiwa pelepasan energi secara tiba-tiba yang menimbulkan tekanan dan suhu tinggi, dapat menyebabkan kerusakan struktur dan bahaya kebakaran.
2. **Bahan Kimia Berbahaya (Hazardous Chemical Substance)**
   Zat kimia yang memiliki sifat mudah meledak, beracun, korosif, reaktif, atau mudah menguap, seperti cairan pembersih peralatan listrik, pelarut, oli genset, atau refrigerant sistem pendingin.

3. **Gas Beracun (Toxic Gas)**
   Gas yang dapat menyebabkan gangguan kesehatan atau kematian bila terhirup dalam jumlah tertentu, misalnya CO, H_2S, NH_3, atau kebocoran refrigerant.
4. **Kebocoran (Leakage)**
   Peristiwa keluarnya gas atau cairan dari sistem tertutup akibat kegagalan mekanis, sambungan pipa, atau kerusakan katup.
5. **Area Terdampak (Affected Area)**
   Zona dalam fasilitas Data Center yang mengalami kontaminasi atau paparan bahan berbahaya, gas, atau ledakan.
6. **Tim Tanggap Darurat (Emergency Response Team / ERT)**
   Tim khusus yang telah dilatih untuk menangani kondisi darurat dengan cepat, aman, dan terkoordinasi.
7. **Evakuasi**
   Proses perpindahan personel dari area berbahaya menuju titik kumpul aman (assembly point).
8. **HSSD/VESDA (High Sensitivity Smoke Detection / Very Early Smoke Detection Apparatus)**
   Sistem deteksi dini yang dapat mengidentifikasi potensi kebakaran atau ledakan akibat akumulasi gas atau partikel sebelum terjadi insiden besar.
9. **BMS (Building Management System)**
   Sistem pemantauan dan kontrol otomatis terhadap kondisi lingkungan, suhu, kelembapan, dan deteksi gas di area Data Center.
10. **Lockdown Area**
    Prosedur penghentian sementara aktivitas dan penutupan akses masuk-keluar ke area terdampak untuk mencegah paparan lebih luas.

5. Ruang Lingkup

SOP ini berlaku untuk seluruh kegiatan dan personel yang beroperasi di lingkungan **Data Center APJII**, termasuk namun tidak terbatas pada:

a. Lokasi yang dicakup

- Area Data Hall (Server Room, Rack Zone, MDA/HDA Zone).
- Area UPS, Battery Room, dan Electrical Room.
- Area Chiller Plant, PAC, dan ruang pendingin lainnya.
- Area Fuel Tank, Generator Set, dan ruang mekanikal.
- Ruang Operasional (NOC), ruang teknisi, dan area pendukung lainnya.
- Area luar gedung (exterior) yang berpotensi terpapar bahan kimia atau gas.

b. Jenis Insiden yang Dicakup

1. **Ledakan akibat**:
   - Kebocoran bahan bakar genset.
   - Korsleting listrik pada area bertekanan tinggi.
   - Reaksi kimia akibat bahan pembersih atau cairan pelumas.
2. **Kebocoran bahan kimia**:
   - Cairan refrigerant dari sistem PAC atau chiller.
   - Tumpahan cairan kimia pada kegiatan pemeliharaan peralatan.
   - Kebocoran pelumas atau oli dari mesin mekanikal.

3. **Kebocoran gas beracun**:
    - Emisi CO_2 atau inert gas dari sistem pemadam api (clean agent).
    - Kebocoran gas bertekanan (R410A, R407C, R134A, NH_3, dll).
    - Gas hasil pembakaran tidak sempurna pada sistem genset.

c. Pihak yang Terlibat

- **Tim Operasional Data Center (Facility & IT Operations)**
- **Tim HSE APJII**
- **Security & Building Management**
- **Pihak Maintenance Vendor atau Contractor**
- **Tim Emergency Response (ERT)**
- **Tim Manajemen APJII**

d. Tahapan Penanganan

SOP ini mengatur langkah-langkah penanganan dalam seluruh siklus tanggap darurat, yaitu:

1. **Peringatan dini (Early Warning)**
2. **Aktivasi rencana darurat**
3. **Koordinasi dengan pihak keamanan dan ERT**
4. **Evakuasi dan lockdown area terdampak**
5. **Komunikasi dan pelaporan ke manajemen**
6. **Pemulihan dan normalisasi operasional**
7. **Evaluasi dan review pasca-insiden**

6. Tanggung Jawab dan Kewenangan

Dalam pelaksanaan penanganan gangguan darurat, setiap pihak memiliki tanggung jawab dan kewenangan yang jelas agar tindakan yang diambil efektif, aman, dan terkoordinasi.

6.1. Manajemen APJII

- Menetapkan dan mengesahkan kebijakan keselamatan dan tanggap darurat di lingkungan Data Center APJII.
- Menyediakan sumber daya, peralatan, dan pelatihan bagi personel tanggap darurat.
- Menyetujui laporan hasil evaluasi pasca-insiden dan rencana perbaikan (Corrective Action Plan).
- Menunjuk penanggung jawab utama (Incident Commander) untuk situasi darurat berskala besar.

6.2. Incident Commander (IC)

- Mengambil alih kendali penuh atas situasi darurat.
- Menentukan apakah area harus di-*lockdown* atau dievakuasi.
- Menjadi penghubung utama dengan otoritas eksternal (pemadam kebakaran, polisi, rumah sakit, BPBD).
- Menyetujui aktivasi sistem darurat seperti *gas suppression*, *HVAC shutdown*, atau *power isolation*.

6.3. Tim Emergency Response (ERT)

- Melakukan identifikasi cepat jenis dan lokasi insiden.
- Melaksanakan prosedur tanggap darurat sesuai kategori kejadian (ledakan, gas, bahan kimia).
- Mengamankan area dan memastikan tidak ada personel yang berada dalam zona bahaya.
- Mengoperasikan peralatan darurat (gas detector, alat pelindung diri, respirator, APAR, dan peralatan spill kit).
- Melakukan pertolongan pertama (First Aid) bila terdapat korban.

6.4. Tim Facility Operation

- Menonaktifkan sistem mekanikal-elektrikal yang berpotensi memperburuk kondisi (contoh: sistem ventilasi, fuel pump).
- Memantau dan menutup katup gas atau refrigerant bila memungkinkan secara aman.
- Memberikan informasi teknis lokasi pipa, tangki, sensor gas, atau valve kepada ERT dan pemadam kebakaran.
- Melakukan verifikasi sistem melalui *BMS (Building Management System)* dan *Fire Alarm Panel*.

6.5. Tim Security / Keamanan

- Melakukan isolasi area terdampak dan membatasi akses.
- Membuka jalur evakuasi dan mengarahkan personel ke titik kumpul aman.
- Berkoordinasi dengan pihak keamanan eksternal dan otoritas darurat.
- Mencatat daftar personel yang berhasil dievakuasi dan memastikan tidak ada yang tertinggal.

6.6. Seluruh Personel Data Center dan Pengunjung

- Segera melapor kepada petugas atau ERT bila mendeteksi bau gas, tumpahan bahan kimia, atau ledakan kecil.
- Mengikuti instruksi evakuasi dengan tertib dan tidak menggunakan lift.
- Tidak kembali ke area terdampak tanpa izin resmi dari IC.

7. Prosedur Penanganan Darurat

Prosedur tanggap darurat dilakukan berdasarkan jenis insiden yang terjadi, dengan prioritas utama keselamatan manusia dan pencegahan eskalasi risiko.

7.1. Peringatan Dini dan Identifikasi Awal

1. Sistem HSSD/VESDA, detektor gas, atau alarm lingkungan BMS mendeteksi anomali.
2. Tim Facility dan Security memverifikasi kondisi di lapangan (tanpa membuka area berbahaya tanpa APD).
3. Bila indikasi ledakan atau kebocoran terkonfirmasi, segera aktifkan **alarm evakuasi** dan **laporkan ke Incident Commander**.

7.2. Aktivasi Rencana Darurat

1. Incident Commander mengumumkan status **"Emergency Level 1 / 2"** tergantung skala insiden.
2. Tim ERT mengaktifkan SOP sesuai kategori (ledakan / gas / bahan kimia).
3. Sistem BMS otomatis memutus suplai listrik atau HVAC di area terdampak.
4. Lockdown area diberlakukan untuk mencegah penyebaran gas atau uap beracun.

7.3. Prosedur Spesifik Berdasarkan Jenis Insiden

a. Ledakan

- Jauhkan seluruh personel dari area yang rusak; hindari penggunaan perangkat elektronik.
- Matikan sumber daya listrik dan bahan bakar di area terkait.
- ERT melakukan pemadaman awal bila masih terdapat api kecil menggunakan APAR jenis CO_2 atau Dry Chemical Powder.
- Periksa potensi ledakan sekunder dari sistem bahan bakar atau baterai UPS.

b. Kebocoran Bahan Kimia

- Gunakan *Chemical Spill Kit* dan APD lengkap (sarung tangan nitril, kacamata pelindung, masker respirator).
- Tutup sumber kebocoran bila aman dilakukan.
- Hindari kontak langsung dengan cairan atau uap.
- Pasang *warning tape* di sekitar area dan nyalakan exhaust system lokal (bila tidak berisiko memperluas paparan).
- Laporkan jenis bahan kimia dan jumlah yang bocor kepada Incident Commander.

c. Kebocoran Gas Beracun

- Aktifkan sistem deteksi gas untuk mengetahui konsentrasi paparan (ppm).
- Tutup katup utama dan aktifkan sistem ventilasi evakuasi.
- Larang penggunaan sumber api atau peralatan listrik di sekitar area.
- Lakukan evakuasi horizontal ke area bertekanan positif.
- ERT memantau kadar gas sampai batas aman tercapai sesuai nilai TLV (Threshold Limit Value).

8. Prosedur Evakuasi dan Lockdown

1. Alarm evakuasi berbunyi disertai pengumuman melalui sistem PA.
2. Seluruh personel mengikuti jalur evakuasi menuju **Assembly Point** yang telah ditetapkan.
3. Security memastikan tidak ada personel tertinggal di area server, panel, atau ruang pendingin.
4. Lockdown diberlakukan dengan menutup akses pintu utama, tangga, dan ruang mekanikal.
5. Petugas ERT memverifikasi kondisi udara di Assembly Point untuk memastikan keamanan.
6. IC melaporkan jumlah evakuasi dan kondisi terakhir ke manajemen APJII.

9. Komunikasi dan Pelaporan

1. **Internal Communication Flow**
   - Deteksi awal → ERT Leader → Incident Commander → Facility Head → Manajemen APJII.
2. **External Communication Flow**
   - Incident Commander → Pemadam Kebakaran, Rumah Sakit, BPBD, Kepolisian.
3. **Media Communication**
   - Hanya juru bicara resmi APJII yang boleh memberikan pernyataan publik.
4. **Pelaporan Insiden**
   - Formulir Laporan Darurat harus diisi maksimal **1 jam** setelah kejadian oleh ERT.
   - Laporan lengkap diserahkan ke Manajemen APJII dalam **1 x 24 jam**.

10. Pemulihan dan Normalisasi Operasional

1. Setelah dinyatakan aman oleh Incident Commander dan pihak berwenang, area dilakukan **ventilasi dan pembersihan**.
2. Tim Facility melakukan **inspeksi teknis** terhadap sistem listrik, mekanikal, pendingin, dan IT.
3. Aktivasi ulang sistem dilakukan secara bertahap sesuai **Standard Operating Restoration Sequence**.
4. Bila ada kerusakan peralatan IT, lakukan prosedur **failover** ke DRC (Disaster Recovery Center) APJII.
5. Data dan sistem monitoring (CCTV, BMS, Alarm Log) disalin untuk kebutuhan audit pasca-insiden.

11. Dokumentasi dan Pelaporan

Semua kejadian dan tindakan penanganan harus didokumentasikan dengan lengkap untuk keperluan audit dan peningkatan sistem keamanan. Dokumen yang wajib disimpan:

1. **Laporan Insiden Darurat (Emergency Incident Report Form)**
2. **Foto dan rekaman CCTV insiden**
3. **Log sistem BMS, alarm, dan sensor gas**
4. **Checklist evaluasi pasca-insiden (Post-Incident Evaluation Form)**
5. **Laporan analisis akar penyebab (Root Cause Analysis – RCA)**
6. **Corrective and Preventive Action (CAPA) Plan**

Seluruh dokumen disimpan oleh **HSE dan Facility Management APJII** selama minimal **5 tahun** atau sesuai kebijakan organisasi.

12. Evaluasi dan Review SOP

1. Evaluasi efektivitas SOP dilakukan setiap **6 bulan sekali** atau setelah terjadi insiden nyata.
2. Hasil evaluasi digunakan untuk memperbarui langkah-langkah pencegahan dan pelatihan tanggap darurat.
3. Simulasi darurat (drill) wajib dilakukan minimal **2 kali per tahun** meliputi skenario ledakan dan kebocoran gas.

4. Setiap perubahan SOP harus disahkan oleh **Manajemen APJII** dan disosialisasikan kepada seluruh personel.
5. Audit kepatuhan terhadap SOP dilakukan dalam rangka sertifikasi **ISO 45001** dan **ISO 22301** untuk Data Center APJII.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XVIII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENANGANAN GANGGUAN DARURAT MAJOR FAILURE SISTEM PENDINGIN UTAMA DATA CENTER APJII

1. Pendahuluan

Sistem pendingin utama atau HVAC (Heating, Ventilation, and Air Conditioning) merupakan salah satu komponen kritikal dalam operasional Data Center APJII. Sistem ini berfungsi menjaga suhu, kelembapan, dan kualitas udara di ruang IT agar tetap berada dalam batas ambang yang ditetapkan sesuai standar operasional, guna memastikan keandalan dan keberlangsungan layanan infrastruktur telekomunikasi dan internet exchange APJII.

Gangguan besar atau *major failure* pada sistem pendingin utama berpotensi menyebabkan peningkatan suhu ruang data secara cepat (*thermal runaway*) yang dapat mengganggu performa server, perangkat jaringan, bahkan berujung pada kerusakan perangkat keras dan downtime layanan.

Oleh karena itu, SOP ini disusun sebagai pedoman resmi bagi seluruh personel operasional, teknisi, dan pihak ketiga yang terlibat dalam pengelolaan sistem pendingin di Data Center APJII untuk menangani situasi gangguan besar secara cepat, sistematis, dan terkoordinasi.

2. Tujuan

SOP ini bertujuan untuk:

1. Menetapkan langkah-langkah terstruktur dalam menangani kondisi *major failure* pada sistem pendingin utama di Data Center APJII.
2. Memastikan kesinambungan operasional layanan IT tetap terjaga dengan meminimalkan risiko downtime akibat gangguan sistem pendingin.
3. Mengatur koordinasi antar tim teknis, keamanan, dan manajemen selama proses penanganan gangguan berlangsung.
4. Melindungi perangkat IT dan fasilitas data center dari risiko kerusakan akibat suhu dan kelembapan ekstrem.
5. Menjamin keselamatan personel dan penerapan prinsip K3 selama proses perbaikan dan pemulihan sistem pendingin.
6. Menerapkan prinsip *lessons learned* dan *post-incident review* untuk peningkatan berkelanjutan (*continuous improvement*).

3. Dasar dan Referensi Standar

SOP ini mengacu pada pedoman, regulasi, dan standar teknis berikut:

No	Standar / Dokumen Referensi	Deskripsi / Relevansi
1	**TIA-942-C Data Center Telecommunications Infrastructure Standard**	Panduan desain dan operasional data center termasuk sistem HVAC dan kontrol lingkungan.
2	**ASHRAE TC 9.9 – Thermal Guidelines for Data Processing Environments**	Panduan suhu dan kelembapan ideal untuk ruang data, serta respon terhadap kegagalan pendinginan.
3	**ISO 22301:2019 Business Continuity Management System (BCMS)**	Referensi untuk memastikan kesinambungan layanan saat terjadi gangguan besar.
4	**ISO 50001:2018 Energy Management Systems**	Mengatur efisiensi dan optimalisasi penggunaan energi sistem pendingin.
5	**ISO 45001:2018 Occupational Health and Safety Management Systems**	Panduan keselamatan kerja bagi teknisi dan petugas maintenance HVAC.
6	**APJII Data Center Operation Manual**	Dokumen internal yang mengatur prosedur operasi harian sistem pendingin.
7	**SOP Emergency Response Plan (ERP) APJII Data Center**	Referensi untuk aktivasi rencana tanggap darurat bila suhu ruang IT melewati ambang batas kritis.

4. Definisi Istilah

Istilah	Definisi
HVAC (Heating, Ventilation and Air Conditioning)	Sistem mekanikal yang berfungsi menjaga suhu, kelembapan, dan sirkulasi udara di area data center.
Precision Air Conditioning (PAC)	Unit pendingin khusus untuk ruang IT dengan kontrol suhu dan kelembapan presisi tinggi.
CRAC/CRAH	*Computer Room Air Conditioner / Air Handler*, bagian dari sistem pendingin yang mendistribusikan udara dingin ke area rack server.

Istilah	Definisi
Major Failure	Gangguan besar yang menyebabkan lebih dari 50% kapasitas pendinginan utama tidak berfungsi atau menyebabkan suhu ruangan IT naik >3°C dalam waktu <10 menit.
Redundansi (N+1 / 2N)	Konsep ketersediaan cadangan unit HVAC agar tetap menjaga operasi meski terjadi kegagalan satu unit atau lebih.
Thermal Runaway	Kondisi peningkatan suhu ruangan secara cepat akibat kegagalan pendingin, berpotensi menyebabkan shutdown sistem IT.
Early Warning System (EWS)	Sistem pemantauan otomatis yang mengeluarkan peringatan dini bila suhu/kelembapan melebihi ambang batas normal.
Emergency Cooling Procedure	Prosedur darurat untuk mengaktifkan unit cadangan, membuka akses udara tambahan, atau melakukan ventilasi manual.
Incident Commander (IC)	Personel bertanggung jawab utama dalam koordinasi penanganan insiden HVAC.

5. Ruang Lingkup

Ruang lingkup SOP ini mencakup seluruh proses penanganan *major failure* sistem pendingin utama di **Data Center APJII**, termasuk aspek teknis, koordinasi, dan keselamatan kerja, dengan rincian sebagai berikut:

5.1 Area Cakupan

- Ruang Operasional Data Center APJII yang berlokasi di Gedung Cyber-1.

5.2 Jenis Gangguan yang Dicakup

- Kegagalan total atau sebagian unit pendingin utama (PAC/CRAC/Chiller/AHU).
- Gangguan kelistrikan yang menyebabkan HVAC berhenti beroperasi.
- Kerusakan sensor suhu/kelembapan yang mengakibatkan sistem kontrol tidak responsif.
- Kegagalan sistem kontrol BMS yang mengatur distribusi udara dingin.
- Kondisi suhu ruang data center mencapai atau melebihi 28°C selama >5 menit.
- Kegagalan simultan pada unit aktif dan cadangan (N+1 atau 2N redundancy gagal).
- Kebocoran refrigerant, drain, atau kondensat yang mengganggu fungsi sistem.

5.3 Pihak yang Terlibat

- **Team Operation Data Center APJII** (Shift Engineer, NOC Engineer)
- **Team Mechanical & Electrical Maintenance**
- **Team Safety / HSE Officer**
- **Team Vendor HVAC / OEM Support**

- **Facility Manager & Incident Commander (IC)**
- **Tim BCP / ERP Coordinator (jika eskalasi ke level darurat)**

5.4 Batasan Ruang Lingkup

SOP ini **tidak mencakup**:

- Kegagalan minor seperti alarm suhu sementara (<2°C dari setpoint) tanpa dampak signifikan.
- Pekerjaan pemeliharaan terjadwal (preventive maintenance).
- Gangguan non-HVAC seperti kebakaran, banjir, atau pemadaman listrik umum (yang diatur dalam SOP ERP dan SOP Power Failure).

6. Tanggung Jawab dan Kewenangan

6.1 Facility Manager (FM)

- Memastikan kesiapan seluruh sistem pendingin utama dan cadangan dalam kondisi operasional.
- Mengotorisasi aktivasi prosedur penanganan *major failure* HVAC.
- Menjadi penanggung jawab utama dalam koordinasi antar tim (operation, vendor, manajemen, dan BCP).
- Menyetujui tindakan pemulihan darurat dan koordinasi dengan pihak eksternal (kontraktor HVAC, OEM vendor).
- Menyampaikan laporan insiden ke Manajemen APJII maksimal 12 jam setelah kejadian.

6.2 Incident Commander (IC)

- Ditunjuk oleh Facility Manager saat kondisi *major failure* terdeteksi.
- Bertanggung jawab langsung dalam mengarahkan seluruh personel yang terlibat di lapangan.
- Memastikan prosedur keselamatan kerja diterapkan (lockout-tagout, APD, area isolation).
- Mengambil keputusan cepat dalam mitigasi sementara (misalnya: aktivasi unit cadangan, membuka airflow tambahan).
- Melakukan briefing dan *handover* selama setiap fase penanganan.

6.3 Shift Engineer / Operation Team

- Melakukan pemantauan suhu dan kelembapan ruang IT secara real-time melalui BMS atau sensor manual.
- Melaporkan secara segera bila suhu >28°C atau kelembapan >60% RH.
- Menginisiasi prosedur **Early Warning Notification** ke IC dan Facility Manager.
- Mengaktifkan **Emergency Cooling Procedure** sesuai instruksi IC.
- Melakukan logging detail setiap perubahan parameter HVAC selama insiden berlangsung.

6.4 Maintenance Team (M&E)

- Melakukan identifikasi penyebab kegagalan sistem pendingin (kelistrikan, mekanikal, refrigerant, dll).
- Melakukan perbaikan darurat (*temporary fix*) dan/atau *switch over* ke unit cadangan.
- Melakukan verifikasi status operasional seluruh unit PAC/CRAC setelah sistem dipulihkan.
- Memberikan laporan teknis ke Facility Manager dan IC.

6.5 HSE Officer

- Memastikan seluruh tindakan lapangan mengikuti standar keselamatan kerja (K3).
- Menyediakan peralatan APD, memastikan area kerja aman dari risiko kebocoran refrigerant atau panas ekstrem.
- Melakukan investigasi bila terjadi cedera atau insiden keselamatan selama penanganan.

6.6 Vendor HVAC / OEM Support

- Memberikan dukungan teknis onsite atau remote terkait troubleshooting sistem pendingin.
- Melakukan inspeksi dan perbaikan komponen utama (compressor, PCB, motor fan, sensor, dll).
- Menyediakan laporan hasil pemeriksaan teknis dalam waktu maksimal 24 jam pasca kejadian.

6.7 NOC / IT Operation Team

- Memantau dampak suhu terhadap performa perangkat IT.
- Mengaktifkan prosedur *server throttling* atau *load balancing* bila suhu kritikal tercapai.
- Melakukan koordinasi dengan tim jaringan dan server untuk mencegah shutdown mendadak.

7. Prosedur Pelaksanaan

7.1 Deteksi Awal (Early Warning Phase)

1. Sistem BMS atau sensor suhu mendeteksi kenaikan suhu ruang IT di atas ambang batas 25°C.
2. Alarm *High Temperature* aktif di NOC.
3. Shift Engineer memverifikasi status semua unit PAC/CRAC dari panel kontrol.
4. Jika lebih dari satu unit PAC berhenti atau performa menurun drastis, dikategorikan sebagai **Major Failure**.

7.2 Aktivasi Prosedur Darurat

1. Shift Engineer segera melaporkan ke IC dan Facility Manager.
2. IC mendeklarasikan status **Major Cooling Failure** dan mengaktifkan SOP ini.
3. Maintenance Team segera melakukan:
    - Pemeriksaan sumber daya listrik ke unit pendingin (MCB, ACB, MCCB).
    - Pemeriksaan tekanan refrigerant dan aliran udara.
    - Aktivasi unit cadangan (redundant PAC/CRAC).

    - Pembukaan *emergency ventilation door* (jika tersedia).
4. NOC Team menyiapkan rencana mitigasi beban IT (shutdown bertahap perangkat non-kritis).

7.3 Koordinasi dan Eskalasi

- Jika suhu ruangan terus naik >28°C selama lebih dari 10 menit:
    - Facility Manager melakukan eskalasi ke **Manajemen APJII dan BCP Team**.
    - Aktivasi **SOP Emergency Response Plan (ERP)** bila suhu mencapai >30°C.
    - Tim keamanan membantu isolasi area dan akses terbatas untuk personel HVAC.

7.4 Tindakan Pemulihan (Recovery Phase)

1. Setelah unit pendingin diperbaiki, dilakukan:
    - Uji fungsional (start-up, airflow, suhu return).
    - Pemantauan suhu ruang selama 30–60 menit.
2. Bila kondisi kembali stabil (<26°C), status *Major Failure* dinyatakan **ditutup sementara**.
3. Tim Maintenance menyusun rencana *root cause analysis* (RCA) dan *preventive action plan*.

7.5 Normalisasi

- Semua sistem HVAC dikembalikan ke konfigurasi normal (auto mode).
- BMS diverifikasi kembali untuk memastikan alarm dan sensor aktif normal.
- Handover laporan dari IC ke Facility Manager dan NOC untuk dokumentasi akhir.

8. Komunikasi dan Eskalasi

Level	Kondisi	Pihak Dihubungi	Waktu Maksimal
Level 1	Suhu naik >26°C, 1 unit PAC gagal	IC, Shift Engineer	0–5 menit
Level 2	Lebih dari 50% unit PAC gagal, suhu >28°C	Facility Manager, Maintenance Team	5–10 menit
Level 3	Semua unit pendingin gagal, suhu >30°C	Manajemen APJII, BCP Team, Vendor HVAC	≤15 menit
Level 4 (Critical)	Suhu >32°C selama >10 menit	Aktivasi ERP, shutdown bertahap beban IT non-kritis	≤20 menit

Semua komunikasi wajib dilakukan melalui jalur resmi (radio komunikasi, telepon darurat, atau aplikasi internal incident channel).

9. Dokumentasi dan Pelaporan

1. **Incident Log Sheet** harus diisi oleh Shift Engineer berisi:
    - Waktu kejadian, suhu, kelembapan, unit yang gagal, dan tindakan awal.
2. **Incident Report Form** disusun oleh Incident Commander mencakup:
    - Kronologi lengkap, penyebab sementara, dan dampak pada layanan.
3. **Technical Service Report (TSR)** dibuat oleh Vendor HVAC.
4. Semua dokumen dikompilasi dalam **Cooling System Incident File** dan diserahkan ke Facility Manager dalam waktu maksimal 24 jam.
5. Facility Manager menyiapkan **Summary Report** untuk manajemen APJII dan BCP Committee dalam 48 jam pasca insiden.

10. Pelatihan dan Sosialisasi

- Seluruh teknisi HVAC, NOC, dan Operation Engineer wajib mengikuti **pelatihan tahunan** penanganan *major failure* pendingin.
- Simulasi *Cooling Failure Drill* dilakukan minimal **2 kali per tahun**.
- Materi pelatihan meliputi:
    - Prosedur aktivasi darurat dan eskalasi.
    - Penggunaan alat ukur suhu dan kelembapan.
    - Keselamatan kerja dan penanganan refrigerant.
    - Prosedur komunikasi insiden dan pelaporan.
- Evaluasi hasil pelatihan dicatat dalam **Training Record Logbook**.

11. Evaluasi dan Review Pasca-Insiden

1. **Post-Incident Review (PIR)** dilaksanakan maksimal 5 hari kerja setelah kejadian.
2. Tim evaluasi terdiri dari:
    - Facility Manager
    - Incident Commander
    - Maintenance & HSE Officer
    - Vendor HVAC (jika relevan)
3. Evaluasi mencakup:
    - Analisis akar penyebab (*Root Cause Analysis*).
    - Efektivitas prosedur penanganan dan waktu pemulihan.
    - Dampak terhadap suhu, perangkat IT, dan layanan.
    - Rekomendasi tindakan pencegahan jangka panjang.
4. Hasil PIR dituangkan dalam **Cooling Failure Evaluation Report** dan menjadi bahan pembaruan SOP.

12. Peningkatan dan Perbaikan Berkelanjutan

- SOP ini direview **setiap 12 bulan sekali** atau setelah terjadi insiden signifikan.
- Perubahan atau revisi dilakukan berdasarkan:
    - Hasil *Post-Incident Review*.
    - Pembaruan standar TIA, ASHRAE, atau ISO.
    - Masukan dari tim operasional dan auditor eksternal.

- Versi terbaru SOP wajib disosialisasikan kepada seluruh personel operasional dan vendor terkait.
- Semua versi terdahulu disimpan dalam arsip dokumentasi resmi Data Center APJII dengan status **“Obsolete – for reference only.”**

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XIX
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PERAWATAN BERKALA FASILITAS DATA CENTER APJII

1. Pendahuluan

Data Center APJII merupakan infrastruktur kritikal yang harus selalu terjaga keandalannya. Perawatan berkala dilakukan untuk memastikan semua fasilitas, infrastruktur pendukung, serta sarana dan prasarana tetap berfungsi optimal sesuai standar. SOP ini disusun sebagai pedoman resmi dalam pelaksanaan perawatan fasilitas Data Center agar mendukung **availability, reliability, dan security** layanan anggota APJII.

2. Tujuan

- Menjamin ketersediaan (availability) dan keandalan (reliability) fasilitas Data Center.
- Mencegah terjadinya gangguan layanan akibat kerusakan fasilitas.
- Memberikan panduan sistematis pelaksanaan preventive, corrective, dan predictive maintenance.
- Menstandarkan prosedur pergantian perangkat dan komponen yang rusak.
- Menjaga kepatuhan pada standar internasional pengelolaan data center.

3. Dasar & Referensi Standar

- **ISO/IEC 27001**: Information Security Management.
- **ISO/IEC 27002**: Security Controls for Physical & Environmental Security.
- **TIA-942-C**: Telecommunications Infrastructure Standard for Data Centers.
- **ISO 22301**: Business Continuity Management System.
- **ASHRAE TC9.9**: Thermal Guidelines for Data Centers.
- **NFPA 70 / NEC**: Electrical Safety Standard.
- **APJII Internal Policies** terkait operasional Data Center.

4. Definisi Istilah

- **Preventive Maintenance (PM)**: Perawatan terjadwal secara rutin untuk mencegah kerusakan.
- **Corrective Maintenance (CM)**: Perawatan/perbaikan setelah terjadi kerusakan.
- **Predictive Maintenance (PdM)**: Perawatan berbasis analisis data (sensor, monitoring) untuk memprediksi kerusakan.

- **Infrastruktur Kritis**: Sistem kelistrikan, pendingin, keamanan, jaringan, dan proteksi kebakaran di Data Center.
- **Sarana & Prasarana**: Fasilitas pendukung (gedung, rak, sistem air, jalur kabel, tata udara).

5. Ruang Lingkup

SOP ini berlaku untuk:

1. **Manajemen Fasilitas Fisik & Infrastruktur Kritis**, meliputi:
    - Sistem listrik (UPS & Baterai, Panel Listrik, Grounding,).
    - Sistem pendingin (CRAC/CRAH, DX (Direct Expansion), precision AC).
    - Sistem keamanan fisik (CCTV, Access Control Door, Alarm).
    - Sistem pencegahan kebakaran (VESDA atau HSSD, gas suppression, fire extinguisher/APAR Class-C).
    - Sistem jaringan infrastruktur (kabel backbone, fiber, patch panel).
2. **Sarana & Prasarana**, meliputi:
    - Struktur gedung, lantai raised floor, plafon, pintu & kunci.
    - Jalur kabel (tray, ladder rack).
    - Ruang pendukung (NOC, Ruang UPS).
3. **Prosedur Perawatan & Pergantian Komponen**, baik untuk preventive, corrective, maupun predictive maintenance.

6. Prosedur Perawatan Berkala

6.1 Preventive Maintenance (PM)

Dilakukan secara **rutin & terjadwal** untuk mencegah kerusakan.

- **Frekuensi:** Harian, Mingguan, Bulanan, Triwulan, Tahunan.
- **Contoh Kegiatan:**
    - Pemeriksaan panel listrik & ACB.
    - Pembersihan filter AC presisi.
    - Uji sistem VESDA/HSSD & alarm kebakaran.
    - Pengecekan CCTV & access control door.
- **Dokumentasi:** Form checklist PM, ditandatangani oleh vendor, teknisi APJII & PIC/Penanggung Jawab Operasional DC APJII.

6.2 Corrective Maintenance (CM)

Dilakukan setelah terjadi **kerusakan atau anomali**.

- **Langkah-langkah:**
    1. Identifikasi kerusakan (alarm, monitoring system, laporan manual).
    2. Isolasi area/komponen yang rusak untuk mencegah gangguan lebih besar.
    3. Laksanakan perbaikan/pergantian komponen.
    4. Uji coba fungsi setelah perbaikan.
    5. Catat dalam logbook CM.
- **Contoh Kasus:**
    - UPS modul rusak → diganti modul baru.

- CRAC unit failure → diganti kompresor.
- Access card reader mati → diperbaiki/diganti.

6.3 Predictive Maintenance (PdM)

Dilakukan berbasis **analisis data sensor & monitoring** untuk memprediksi kegagalan.

- **Metode:**
  - Monitoring suhu & kelembapan real-time (IoT sensor).
  - Thermal imaging untuk mendeteksi panas berlebih di panel listrik.
  - Battery monitoring UPS untuk health check.
- **Tujuan:**
  - Mengantisipasi kegagalan sebelum terjadi.
  - Mengurangi downtime yang tidak terencana.

7. Manajemen Fasilitas Fisik & Infrastruktur

- **Listrik:** Dilakukan load balancing, UPS & battery testing.
- **Pendingin:** Pemeriksaan refrigerant, cleaning coil, kalibrasi sensor suhu & kelembapan yang dilakukan oleh pihak ketiga/vendor.
- **Keamanan:** Uji coba pengendalian akses pintu, audit rekaman CCTV, testing alarm yang dilakukan oleh pihak ketiga/vendor.
- **Proteksi Kebakaran:** Uji HSSD/VESDA bulanan, kalibrasi sensor asap, inspeksi silinder gas suppression yang dilakukan oleh pihak ketiga.
- **Jaringan:** Cek patch panel, Cross-Connect, fiber loss test, pembersihan konektor yang dilakukan oleh Tim Teknis APJII.

8. Prosedur Perawatan Sarana & Prasarana

1. **Ruangan Datahall/Data Center APJII**
   - Pengecekan secara visual terhadap sealed-dinding dan partisi dari kemungkinan adanya rembesan air.
   - Pengecekan secara visual adanya kontaminasi debu/residu di Rack MMR.
2. **Raised Floor & Jalur Kabel**
   - Cek stabilitas dan kelengkapan raised-floor, tray kabel (dilakukan per bulan).
   - Bersihkan dari debu untuk menghindari overheating.
3. **Ruang Pendingin**
   - Cek kelembapan & kebocoran pipa pembuangan air dari unit AC Presisi (dilakukan per bulan).
   - Cek Ducting Air-Flow.

9. Prosedur Perawatan & Pergantian Perangkat/Komponen Rusak

1. **Identifikasi** → laporan dari monitoring system / teknisi lapangan.
2. **Analisis** → tentukan apakah komponen perlu diperbaiki atau diganti.
3. **Approval** → PIC/Penanggung Jawab Operasional DC APJII menyetujui tindakan perbaikan/pergantian.
4. **Pelaksanaan** → Vendor melakukan penggantian dengan spare part resmi & sesuai standar.

5. **Testing** → uji coba perangkat untuk memastikan berfungsi normal.
6. **Dokumentasi** → update logbook PM (Preventive Maintenance), simpan berita acara pergantian.
7. **Disposal** → komponen rusak dibuang sesuai prosedur e-waste.

10. Dokumentasi & Pelaporan

- Semua aktivitas maintenance (PM, CM, PdM) wajib tercatat dalam **logbook & CMMS (Computerized Maintenance Management System)**.
- Laporan bulanan dikompilasi oleh **PIC/Penanggung Jawab Operasional DC APJII**.
- Audit internal dilakukan minimal **setahun sekali**.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XX
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

MATRIKS PERAWATAN BERKALA FASILITAS DATA CENTER APJII

Fasilitas	Daily	Weekly	Monthly	Quarterly (3 bulanan)	Yearly
Sistem Kelistrikan (UPS, Panel, Battery)	- Cek status panel listrik & indikator alarm. - Cek level baterai UPS di monitoring system.	- Uji beban ringan genset (tanpa load) & catat jam operasional. - Bersihkan area panel listrik dari debu.	- Uji beban genset dengan load dummy. - Cek tegangan, arus, frekuensi panel distribusi. - Cek sistem grounding.	- Tes baterai UPS (discharge test). - Kalibrasi metering panel listrik.	- Servis lengkap genset (oli, filter, radiator). - Infrared scan panel listrik (thermal imaging). - Load bank test UPS & genset.
Sistem Pendinginan (CRAC, Chiller, DX, AC Presisi, Piping)	- Monitoring suhu & kelembapan di ruang data hall. - Cek alarm AC presisi.	- Bersihkan filter AC presisi. - Periksa kebocoran air kondensasi.	- Kalibrasi sensor suhu & kelembapan. - Cek refrigerant level.	- Cuci coil pendingin & blower. - Uji performa cooling system.	- Servis besar unit AC presisi. - Pressure test pipa refrigerant.
Sarana & Prasarana (Gedung, Raised Floor, Kabel Tray, Ruang Pendukung)	- Cek kebersihan area (data hall, NOC, ruang genset).	- Bersihkan raised floor & jalur kabel dari debu.	- Periksa kondisi lantai, pintu, kunci akses.	- Audit kondisi struktur bangunan (plafon, dinding).	- Renovasi/perbaikan besar sarana fisik (pengecatan, penggantian karpet, lantai rusak).
Fire Protection (VESDA, HSSD,	- Cek indikator	- Tes manual alarm	- Cek tabung gas	- Uji simulasi	- Full system test fire suppression.

Fasilitas	Daily	Weekly	Monthly	Quarterly (3 bulanan)	Yearly
Alarm, Gas Suppression, Hydrant)	panel VESDA & fire alarm.	kebakaran di control panel.	suppression (tekanan & segel).	partial discharge VESDA. - Audit hydrant & APAR.	- Kalibrasi semua sensor asap & suhu.
Sistem Telekomunikasi (Fiber Backbone, Patch Panel, Distribution Frame)	- Monitoring link status via NMS.	- Cek patch cord & koneksi di rack.	- Bersihkan konektor fiber & copper.	- Loss test fiber optic link.	- Audit jaringan backbone & labeling kabel.
Keamanan Fisik (CCTV, Access Control, Alarm)	- Pastikan semua CCTV & access reader online.	- Review rekaman CCTV random.	- Tes sistem access control (biometrik, kartu).	- Uji panic button & alarm sistem.	- Audit total sistem security & upgrade firmware perangkat.

📌 Catatan Pelaksanaan

1. **Daily check** → dilakukan oleh teknisi on-duty (NOC & facility team).
2. **Weekly & Monthly** → dilakukan oleh teknisi fasilitas & vendor maintenance.
3. **Quarterly & Yearly** → dilakukan bersama vendor resmi, dokumentasi wajib disimpan.
4. Semua kegiatan dicatat dalam **logbook & CMMS (Computerized Maintenance Management System)** dengan checklist yang ditandatangani supervisor.
5. Jika ditemukan anomali → langsung dibuatkan tiket **Corrective Maintenance (CM)**.

Form Checklist Operasional Data Center APJII

1. Sistem Kelistrikan

Frekuensi	Item Pemeriksaan	Hasil (√/X)	Catatan Teknisi Supervisor
Daily	Panel listrik utama (indikator normal, tidak ada alarm)		
Daily	Status UPS (load %, alarm, battery health)		
Daily	Status genset (standby mode, level bahan bakar)		
Weekly	Uji start genset tanpa beban		
Weekly	Bersihkan ruang panel listrik & UPS		
Weekly	Cek kondisi baterai UPS (fisik, terminal, suhu)		
Monthly	Uji beban genset dengan load dummy		
Monthly	Battery UPS discharge test singkat		
Quarterly	Uji beban penuh genset (on-load test)		
Quarterly	Tes otomatisasi transfer switch (ATS)		
Yearly	Load bank test genset 4 jam		
Yearly	Ganti oli, filter udara & filter bahan bakar genset		
Yearly	Thermography panel listrik (deteksi hotspot)		

2. Sistem Pendinginan (Cooling System)

Frekuensi	Item Pemeriksaan	Hasil (√/X)	Catatan Teknisi Supervisor
Daily	Cek suhu & kelembapan ruang server (sesuai ASHRAE)		
Daily	Status AC Presisi (tidak ada alarm)		
Daily	Cek kebocoran air kondensasi		
Weekly	Bersihkan filter AC presisi		

Frekuensi	Item Pemeriksaan	Hasil (√/X)	Catatan Teknisi Supervisor
Weekly	Periksa level refrigerant		
Monthly	Kalibrasi sensor suhu & kelembapan		
Monthly	Cuci coil pendingin AC presisi		
Quarterly	Cuci coil kondensor & evaporator		
Quarterly	Balance airflow raised floor / aisle containment		
Yearly	Service besar kompresor AC presisi		
Yearly	Ganti filter udara AC presisi		
Yearly	Pressure test pipa refrigerant		

3. Fire Protection & Keamanan

Frekuensi	Item Pemeriksaan	Hasil (√/X)	Catatan Teknisi Supervisor
Daily	Panel alarm kebakaran (normal, tidak ada fault)		
Daily	CCTV online & rekaman aktif		
Daily	Access control berfungsi normal		
Daily	Lampu darurat menyala normal		
Weekly	Tes manual alarm kebakaran		
Weekly	Cek tabung APAR (tekanan, segel)		
Monthly	Tes fungsi VESDA/HSSD		
Monthly	Cek tabung suppression (tekanan, kondisi fisik)		
Quarterly	Uji integrasi sistem alarm & suppression		
Quarterly	Audit akses kontrol & database user aktif		
Yearly	Hydrostatic test tabung suppression		

Frekuensi	Item Pemeriksaan	Hasil (√/X)	Catatan Teknisi Supervisor
Yearly	Smoke test VESDA/HSSD		
Yearly	Uji evakuasi darurat (fire drill bersama tenant)		

4. Sarana & Prasarana

Frekuensi	Item Pemeriksaan	Hasil (√/X)	Catatan Teknisi Supervisor
Daily	Kebersihan ruang data hall		
Daily	Kondisi pintu & kunci ruang data center		
Daily	Raised floor rapi & tidak rusak		
Weekly	Bersihkan jalur kabel & ruang kerja		
Monthly	Audit struktural (raised floor, dinding, pintu)		
Monthly	Audit pencahayaan & emergency light		
Quarterly	Audit integritas struktur tambahan (ceiling, panel, wall)		
Yearly	Audit besar sarana prasarana (ruang, rak, containment)		
Yearly	Renovasi / penyesuaian kapasitas fasilitas		

5. Sistem Telekomunikasi & Monitoring

Frekuensi	Item Pemeriksaan	Hasil (√/X)	Catatan Teknisi Supervisor
Daily	Status link backbone & interkoneksi (NMS/BMS normal)		
Weekly	Cek log jaringan (traffic, error, alarm)		
Monthly	Kalibrasi sensor monitoring (BMS/EMS)		
Monthly	Audit kapasitas link utama & backup		
Quarterly	Uji failover backbone & perangkat core		

Frekuensi	Item Pemeriksaan	Hasil (√/X)	Catatan Teknisi Supervisor
Yearly	Audit menyeluruh sistem telekomunikasi		
Yearly	Uji DR test & BCP scenario		

📌 Catatan Penggunaan Form

- **Kolom hasil (√/X)**: diisi sesuai kondisi normal (√) atau ada temuan (X).
- **Catatan**: diisi bila ada anomali (misal: “tegangan tidak stabil”, “filter AC kotor”).
- **Teknisi**: tanda tangan setelah inspeksi.
- **Supervisor**: verifikasi & tanda tangan setelah validasi.
- Semua form dikumpulkan ke **CMMS/arsip digital** untuk audit & rekam jejak.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXI
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

MOP PREVENTIVE MAINTENANCE DATA CENTER APJII

1. Pendahuluan

Pemeliharaan infrastruktur Data Center APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) merupakan bagian dari upaya memastikan keandalan, ketersediaan, keamanan, dan keselamatan seluruh sistem penunjang operasional data center. Metode pelaksanaan pekerjaan pemeliharaan dilakukan melalui dokumen **MOP (Method of Procedure)** sebagai acuan pelaksanaan teknis oleh tim engineering, teknisi, dan vendor terkait.

MOP ini menetapkan prosedur pelaksanaan **Preventive Maintenance** terhadap seluruh infrastruktur utama dan pendukung, dengan interval waktu harian, mingguan, bulanan, triwulan, dan tahunan.

2. Tujuan

Tujuan utama penyusunan MOP ini adalah untuk:

1. Menetapkan metode pelaksanaan pemeliharaan yang aman, terukur, dan terdokumentasi.
2. Memastikan seluruh sistem infrastruktur berjalan sesuai dengan spesifikasi desain dan standar keandalan (availability).
3. Meminimalkan risiko downtime, gangguan, atau kerusakan akibat kegagalan peralatan.
4. Menjamin kegiatan pemeliharaan dilakukan dengan koordinasi lintas fungsi (Operations, Security, Network, dan Facility).
5. Memastikan hasil pemeliharaan terdokumentasi dalam logbook, CMMS (Computerized Maintenance Management System), atau sistem manajemen aset.

3. Dasar dan Referensi Standar

MOP ini disusun berdasarkan acuan standar nasional dan internasional, antara lain:

No	Standar / Dokumen Acuan	Deskripsi
1	**TIA-942-C**	Telecommunications Infrastructure Standard for Data Centers
2	**NFPA 70 / 75 / 76**	Electrical Safety & Fire Protection of IT Equipment
3	**ISO 30134**	Data Center Key Performance Indicators (PUE, WUE, REF, dll)
4	**ISO 20000-1:2018**	IT Service Management System
5	**ISO 27001:2022**	Information Security Management System
6	**ISO 22301:2019**	Business Continuity Management System
7	**ASHRAE TC9.9 Guidelines**	Thermal Guidelines for Data Center Equipment
8	**Vendor Manual & OEM Recommendations**	Manual teknis pabrikan (UPS, PAC, Fire Suppression, dsb.)
9	**SOP Layanan Data Center APJII**	Dokumen internal terkait operasional, keamanan, dan keselamatan

4. Definisi Istilah

Istilah	Definisi
MOP (Method of Procedure)	Dokumen resmi berisi langkah-langkah teknis pelaksanaan kegiatan pemeliharaan atau perubahan infrastruktur secara aman dan terkontrol.
Preventive Maintenance (PM)	Kegiatan pemeliharaan terjadwal untuk mencegah kerusakan, mempertahankan performa, dan memperpanjang usia peralatan.
PAC / CRAC / CRAH	Precision Air Conditioning / Computer Room Air Conditioning / Computer Room Air Handling – sistem pendingin ruangan data center dengan kontrol kelembapan dan suhu presisi.
PDU (Power Distribution Unit)	Perangkat distribusi daya ke rak server.
VESDA / HSSD	Very Early Smoke Detection Apparatus / High Sensitivity Smoke Detector – sistem deteksi asap sensitif untuk area kritikal.

Istilah	Definisi
Fire Suppression System	Sistem pemadam kebakaran otomatis berbasis gas (Novec 1230/FM200) atau inert gas (IG-55, IG-541).
Access Control System	Sistem kendali akses fisik ke area data center menggunakan biometrik, kartu, atau PIN.
CMMS (Computerize Maintenance Management System)	Sistem berbasis perangkat lunak untuk mengelola jadwal dan catatan pemeliharaan.

5. Ruang Lingkup

Ruang lingkup MOP ini mencakup **seluruh aktivitas Preventive Maintenance** terhadap sistem infrastruktur utama Data Center APJII, meliputi:

A. Sistem Kelistrikan

1. **UPS (Uninterruptible Power Supply)**
    - Pemeriksaan visual indikator, alarm, fan, suhu modul.
    - Pengukuran tegangan input/output.
    - Simulasi transfer beban (manual/otomatis) – tahunan.
    - Kalibrasi sensor dan controller – tahunan.
2. **Baterai**
    - Pemeriksaan visual kebocoran, korosi terminal.
    - Pengukuran tegangan dan resistansi internal – bulanan/triwulan.
    - Load test tahunan.
3. **PDU & Kabel Daya**
    - Pemeriksaan arus dan tegangan output PDU.
    - Pemeriksaan konektor, kabel, dan panel distribusi.
    - Pembersihan panel & tightening terminal – bulanan.
4. **Panel & Generator (Berkoordinasi dengan pihak Pengelola Gedung)**
    - Simulasi start otomatis genset (Auto Test) – mingguan.
    - Pemeriksaan bahan bakar, filter, pelumas – bulanan.
    - Load test tahunan.

B. Sistem Pendinginan (PAC / CRAC / CRAH)

1. **Harian**
    - Cek suhu & kelembapan ruangan.
    - Cek indikator alarm, display, dan kondisi filter.
2. **Mingguan**
    - Cek drain line & kondensasi air.
    - Bersihkan filter udara.

3. **Bulanan**
    - Cek refrigerant pressure, electrical connection, fan, dan belt.
4. **Triwulan**
    - Pengujian fungsi humidifier/dehumidifier.
    - Kalibrasi sensor suhu dan kelembapan.
5. **Tahunan**
    - General cleaning coil evaporator & condenser.
    - Penggantian filter dan refrigerant jika diperlukan.
    - Pengujian integrasi ke portal DCIM.

C. Sistem Fire Suppression

- Pemeriksaan tekanan tabung dan segel (bulanan).
- Kalibrasi panel kontrol alarm kebakaran (triwulan).
- Simulasi discharge tanpa gas (semi-tahunan).
- Uji fungsi interlock dengan Access Control & CRAC (tahunan).
- Verifikasi sertifikat tabung & masa berlaku gas (tahunan).

D. Sistem Access Control dan CCTV

- Pemeriksaan sensor pintu dan reader (mingguan).
- Pengujian alarm pintu terbuka, akses gagal, duplikasi kartu (bulanan).
- Backup konfigurasi controller (triwulan).
- Pengujian failover & integrasi ke BMS (tahunan).

E. Sistem VESDA / HSSD

- Pemeriksaan indikator alarm dan status sistem (mingguan).
- Tes fungsi fan aspirasi dan kalibrasi (triwulan).
- Uji fungsi sensor dengan smoke test (tahunan).
- Pembersihan pipa sampling dan manifold (tahunan).

F. Sistem Telekomunikasi (Fibre & Copper Infrastructure)

- Pemeriksaan fisik patch cord dan label (mingguan).
- Cek kualitas sinyal dan loss measurement (triwulan).
- Pembersihan port & ODF/MDF (triwulan).
- Uji continuity dan sertifikasi ulang kabel (tahunan).

6. Jenis dan Frekuensi Preventive Maintenance

Jenis Pemeliharaan	Frekuensi	Pelaksana	Contoh Aktivitas
Harian (Daily Check)	Setiap hari	Tim Teknis/NOC	Monitoring alarm, suhu, kelembapan, indikator sistem
Mingguan (Weekly)	Setiap minggu	Tim Teknis	Pemeriksaan visual, cleaning ringan
Bulanan (Monthly)	1x per bulan	Tim Teknis/Vendor	Pengukuran arus, tegangan, logbook update
Triwulan (Quarterly)	1x per 3 bulan	Vendor	Kalibrasi, pengujian sistem, cleaning berat
Tahunan (Annual)	1x per tahun	OEM/Vendor Resmi	General overhaul, load test, integrasi DCIM, uji fungsi penuh

7. Dokumentasi dan Pelaporan

1. Setiap kegiatan PM harus memiliki:
    - **Form MOP** yang berisi langkah-langkah kerja, risiko, mitigasi, dan PIC.
    - **Checklist Hasil PM** yang mencatat nilai pengukuran dan observasi.
    - **Laporan Akhir PM** (dalam format PDF/Excel) yang diserahkan ke PIC/Penanggung Jawab Operasional DC APJII.
2. Semua dokumen diunggah ke sistem **Portal DCIM**.
3. Temuan atau anomali dikategorikan dalam **Minor, Major, atau Critical**, dan ditindaklanjuti melalui **Work Order (WO)** atau **Incident Report (IR)**.

8. Keselamatan dan K3

- Gunakan APD (Alat Pelindung Diri) sesuai jenis pekerjaan: sarung tangan isolasi, safety shoes, goggles, ear protection.
- Pastikan pekerjaan dengan risiko tinggi (HV system, gas suppression) dilakukan dengan **Permit To Work (PTW)**.
- Lockout/Tagout (LOTO) wajib diterapkan pada pekerjaan listrik tegangan tinggi.
- Vendor wajib mengikuti **Safety Induction** APJII sebelum pelaksanaan pekerjaan.

9. Koordinasi dan Komunikasi

- Setiap pekerjaan MOP wajib mendapatkan **persetujuan PIC/Penanggung Jawab Operasional DC APJII** minimal **3 hari kerja sebelum pelaksanaan pekerjaan**.

- Pemberitahuan ke NOC dan PIC/Penanggung Jawab Operasional DC APJII dilakukan sebelum, selama, dan setelah pekerjaan.
- Laporan akhir pekerjaan dikirim kepada pihak PIC/Penanggung Jawab Operasional DC APJII dalam waktu maksimal **24 jam** setelah pekerjaan selesai.

10. Penutup

Dokumen ini menjadi acuan wajib bagi seluruh kegiatan pemeliharaan infrastruktur Data Center APJII. Setiap perubahan prosedur atau peralatan baru harus direvisi dan disetujui kembali oleh PIC/Penanggung Jawab Operasional DC APJII dan Manajemen APJII.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PREVENTIVE MAINTENANCE DATA CENTER APJII

1. Pendahuluan

SOP ini disusun untuk memastikan bahwa seluruh infrastruktur pendukung operasional Data Center APJII dapat berfungsi optimal, andal, aman, dan sesuai standar. Pemeliharaan dilakukan secara terencana dan terukur guna mencegah kegagalan sistem, mendukung ketersediaan layanan (availability), serta memperpanjang umur operasional peralatan.

SOP ini juga merupakan bagian integral dari sistem manajemen operasional fasilitas yang mendukung kepatuhan terhadap standar **TIA-942-C**, **ISO 27001 (Keamanan Informasi)**, **ISO 22301 (Business Continuity Management)**, **ISO 50001 (Manajemen Energi)**, serta **NFPA-75/76 (Fire Protection for IT Facilities)**.

2. Tujuan

Tujuan dari SOP ini adalah:

1. Menetapkan prosedur standar pelaksanaan kegiatan **Preventive Maintenance** (**PM**) pada seluruh sistem infrastruktur data center APJII.
2. Menjamin **keandalan sistem kelistrikan, pendinginan, keamanan, dan telekomunikasi** agar mendukung uptime operasional sesuai SLA.
3. Mencegah terjadinya **unplanned downtime** akibat kegagalan perangkat atau kelalaian perawatan.
4. Mendefinisikan **frekuensi, tanggung jawab, dan dokumentasi kegiatan pemeliharaan** untuk setiap sistem utama.
5. Memastikan kegiatan pemeliharaan sesuai dengan **spesifikasi teknis, rekomendasi pabrikan (OEM)**, serta **standar industri internasional**.

3. Dasar dan Referensi Standar

Pelaksanaan pemeliharaan mengacu pada standar berikut:

- **TIA-942-C** – Telecommunications Infrastructure Standard for Data Centers
- **ASHRAE TC 9.9** – Thermal Guidelines for Data Processing Environments
- **NFPA 70 (NEC)** – National Electrical Code
- **NFPA 75 & 76** – Fire Protection for IT Equipment & Telecommunications Facilities

- **ISO 27001:2022** – Information Security Management System (Annex A.11 – Physical and Environmental Security)
- **ISO 22301:2019** – Business Continuity Management System
- **ISO 50001:2018** – Energy Management System
- **Vendor Manual / OEM Maintenance Schedule** masing-masing perangkat
- **Kebijakan Internal Operasional Data Center APJII**

4. Definisi Istilah

Istilah	Definisi
Preventive Maintenance (PM)	Pemeliharaan terencana yang dilakukan secara berkala untuk mencegah kerusakan sistem.
UPS (Uninterruptible Power Supply)	Sistem penyedia daya listrik cadangan yang tanpa jeda bagi peralatan IT.
Battery Bank	Unit penyimpanan energi listrik yang mendukung UPS saat sumber utama padam.
PAC/CRAC/CRAH	Precision Air Conditioner / Computer Room Air Conditioner / Air Handler – sistem pendingin ruang data center.
VESDA/HSSD	Very Early Smoke Detection Apparatus / High Sensitivity Smoke Detection – sistem deteksi asap dini berbasis sampling udara.
Fire Suppression System	Sistem pemadam kebakaran otomatis.
Access Control System	Sistem kontrol akses fisik untuk pembatasan masuk area terbatas.
PDU	Power Distribution Unit – unit distribusi daya ke rak IT equipment.
SOP	Standard Operating Procedure, panduan prosedur kerja standar.

5. Ruang Lingkup

Ruang lingkup SOP ini mencakup seluruh kegiatan **Preventive Maintenance (PM)** terhadap infrastruktur pendukung data center APJII, yang terdiri dari:

1. **Sistem Kelistrikan**
    - UPS dan Battery Bank
    - Panel listrik (ACB, MCCB, MCB, DB)
    - Kabel daya dan konektor
    - PDU / Rack PDU
    - Grounding & Bonding System
2. **Sistem Pendinginan (HVAC)**
    - PAC / CRAC / CRAH Unit
    - Condenser Unit / DX Cooling / Air Cooled
    - Compressor, filter, sensor, dan ducting
    - Airflow management (cold aisle/hot aisle)

3. **Sistem Keamanan dan Keselamatan**
    - Fire Suppression System (FSS)
    - Fire Alarm System (FAS)
    - VESDA / HSSD System
    - Water Leak Detection System (WLDS)
    - Access Control System (ACS) dan CCTV
4. **Sistem Telekomunikasi dan Monitoring**
    - Rack Bersama di MMR
    - Portal DCIM
5. **Kegiatan Pemeliharaan**
    - Harian
    - Mingguan
    - Bulanan
    - Triwulanan (Quarterly)
    - Tahunan

6. Jenis & Frekuensi Pemeliharaan Preventive Maintenance

A. Harian

Dilakukan oleh Tim Teknis operasional on-site.

- Pemeriksaan visual sistem UPS (indikator, alarm, suhu ruangan baterai) untuk Rack MMR Bersama.
- Pemeriksaan visual terhadap sistem UPS yang dimiliki oleh Anggota/Tenant akan dilakukan oleh vendor/tim teknis dari Anggota/Tenant sendiri.
    - Catatan: Anggota/Tenant sangat disarankan untuk menggunakan tipe/jenis sistem UPS dari Pabrikan atau menggunakan sistem Smart UPS dan bukan sistem UPS rakitan (lihat lampiran-1).
- Pengecekan beban listrik dan suhu pada panel distribusi
- Monitoring temperatur & kelembapan ruang (melalui sistem monitoring)
- Pemeriksaan alarm FAS, VESDA/HSSD, PAC status
- Pemeriksaan akses pintu & CCTV online status
- Pencatatan log sheet operasional harian

B. Mingguan

- Uji fungsi manual alarm UPS & log event
- Pemeriksaan fan filter CRAC
- Pembersihan area CRAC return air grill
- Verifikasi kondisi terminal kabel utama dan konektor
- Tes alarm VESDA/HSSD sampling
- Uji alarm & sensor kebocoran air (WLDS)
- Verifikasi sistem komunikasi monitoring

C. Bulanan

- Tes transfer beban (load transfer test) UPS
- Pengukuran tegangan dan arus tiap fasa
- Pemeriksaan kapasitas baterai via load test ringan

- Pemeriksaan kebocoran refrigerant CRAC
- Pemeriksaan sensor suhu & RH
- Uji discharge alarm Fire Suppression tanpa aktivasi agent
- Tes akses kontrol dan log pengguna

D. Triwulanan (Quarterly)

- Pengujian kapasitas daya UPS dan kalibrasi sensor
- Pengujian ketahanan uji dari sistem Genset.
- Kalibrasi sensor sistem monitoring, suhu, dan kelembapan
- Pemeriksaan sistem VESDA/HSSD, sensor FAS, dan WLDS
- Pemeriksaan kondisi grounding dan resistansi (earth test)
- Pemeriksaan airflow balanced dan CRAC/PAC performance test

E. Tahunan

Dilakukan bersama vendor OEM dan kontraktor berlisensi.

- Load bank test UPS dan genset
- Battery impedance test & replacement (jika diperlukan)
- Penggantian filter udara CRAC/PAC
- Kalibrasi ulang semua sensor FAS & Monitoring sistem
- Pengujian penuh sistem Fire Suppression (Discharge Test)
- Pengujian ulang grounding system dan bonding
- Pembersihan menyeluruh Rack MMR Bersama dan Data Center secara umum
- Evaluasi kinerja sistem melalui trend log dari sistem monitoring selama 12 bulan terakhir

7. Dokumentasi & Pelaporan

Setiap kegiatan PM wajib:

- Dicatat dalam **Log Sheet Harian, Check Sheet, dan Work Order (WO)**
- Didokumentasikan dalam sistem tiket portal DCIM
- Disertai **Form Laporan PM** yang ditandatangani oleh Tim Teknis, Pihak Ketiga/Vendor, dan PIC/Penanggung Jawab Operasional DC APJII
- Semua hasil pengukuran (tegangan, suhu, kelembapan, resistansi, kapasitas baterai) disimpan minimal **5 tahun** untuk keperluan audit.

8. Evaluasi & Review

- Evaluasi hasil PM dilakukan setiap **bulan dan triwulan** oleh **PIC/Penanggung Jawab Operasional DC APJII**.
- Hasil analisis trend kinerja sistem digunakan untuk perencanaan **Predictive Maintenance** dan **Capex Replacement Plan**.
- SOP ini direview **setiap 12 bulan** atau setelah terjadi insiden besar, untuk disesuaikan dengan update standar atau kondisi lapangan.

Lampiran:

Tabel Checklist Preventive Maintenance Infrastruktur Data Center APJII

1. Sistem Kelistrikan – UPS dan Battery Bank

Frekuensi	Aktivitas Pemeliharaan	Tujuan / Keterangan	Penanggung Jawab	Bukti / Form
Harian	Periksa status display UPS (alarm, load, battery charge)	Memastikan UPS bekerja normal	Tim Teknis/NOC	Logsheet Harian
Harian	Monitor suhu ruang UPS dan baterai	Menjaga suhu sesuai standar (20–25°C)	Tim Teknis/NOC	Logsheet
Mingguan	Tes indikator alarm dan event log UPS	Deteksi dini anomali	Tim Teknis	Checklist Mingguan
Bulanan	Periksa koneksi terminal kabel UPS dan baterai	Cegah loose connection	Tim Teknis	Form PM Bulanan
Bulanan	Tes simulasi transfer beban bypass UPS	Verifikasi switching otomatis	Tim Teknis	Form PM Bulanan
Triwulan	Uji discharge parsial baterai	Evaluasi performa baterai	Vendor & Tim Teknis	Form PM Triwulan
Triwulan	Kalibrasi sensor suhu dan arus UPS	Akurasi pengukuran	Vendor	Laporan Kalibrasi
Tahunan	Load Bank Test UPS	Uji performa beban penuh	Vendor Resmi	Laporan Tahunan
Tahunan	Battery Impedance Test & penggantian jika perlu	Menjamin kapasitas optimal	Vendor	Laporan Baterai Tahunan

2. Sistem Pendinginan – CRAC/PAC/CRAH

Frekuensi	Aktivitas Pemeliharaan	Tujuan / Keterangan	Penanggung Jawab	Bukti / Form
Harian	Cek status alarm, suhu, RH di display CRAC	Memastikan suhu & kelembapan stabil	Tim Teknis/NOC	Logsheet Harian
Harian	Bersihkan filter udara luar CRAC	Menjaga airflow optimal	Tim Teknis/NOC	Logsheet
Mingguan	Periksa getaran, suara abnormal, dan kebocoran refrigerant	Deteksi kerusakan dini	Tim Teknis	Checklist Mingguan

Frekuensi	Aktivitas Pemeliharaan	Tujuan / Keterangan	Penanggung Jawab	Bukti / Form
Bulanan	Pembersihan coil evaporator dan kondensor	Efisiensi termal	Tim Teknis	Form PM Bulanan
Bulanan	Verifikasi kerja heater/humidifier	Stabilitas kelembapan	Tim Teknis	Form PM Bulanan
Triwulan	Uji kinerja CRAC (cooling load & return air temp)	Validasi kapasitas pendinginan	Vendor	Laporan PM
Triwulan	Kalibrasi sensor suhu & kelembapan	Ketepatan data BMS	Vendor	Laporan Kalibrasi
Tahunan	Servis besar (penggantian filter, oil check, pressure test)	Menjamin efisiensi tahunan	Vendor Resmi	Laporan Tahunan
Tahunan	Evaluasi airflow & containment performance	Optimasi efisiensi energi	Tim Teknis	Laporan Tahunan

3. Fire Suppression System

Frekuensi	Aktivitas Pemeliharaan	Tujuan / Keterangan	Penanggung Jawab	Bukti / Form
Harian	Cek indikator panel FAS & tekanan tabung agent	Pastikan sistem aktif & siap	Tim Teknis/NOC	Logsheet
Mingguan	Uji manual alarm & bell sounder	Uji fungsi sistem alarm	Tim Teknis	Checklist Mingguan
Bulanan	Periksa segel & valve actuator	Pastikan tidak ada kebocoran	Tim Teknis	Form PM
Triwulan	Tes integrasi FAS – BMS – HVAC shutdown	Validasi interlock sistem	Vendor	Laporan Integrasi
Tahunan	Full Discharge Test (rotasi antar area)	Uji nyata pemadaman agent	Vendor Resmi	Laporan Tahunan
Tahunan	Uji tekanan & berat isi tabung agent	Kepatuhan NFPA 2001	Vendor	Laporan Test Agent

4. Access Control System (ACS)

Frekuensi	Aktivitas Pemeliharaan	Tujuan / Keterangan	Penanggung Jawab	Bukti / Form
Harian	Verifikasi status online setiap pintu	Pastikan kontrol akses aktif	Tim Teknis/NOC	Logsheet
Mingguan	Tes fungsi reader, sensor pintu, dan lock	Pastikan sistem berfungsi normal	Tim Teknis	Checklist
Bulanan	Cek cadangan daya UPS ACS	Keandalan saat listrik padam	Tim Teknis	Form PM Bulanan
Triwulan	Review daftar akses & hak pengguna	Kepatuhan keamanan	Facility Security	Laporan Review
Tahunan	Kalibrasi pembaca kartu biometrik	Akurasi identifikasi	Vendor	Laporan Tahunan

5. CCTV System

Frekuensi	Aktivitas Pemeliharaan	Tujuan / Keterangan	Penanggung Jawab	Bukti / Form
Harian	Cek koneksi & tampilan setiap kamera	Pastikan semua aktif	Tim Teknis/NOC	Logsheet
Mingguan	Cek kebersihan lensa & housing kamera	Gambar tetap jernih	Tim Teknis	Checklist
Bulanan	Tes rekaman NVR dan playback	Pastikan data tersimpan	Tim Teknis	Form PM
Triwulan	Uji backup power & jaringan CCTV	Ketahanan sistem	Tim Teknis	Laporan
Tahunan	Upgrade firmware kamera & NVR	Keamanan & stabilitas sistem	Vendor	Laporan Tahunan

6. VESDA / HSSD System

Frekuensi	Aktivitas Pemeliharaan	Tujuan / Keterangan	Penanggung Jawab	Bukti / Form
Harian	Cek indikator panel VESDA/HSSD	Deteksi asap dini aktif	Tim Teknis/NOC	Logsheet

Frekuensi	Aktivitas Pemeliharaan	Tujuan / Keterangan	Penanggung Jawab	Bukti / Form
Mingguan	Uji alarm pre-warning & fire alarm stage	Pastikan sistem respon cepat	Tim Teknis	Checklist
Bulanan	Pembersihan dan kalibrasi sampling point	Cegah false alarm	Tim Teknis	Form PM
Triwulan	Tes integrasi VESDA – FAS – BMS	Sinkronisasi sistem	Vendor	Laporan Integrasi
Tahunan	Kalibrasi sensor laser dan pompa sampling	Ketepatan deteksi asap	Vendor	Laporan Kalibrasi

7. DCIM / BMS (Building Management System)

Frekuensi	Aktivitas Pemeliharaan	Tujuan / Keterangan	Penanggung Jawab	Bukti / Form
Harian	Monitor dashboard BMS/DCIM	Pantau status perangkat	Tim Teknis/NOC	Logsheet
Mingguan	Cek komunikasi node sensor	Pastikan data real-time	Tim Teknis	Checklist
Bulanan	Backup data trend log & konfigurasi	Mencegah kehilangan data	Tim Teknis	Form PM
Triwulan	Uji fungsi alarm dan notifikasi otomatis	Validasi sistem alert	Vendor	Laporan PM
Tahunan	Update firmware dan patch sistem DCIM	Keamanan sistem	Vendor	Laporan Tahunan

8. Sistem Telekomunikasi & Distribusi Jaringan

Frekuensi	Aktivitas Pemeliharaan	Tujuan / Keterangan	Penanggung Jawab	Bukti / Form
Harian	Cek status link backbone	Ketersediaan koneksi	Tim Teknis/NOC	Logsheet
Mingguan	Tes patchcord dan labeling port	Validasi koneksi fisik	Tim Teknis	Checklist
Bulanan	Verifikasi patch panel & tray kabel	Keamanan & kerapihan instalasi	Tim Teknis	Form PM

Frekuensi	Aktivitas Pemeliharaan	Tujuan / Keterangan	Penanggung Jawab	Bukti / Form
Triwulan	Fiber OTDR test dan UTP certification	Menilai kualitas link	Vendor	Laporan PM
Tahunan	Audit kabel data & dokumentasi labeling	Standarisasi TIA-942 compliance	Engineer	Laporan Tahunan

9. Dokumentasi Pendukung

Dokumen	Keterangan	Retensi
Logsheet Operasional Harian	Pemantauan suhu, RH, alarm, beban	5 tahun
Checklist PM	Bukti kegiatan PM tiap periode	5 tahun
Laporan Kalibrasi & Uji Beban	Bukti hasil test tahunan	5 tahun
Foto Dokumentasi PM	Bukti fisik hasil perawatan	3 tahun
Sertifikat Vendor / OEM	Bukti kepatuhan standar	5 tahun

10. Catatan Khusus

- Semua kegiatan PM harus dijadwalkan melalui WhatsApp, Email dan/atau **portal DCIM APJII** dan mendapat **approval dari PIC/Penanggung Jawab Operasional DC APJII.**
- Pekerjaan tahunan yang berdampak downtime harus melalui proses persetujuan **PIC/Penanggung Jawab Operasional DC APJII**.
- Setiap vendor wajib menyerahkan **Laporan Hasil Pekerjaan (BAST + PM Report)** setelah kegiatan triwulan dan tahunan PM.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXIII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP MANAJEMEN FASILITAS (KEBERSIHAN & TATA RUANG) DATA CENTER APJII

1. Pendahuluan

Data Center APJII merupakan infrastruktur kritikal yang menampung perangkat jaringan, server, serta sistem pendukung layanan internet nasional. Untuk menjamin keandalan dan keberlangsungan operasional, diperlukan manajemen fasilitas yang baik khususnya pada aspek **kebersihan, tata ruang, dan pengelolaan limbah**. SOP ini disusun untuk memberikan panduan standar dalam menjaga kualitas lingkungan Data Center agar sesuai dengan praktik terbaik internasional.

2. Tujuan

- Menjamin kondisi kebersihan dan tata ruang Data Center tetap sesuai standar internasional.
- Mengurangi risiko gangguan operasional akibat debu, kelembaban, dan limbah kabel.
- Meningkatkan efisiensi alur kerja dengan penataan fasilitas dan ruang yang teratur.
- Memberikan pedoman kepada staf APJII, tenant, dan vendor terkait tanggung jawab kebersihan area masing-masing.

3. Dasar & Referensi Standar

- **ISO/IEC 27001** – Information Security Management System (Physical & Environmental Security).
- **ISO/IEC 14763-2** – Implementation and Operation of Customer Premises Cabling (Housekeeping & Cabling Management).
- **TIA-942-C** – Telecommunications Infrastructure Standard for Data Centers (Facility & Space Planning).
- **ASHRAE TC9.9** – Environmental Guidelines for Data Centers.
- Kebijakan Internal APJII terkait pengelolaan fasilitas dan housekeeping.

4. Definisi Istilah

- **Rack Tenant**: Rak server milik anggota/tenant yang berada di dalam Data Center APJII.
- **MMR (Meet Me Room)**: Ruangan khusus interkoneksi antar-tenant dan backbone jaringan.
- **Housekeeping**: Kegiatan kebersihan rutin meliputi pembersihan lantai, dinding, ceiling, serta peralatan.
- **Waste Management**: Proses pengelolaan limbah termasuk kabel bekas, material elektronik, dan benda berbahaya.
- **HAZMAT (Hazardous Material)**: Bahan limbah berbahaya seperti kabel PVC, baterai UPS, atau cairan pendingin.

5. Ruang Lingkup

SOP ini berlaku untuk seluruh area operasional Data Center APJII, mencakup:

1. Kebersihan **Rack Anggota/Tenant**.
2. Kebersihan **Rack MMR Bersama**.
3. Kebersihan **Area Umum Data Center** (lantai, lorong, ceiling, CRAC/PAC unit).
4. **Waste Management** (pengelolaan limbah kabel, elektronik, dan bahan berbahaya).

6. Kebersihan Rack Anggota/Tenant

1. **Tanggung Jawab**:
    - Anggota/Tenant bertanggung jawab terhadap kebersihan dan kerapihan di dalam rak masing-masing (cabling system).
2. **Prosedur**:
    - Anggota/Tenant wajib menutup panel blanking pada slot kosong untuk menghindari akumulasi debu & menjaga aliran udara.
    - Pembersihan perangkat Anggota/Tenant hanya boleh dilakukan oleh **Authorized Personnel** dari pihak Anggota/Tenant.
    - Sistem perkabelan Anggota/Tenant wajib ditata dengan rapih dan tidak boleh menutupi fisik perangkat yang berada di dalam rak.
    - Aktivitas housekeeping atau pekerjaan yang akan dilakukan oleh Anggota/Tenant wajib dijadwalkan dan diinformasikan ke NOC APJII minimal **H-2**.

7. Kebersihan Rack MMR Bersama

1. **Tanggung Jawab**:
    - Tim Teknis APJII bertanggung jawab penuh atas kebersihan dan kerapihan rack bersama baik itu sistem perkabelan yang berada di depan rack MMR bersama dan yang berada di belakang rack MMR bersama.

- Vendor/Tenaga Kontrak Kerja hanya boleh melakukan pekerjaan/perapihan sistem perkabelan di MMR bersama dengan izin resmi dan mendapatkan Work Order dari NOC untuk melakukan dismantle atau melakukan penarikan kabel baru.

2. **Prosedur**:
   - Pembersihan Rack MMR bersama dilakukan rutin setiap **minggu** menggunakan **vacuum anti-static** terhadap kontaminasi debu.
   - Patch cord/Kabel yang tidak digunakan wajib dicabut & dipindahkan ke area penyimpanan kabel bekas.
   - Labelisasi kabel wajib dilakukan sesuai standar APJII (kode warna & nomor port).
   - Perapihan terhadap sistem perkabelan mengacu ke SOP Interkoneksi DC APJII.\

8. Kebersihan Area Data Center Secara Umum

1. **Frekuensi Kebersihan**:
   - Harian: Melakukan Pembersihan & Perapihan dari bahan-bahan material yang berada di atas raised-floor dengan menggunakan Vacuum HEPA Filter.
   - Mingguan: Pembersihan & Perapihan area lorong dingin & lorong panas (cold aisle & hot aisle).
   - Bulanan: Pembersihan & Perapihan di bawah raised floor, ceiling, sensor monitoring, PAC/CRAC unit filter yang dilakukan oleh pihak ketiga/vendor.
   - Tahunan: General cleaning (deep cleaning) seluruh area Data Center.
2. **Larangan**:
   - Tidak diperkenankan menggunakan sapu biasa atau kain basah yang meninggalkan residu (Non Bebas Serat/Non-Lint-Free) dan tidak diperkenankan menggunakan kain Non-Anti Statis (Non-ESD Free).
   - Tidak boleh ada makanan, minuman, atau benda asing di dalam ruang Data Center.
   - Setiap kegiatan pembersihan & perapihan wajib didampingi oleh Tim Teknis **APJII**.

9. Waste Management (Pengelolaan Limbah Kabel & Bahan Berbahaya)

1. **Identifikasi Limbah**:
   - Limbah kabel bekas (PVC, fiber, copper).
   - Material elektronik rusak (switch, server, power supply).
   - Baterai UPS bekas dan cairan refrigerant (kategori B3).
2. **Prosedur Pengelolaan Limbah**:
   - Kabel bekas wajib dipotong dan ditempatkan di wadah tertutup khusus.
   - Limbah elektronik dikumpulkan di gudang sementara dengan label **E-Waste**.
   - Baterai dan refrigerant hanya boleh ditangani oleh vendor bersertifikat B3 (Bahan Berbahaya & Beracun).
3. **Penyimpanan & Transportasi**:
   - Limbah Elektronik dan B3 disimpan maksimal **6 bulan** sebelum diserahkan ke pihak ketiga berizin (vendor pengelola limbah B3).

    - Semua proses harus sesuai dengan **Peraturan Pemerintah RI tentang Pengelolaan Limbah B3**.
4. **Dokumentasi & Audit**:
    - Setiap pengelolaan limbah dicatat dalam **Logbook Waste Management**.
    - Audit dilakukan minimal **2 kali setahun** oleh tim Internal Audit APJII.

10. Catatan & Dokumentasi

- Laporan kebersihan dan perapihan rutin harian, mingguan, bulanan, dan tahunan harus terdokumentasi dalam **Tim Teknis Maintenance Logbook**.
- Logbook waste management disimpan minimal **5 tahun** sebagai bagian dari kepatuhan audit.
- Semua kegiatan kebersihan dan waste management wajib sesuai standar K3 dan ISO 14001 (Environmental Management).

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

Contoh Checklist Operasional Manajemen Fasilitas Data Center APJII

1. Contoh Checklist Harian

No	Aktivitas	Area	Metode	PIC	Status (✓/✗)	Catatan
1	Pembersihan lantai raised floor dari debu	Data Hall	Vacuum anti-static	Housekeeping		
2	Pemeriksaan kondisi lorong dingin & panas (tidak ada barang asing)	Cold/Hot Aisle	Visual check	Security & Tim Teknis		
3	Pemeriksaan tidak ada makanan/minuman	Seluruh area	Visual check	Security		
4	Pemeriksaan kebersihan rak tenant (tidak ada kabel jatuh/berserakan)	Rack Tenant	Visual check	NOC + Tenant escort		
5	Pemeriksaan area MMR bebas kabel tidak terpakai	MMR	Visual check	Tim Teknis		

2. Contoh Checklist Mingguan

No	Aktivitas	Area	Metode	PIC	Status (✓/✗)	Catatan
1	Pembersihan lorong cold aisle & hot aisle	Data Hall	Vacuum anti-static	Housekeeping		
2	Pembersihan rak MMR bersama	MMR	Vacuum anti-static	Facility		
3	Pengecekan patch cord idle (tidak digunakan)	MMR	Visual check + labeling	NOC		

No	Aktivitas	Area	Metode	PIC	Status (✓/✗)	Catatan
4	Pemeriksaan panel blanking pada rack tenant	Rack Tenant	Visual check	Tenant escort + Facility		
5	Pembersihan area resepsionis & ruang tunggu	Area Umum	Vacuum + lap kering	Housekeeping		

3. Contoh Checklist Bulanan

No	Aktivitas	Area	Metode	PIC	Status (✓/✗)	Catatan
1	Pembersihan ceiling & sensor (HSSD/VESDA, WLDS)	Data Hall	Vacuum + brush anti-static	Facility		
2	Pembersihan filter PAC/CRAC unit	Cooling Room	Filter cleaning	Facility + Vendor AC		
3	Audit penataan kabel tenant & MMR	Rack & MMR	Visual check + dokumentasi	NOC + Facility		
4	Pemeriksaan kondisi lantai raised floor (panel longgar/rusak)	Data Hall	Visual & mekanis	Facility		
5	Pemeriksaan gudang penyimpanan limbah kabel/elektronik	Gudang Limbah	Visual check	Facility		

4. Contoh Checklist Tahunan

No	Aktivitas	Area	Metode	PIC	Status (✓/✗)	Catatan
1	**General deep cleaning** seluruh area Data Center	Semua area	Jasa cleaning khusus data center (anti-static)	Vendor + Facility		
2	**Audit lengkap waste management** (kabel, baterai UPS, refrigerant)	Gudang & Storage	Audit + dokumentasi	Facility + Auditor Internal		
3	Pemeriksaan kondisi fisik raised floor (pengangkatan panel total & cleaning bawah lantai)	Data Hall	Deep clean	Vendor + Facility		
4	Pemeriksaan total tata ruang (racking, cold/hot aisle, clearance)	Semua area	Site survey	Facility + NOC		
5	Evaluasi kontrak vendor housekeeping & limbah B3	Manajemen APJII	Review kontrak	Management		

Contoh Logbook Manajemen Fasilitas Data Center APJII

1. Contoh Identitas Logbook

- **Nama Fasilitas / Data Hall** : _____
- **Tanggal Pemeriksaan** : _____
- **Waktu Pemeriksaan** : _____
- **PIC Pemeriksa** : _____
- **Shift** : ☐ Pagi ☐ Siang ☐ Malam

2. Contoh Checklist Operasional

No	Aktivitas	Area	Frekuensi (H/M/B/T)	Status (✓/✗)	Catatan Temuan	Tindak Lanjut	Nama & Tanda Tangan PIC
1	Pembersihan lantai raised floor	Data Hall	H				
2	Pemeriksaan cold/hot aisle (barang asing, kabel jatuh)	Data Hall	H				
3	Pembersihan rack MMR bersama	MMR	M				
4	Pembersihan filter PAC/CRAC unit	Cooling Room	B				
5	Audit penataan kabel tenant & patch panel	Rack Tenant & MMR	B				
6	General deep cleaning & audit limbah B3	Seluruh Area	T				

Keterangan Frekuensi:

- H = Harian
- M = Mingguan
- B = Bulanan
- T = Tahunan

3. Contoh Temuan Khusus

📌 (Diisi jika ada kondisi abnormal, misalnya debu berlebih, kabel semrawut, panel raised floor longgar, tumpukan limbah kabel, dll.)

- _____
- _____
- _____

4. Contoh Tindak Lanjut & Status

📌 (Dicatat oleh supervisor/APJII terkait aksi korektif atau perbaikan)

- _____
- _____
- _____

5. Contoh Verifikasi & Approval

Jabatan	**Nama**	**Tanda Tangan**	**Tanggal**
Petugas Housekeeping			
Petugas Facility/NOC			
Supervisor APJII			

LAMPIRAN XXIV
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP KEAMANAN FISIK DATA CENTER APJII

1. Pendahuluan

Keamanan fisik Data Center merupakan salah satu faktor kritikal dalam menjamin keberlangsungan layanan dan integritas infrastruktur yang dikelola APJII. SOP ini disusun untuk memastikan bahwa setiap individu maupun barang yang keluar-masuk Data Center mengikuti standar keamanan ketat yang berlaku, sehingga dapat mencegah potensi ancaman, penyalahgunaan, maupun insiden keamanan lainnya.

2. Tujuan

- Menetapkan standar keamanan fisik di area Data Center APJII.
- Menjamin hanya individu yang berwenang dapat masuk dan melakukan aktivitas di Data Center.
- Mengatur prosedur pemeriksaan visitor, barang bawaan, dan kartu akses.
- Menyediakan mekanisme hak akses darurat sesuai kebutuhan operasional.

3. Dasar & Referensi Standar

- **ISO/IEC 27001** – Information Security Management Systems.
- **ISO/IEC 27002** – Controls for Physical & Environmental Security.
- **ISO 22301** – Business Continuity Management Systems.
- **TIA-942-C** – Data Center Standard (Facility & Security).
- Kebijakan Internal APJII tentang Pengelolaan Data Center.

4. Definisi Istilah

- **Visitor**: Individu dari luar APJII yang berkunjung ke Data Center (tenant, vendor, kontraktor, atau tamu).
- **Hak Akses**: Izin resmi yang diberikan untuk memasuki area Data Center.
- **Kartu Akses**: Kartu identifikasi resmi yang digunakan untuk otorisasi akses fisik.
- **Hak Akses Darurat**: Otorisasi khusus yang diberikan dalam kondisi mendesak dengan prosedur tertentu.
- **Barang Bawaan**: Perangkat, alat kerja, atau benda lain yang dibawa masuk/keluar oleh visitor.

5. Ruang Lingkup

SOP ini berlaku untuk seluruh aktivitas yang melibatkan:

- Pengecekan visitor sebelum memasuki Data Center.
- Pengecekan barang bawaan masuk dan keluar.
- Prosedur pemeriksaan keamanan fisik.
- Prosedur verifikasi hak akses visitor.
- Prosedur hak akses normal dan hak akses darurat.
- Penggunaan kartu akses selama berada di area Data Center.

6. Prosedur Keamanan Fisik

6.1 Pengecekan Visitor Sebelum Masuk

1. Visitor wajib mendaftar di pos keamanan/lobi dengan menunjukkan identitas diri asli (KTP, SIM, atau paspor).
2. Petugas keamanan memeriksa apakah visitor sudah memiliki **konfirmasi hak akses**.
3. Visitor yang tidak terdaftar atau tanpa konfirmasi tidak diperbolehkan masuk.

6.2 Pengecekan Barang Bawaan

1. Semua barang bawaan diperiksa secara fisik oleh petugas keamanan.
2. Barang-barang elektronik, perangkat jaringan, dan alat kerja harus tercantum dalam **Formulir Barang Bawaan**.
3. Saat keluar, barang bawaan dicocokkan kembali dengan daftar yang tercatat pada saat masuk.
4. Barang yang tidak sesuai akan ditahan hingga ada klarifikasi dari pemilik sah atau tenant.

6.3 Pemeriksaan Keamanan

1. Semua visitor melewati **detektor logam** atau pemeriksaan manual oleh petugas.
2. Dilarang membawa makanan, minuman, senjata, bahan kimia berbahaya, atau perangkat perekam tanpa izin tertulis.
3. Jika ada temuan mencurigakan, visitor tidak diizinkan masuk sebelum mendapat persetujuan Data Center Manager.

6.4 Pengecekan Hak Akses Visitor

1. Visitor wajib **mengajukan hak akses paling lambat H-1** sebelum kunjungan.
2. Hak akses hanya berlaku untuk area tertentu dan memiliki **batas waktu kunjungan**.
3. Visitor wajib membawa identitas asli yang **sesuai dengan data hak akses**.
4. Hak akses diverifikasi di sistem **Visitor Management System (VMS)**.
5. Jika ada ketidaksesuaian maka akses ditolak.

6.5 Konfirmasi Hak Akses

1. Visitor hanya dapat masuk setelah menerima **konfirmasi hak akses** melalui Portal Pusat Layanan APJII.

2. Petugas keamanan hanya mengizinkan visitor yang ada dalam daftar konfirmasi.
3. Kartu akses diberikan sesuai durasi kunjungan dan harus dikembalikan setelah keluar.

6.6 Penggunaan Kartu Akses

1. Kartu akses wajib dipakai dan terlihat jelas selama berada di area Data Center.
2. Kartu akses **tidak boleh dipinjamkan** kepada orang lain.
3. Kartu akses visitor/vendor hanya berlaku untuk jangka waktu tertentu sesuai konfirmasi.
4. Kehilangan kartu akses harus segera dilaporkan ke petugas keamanan.

7. Prosedur Hak Akses Darurat

7.1 Kondisi Darurat

Hak akses darurat dapat diberikan hanya dalam kondisi:

- Kegagalan layanan kritikal tenant.
- Kebutuhan pemeliharaan segera yang tidak dapat ditunda.
- Permintaan resmi dari anggota/tenant dengan urgensi tinggi.

7.2 Prosedur Mendapatkan Hak Akses Darurat

1. Visitor membawa **surat resmi** dari perusahaan tenant/anggota yang menjelaskan kebutuhan darurat.
2. Visitor membawa **identitas diri yang masih valid** (KTP, SIM, paspor).
3. NOC APJII melakukan verifikasi cepat dengan pihak tenant terkait.
4. Jika disetujui, Data Center Manager atau pejabat berwenang memberikan otorisasi.
5. Visitor diberikan **kartu akses darurat** yang berlaku hanya untuk periode tertentu (maksimal 1 hari).
6. Setelah pekerjaan selesai, kartu akses wajib dikembalikan.

8. Catatan & Dokumentasi

- Semua aktivitas visitor dicatat dalam **Visitor Management System (VMS)**.
- Log akses kartu disimpan minimal **2 tahun** untuk kepentingan audit.
- Semua hak akses darurat dilaporkan ke Data Center Manager untuk evaluasi bulanan.

9. Patroli Berkala di Area Data Center

1. **Tujuan Patroli**
    - Memastikan kondisi area Data Center aman dari potensi ancaman fisik.
    - Menjamin bahwa semua individu yang berada di dalam area sesuai otorisasi.
    - Mencegah tindakan yang mencurigakan atau melanggar SOP.
2. **Frekuensi Patroli**
    - Minimal dilakukan **setiap 2 jam sekali** oleh petugas keamanan.
    - Intensitas patroli ditingkatkan pada jam kerja vendor/visitor atau saat maintenance berlangsung.

3. **Area Patroli**
    - Perimeter luar Data Center (pagar, parkir, akses masuk).
    - Lobi, ruang resepsionis, ruang meeting.
    - Area kritikal (server hall, ruang listrik, ruang UPS, ruang genset, ruang PAC).
    - Jalur evakuasi & area darurat.
4. **Dokumentasi Patroli**
    - Setiap patroli dicatat pada **Log Book Patroli Keamanan**.
    - Jika ada temuan mencurigakan, wajib dibuatkan **Incident Report** dan segera dilaporkan ke Data Center Manager.

10. Kewajiban Penggunaan Kartu Hak Akses

1. **Visitor wajib menggunakan kartu hak akses** yang diberikan selama berada di area Data Center.
2. Kartu harus selalu terlihat jelas (dipakai di dada dengan lanyard).
3. Kartu tidak boleh dipindahtangankan.
4. Kartu akses visitor harus dikembalikan saat keluar dari Data Center.

11. Batasan Waktu Kunjungan

1. Visitor hanya diperbolehkan berada di Data Center sesuai dengan **durasi kunjungan** yang sudah disetujui dalam hak akses.
2. Jika waktu kunjungan telah habis, visitor wajib segera meninggalkan area Data Center.
3. Perpanjangan waktu kunjungan harus mendapat persetujuan tambahan dari Customer Service dan Data Center Manager.

12. Zona Akses Berdasarkan Color Coding

Setiap karyawan APJII, tenant, vendor, maupun visitor wajib mematuhi **Zona Akses** sesuai warna kartu hak akses:

Warna Kartu	Kategori	Area Akses
● **Merah**	Restricted Area / Critical Area	Ruang server, ruang listrik, ruang UPS – hanya authorized personnel tertentu
● **Biru**	Staff Operasional / Engineer	Area teknis & operasional sesuai tugas
□ **Hijau**	Tenant / Customer / Klien	Rak/ruang tenant sesuai kontrak layanan
□ **Kuning**	Vendor / Kontraktor	Area kerja sesuai izin kerja & didampingi
○/● **Putih/Abu-Abu**	Visitor / Guest / Tamu	Area resepsionis, ruang meeting, area terbatas dengan escort

Warna Kartu	Kategori	Area Akses
●/✨ **Hitam/Emas**	Security / Emergency Access	Seluruh area, khusus untuk pengamanan & keadaan darurat

13. Monitoring Perilaku Visitor

1. Petugas keamanan wajib **memastikan visitor tidak melakukan tindakan mencurigakan**, seperti:
    - Mengambil foto/video tanpa izin.
    - Membuka perangkat atau rak yang tidak berwenang.
    - Membawa barang keluar tanpa izin.
    - Berada di area di luar zona akses yang diperbolehkan.
    - Melakukan interaksi tidak sah dengan perangkat ICT.
2. Jika ditemukan tindakan mencurigakan:
    - Visitor segera dihentikan dan diamankan.
    - Dilaporkan ke Data Center Manager dan, bila perlu, ke pihak berwenang.
    - Dicatat dalam **Incident Log**.

Alur Akses Data Center APJII

1. Alur Akses Normal (Standard Access)

Tahapan Proses

1. **Pengajuan Hak Akses (H-1 sebelum kunjungan)**
    - Visitor/tenant/vendor mengirim **Formulir Permohonan Akses** + identitas diri.
    - NOC APJII melakukan verifikasi ke tenant/anggota.
2. **Konfirmasi Hak Akses**
    - Jika disetujui maka hak akses dicatat dalam **Visitor Management System (VMS)**.
    - Visitor menerima notifikasi konfirmasi (email/tertulis).
3. **Kedatangan ke Data Center**
    - Visitor datang ke pos keamanan/lobi.
    - Menunjukkan **identitas asli** (KTP/SIM/Passport).
4. **Pemeriksaan Awal**
    - Petugas keamanan mencocokkan identitas dengan daftar konfirmasi VMS.
    - Pemeriksaan keamanan (detektor logam, body check bila diperlukan).
5. **Pengecekan Barang Bawaan**
    - Barang dicatat dalam **Formulir Barang Bawaan**.
    - Jika membawa perangkat kerja → diverifikasi sesuai permohonan.
6. **Penerbitan Kartu Akses**
    - Visitor diberikan **kartu akses sementara** (warna merah untuk tamu/vendor).
    - Berlaku hanya untuk area yang diizinkan dan durasi tertentu.
7. **Pendampingan**
    - Vendor/kontraktor wajib didampingi oleh NOC APJII.
8. **Akses ke Data Center**
    - Visitor masuk sesuai area otorisasi.
    - Wajib mengenakan kartu akses yang terlihat jelas.

9. **Keluar dari Data Center**
    - Barang bawaan diperiksa ulang dan dicocokkan dengan daftar saat masuk.
    - Visitor mengembalikan kartu akses sementara.
    - Exit dicatat dalam VMS.

2. Alur Akses Darurat (Emergency Access)

Tahapan Proses

1. **Pengajuan Hak Akses Darurat**
    - Tenant/anggota mengirim **surat resmi** yang menjelaskan kebutuhan darurat (via email) dan melakukan permohonan melalui Portal Pusat Layanan APJII.
    - Visitor wajib membawa **identitas diri asli** yang valid.
2. **Verifikasi Cepat**
    - NOC APJII segera konfirmasi dengan pihak tenant/anggota.
    - Data Center Manager (atau pejabat berwenang) melakukan approval cepat.
3. **Registrasi di Pos Keamanan**
    - Visitor menyerahkan identitas asli.
    - Dicatat dalam **Visitor Management System (VMS)** dengan status darurat.
4. **Pemeriksaan Keamanan**
    - Visitor tetap melewati detektor logam & pengecekan barang bawaan.
    - Barang kerja dicatat dalam **Formulir Barang Bawaan Darurat**.
5. **Penerbitan Kartu Akses Darurat**
    - Kartu akses khusus **darurat (warna berbeda atau dengan label "Emergency")** diberikan.
    - Berlaku maksimal **1 hari** dan hanya pada area yang relevan dengan insiden darurat.
6. **Pendampingan Wajib**
    - Visitor dengan hak akses darurat **wajib didampingi** NOC APJII sepanjang aktivitas.
7. **Pekerjaan Darurat**
    - Visitor melakukan pekerjaan sesuai kebutuhan darurat.
    - Semua aktivitas dicatat dalam **Incident Log**.
8. **Keluar dari Data Center**
    - Barang bawaan diverifikasi ulang.
    - Kartu akses darurat dikembalikan.
    - Exit dicatat di VMS & dilaporkan dalam **Laporan Insiden** ke Data Center Manager.

Ringkasan Perbedaan Akses Normal vs Akses Darurat

Aspek	Akses Normal	Akses Darurat
Waktu Permohonan	H-1 sebelum kunjungan	Saat kondisi darurat (real-time)
Dokumen	Formulir Akses + Konfirmasi CS	Surat resmi tenant + identitas valid
Approval	Customer Service + Manager DC (standar)	Manager DC / pejabat berwenang (cepat)

Aspek	Akses Normal	Akses Darurat
Jenis Kartu Akses	Visitor/Tenant/Vendor sesuai kategori (color coding)	Kartu akses khusus darurat (label Emergency)
Durasi Berlaku	Sesuai permohonan (bisa harian/mingguan)	Maksimal 1 hari
Pendampingan	Tidak wajib untuk tenant, wajib untuk vendor	Wajib didampingi staf APJII
Dokumentasi	Tercatat di VMS	Tercatat di VMS + Incident Log + Laporan ke Manajemen

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXV
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PELAPORAN, MONITORING & EVALUASI (MONEV) DATA CENTER APJII

1. Pendahuluan

Data Center APJII merupakan fasilitas strategis yang digunakan oleh anggota APJII untuk layanan interkoneksi, colocation, serta berbagai kebutuhan infrastruktur ICT. Agar operasional berjalan dengan baik, diperlukan mekanisme **pelaporan, monitoring, dan evaluasi** yang sistematis, terukur, dan terdokumentasi. SOP ini menetapkan tata cara pencatatan, pemantauan, dan pelaporan aktivitas Data Center sehingga manajemen APJII memiliki data akurat untuk evaluasi, pengambilan keputusan, dan perencanaan pengembangan layanan.

2. Tujuan

- Menstandarkan proses pencatatan, pemantauan, dan pelaporan aktivitas operasional Data Center APJII.
- Menyediakan data statistik terkini mengenai pemanfaatan layanan Data Center oleh anggota APJII.
- Menjamin akurasi dan transparansi laporan kepada manajemen APJII dan anggota.
- Mendukung perencanaan kapasitas (capacity planning) dan pengelolaan aset Data Center.

3. Dasar & Referensi Standar

- **ISO/IEC 20000-1** – IT Service Management (service reporting & monitoring).
- **ISO/IEC 27001** – Information Security Management (logging & monitoring).
- **ISO/IEC 27002** – Controls for monitoring & review of access and operations.
- **ISO/IEC 22237** – Data Center Standards for facility & operational management.
- **Kebijakan Internal APJII** terkait pengelolaan Data Center dan pelaporan anggota.

4. Definisi Istilah

- **Pelaporan Data Center**: Penyajian data statistik terkait aktivitas, kapasitas, dan penggunaan layanan Data Center APJII.

- **Monitoring**: Proses pemantauan berkelanjutan terhadap layanan, perangkat, dan aktivitas Data Center.
- **Evaluasi**: Proses evaluasi yang berkelanjutan terhadap layanan, perangkat, dan aktivitas Data Center.
- **Colocation**: Layanan penyediaan ruang, daya, pendingin dan telekomunikasi untuk perangkat anggota di dalam Data Center APJII.
- **Interkoneksi**: Koneksi fisik/logis antar anggota melalui fasilitas Data Center APJII.
- **Install**: Proses pemasangan perangkat baru oleh tenant/anggota.
- **Dismantle**: Proses pencopotan perangkat atau interkoneksi yang tidak digunakan lagi.

5. Ruang Lingkup

SOP ini berlaku untuk seluruh proses pelaporan, monitoring, dan evaluasi Data Center APJII, mencakup:

- Layanan colocation.
- Layanan interkoneksi.
- Pencatatan perangkat anggota.
- Aktivitas install & dismantle perangkat.
- Penyusunan laporan statistik periodik untuk manajemen APJII.

6. Indikator Pelaporan, Monitoring & Evaluasi

Laporan Data Center APJII minimal memuat indikator berikut:

6.1 Statistik Pengguna Layanan

1. **Jumlah anggota APJII yang menggunakan layanan Data Center**:
    - **Jumlah anggota APJII yang memiliki Rack (*Dedicated*/*Partial*)**.
    - **Jumlah anggota APJII yang masuk dalam layanan:**
        - **Colocation**.
        - **Cross-Connect**.
        - **Traffic**.
        - **Mitra DC APJII**.

6.2 Statistik Perangkat

1. **Jumlah perangkat baru yang dipasang (Install)** dalam periode pelaporan.
2. **Jumlah perangkat yang dibongkar/dicopot (Dismantle)** dalam periode pelaporan.
3. **Tipe perangkat yang dipasang/terpasang (Installed Equipment Types)** → seperti: UPS Standalone, Router, Switch, Server, Firewall, Storage, Optical Device.

6.3 Statistik Interkoneksi

1. **Jumlah interkoneksi baru** yang terpasang.
2. **Jumlah interkoneksi** yang dibongkar/dicopot (Dismantle).
3. **Jumlah kabel interkoneksi** yang rusak/failure.

7. Prosedur Pelaporan, Monitoring, & Evaluasi

7.1 Pencatatan

- Setiap aktivitas **install/dismantle perangkat atau interkoneksi** wajib didokumentasikan melalui portal DCIM.
- Data colocation & rack dimutakhirkan setiap ada perubahan kontrak layanan.
- Semua log masuk Data Center terkait aktivitas teknis dihubungkan dengan sistem monitoring.

7.2 Monitoring

- Monitoring dilakukan oleh Tim **NOC secara real-time**.
- Data penggunaan listrik, pendingin, telekomunikasi dan kapasitas rack dimonitor secara otomatis melalui portal DCIM.
- Data interkoneksi dimonitor melalui portal DCIM & cross-connect register.

7.3 Evaluasi

- Evaluasi dilakukan oleh Tim **NOC** dan berkoordinasi dengan PIC/Penanggung Jawab Operasional DC APJII.
- Evaluasi terhadap data penggunaan listrik, pendingin, telekomunikasi dan kapasitas rack dilakukan oleh TIM **NOC** dan berkoordinasi dengan PIC/Penanggung Jawab Operasional DC APJII.
- Data interkoneksi & cross-connect dievaluasi antara Tim **NOC** dan berkoordinasi dengan PIC/Penanggung Jawab Operasional DC APJII.

7.4 Pelaporan Periodik

- **Harian** → aktivitas install/dismantle, kunjungan anggota, status interkoneksi.
- **Mingguan** → rekap statistik perangkat dan interkoneksi.
- **Bulanan** → laporan colocation, rack, dan kapasitas utilisasi.
- **Triwulanan** → laporan konsolidasi untuk evaluasi manajemen APJII.
- **Tahunan** → laporan strategis untuk Rapat Anggota & pengembangan Data Center.

7.4 Distribusi Laporan

- Laporan harian & mingguan → Tim NOC.
- Laporan bulanan & triwulanan → PIC/Penanggung Jawab Operasional DC APJII & Manajemen APJII (Rapat Bulanan BPP & Rapat Pleno BPP dengan Dewas)

- Laporan tahunan → Rakernas (Rapat Kerja Nasional).

8. Catatan & Dokumentasi

- Semua laporan disimpan minimal **5 tahun** untuk keperluan audit.
- Laporan elektronik (Excel/Database) harus memiliki backup di sistem DRC (Disaster Recovery Center).
- Perubahan data perangkat & interkoneksi wajib diverifikasi dengan **Berita Acara Aktivitas (BAA).**

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

Struktur Pelaporan, Monitoring & Evaluasi Data Center APJII

1. Laporan Harian

Fokus:

- Aktivitas operasional dan teknis di Data Center.
- Install/dismantle perangkat.
- Akses masuk/keluar anggota, vendor, visitor.

Parameter:

- Tanggal & Shift.
- Nama anggota/vendor.
- Jenis aktivitas (install/dismantle/maintenance).
- Jumlah perangkat yang dipasang/dicopot.
- Log interkoneksi baru/dicopot.
- Catatan insiden (jika ada).

Contoh Tabel Harian:

Tanggal	Nama Anggota	Aktivitas	Jumlah Perangkat	Tipe Perangkat	Interkoneksi	Catatan
13/09/2025	PT XYZ Net	Install	2	Router, Switch	1 Baru	Normal
13/09/2025	PT ABC Com	Dismantle	1	Server	-	Pemutusan layanan

2. Laporan Mingguan

Fokus:

- Rekapitulasi aktivitas harian.
- Tren install/dismantle.

- Penggunaan akses.

Parameter:

- Jumlah total perangkat yang di-install/dismantle dalam seminggu.
- Jumlah interkoneksi baru/dicopot.
- Jumlah kunjungan anggota/vendor.
- Catatan insiden mingguan.

Contoh Tabel Mingguan:

Minggu Ke-	Install (Unit)	Dismantle (Unit)	Interkoneksi Baru	Interkoneksi Dismantle	Jumlah Visitor	Catatan
Minggu 2 (7–13 Sept 2025)	5	2	3	1	18	Semua normal, 1 downtime singkat

3. Laporan Bulanan

Fokus:

- Utilisasi layanan colocation & rack.
- Statistik anggota pengguna Data Center.
- Konsolidasi aktivitas perangkat & interkoneksi.

Parameter:

- Jumlah anggota pengguna layanan Data Center.
- Jumlah anggota dengan rack dedicated/partial.
- Jumlah colocation aktif.
- Total perangkat terpasang.
- Breakdown tipe perangkat.

- Rekap interkoneksi baru & dismantle.

Contoh Tabel Bulanan:

Bulan	Jumlah Anggota DC	Jumlah Rack Aktif	Colocation Aktif	Install (Unit)	Dismantle (Unit)	Interkoneksi Baru	Interkoneksi Dismantle	Tipe Perangkat Terpasang
Sept 2025	54	72	45	15	8	12	6	Router: 30, Switch: 25, Server: 120, Storage: 20

4. Laporan Triwulanan

Fokus:

- Analisis tren 3 bulan.
- Kapasitas Data Center (rack, daya, pendingin, telekomunikasi).
- Evaluasi utilisasi layanan.

Parameter:

- Tren perangkat terpasang per bulan.
- Tren interkoneksi per bulan.
- Ketersediaan kapasitas (rack space, power).
- Evaluasi SLA & downtime.

Contoh Tabel Triwulanan:

Periode	Total Install	Total Dismantle	Total Interkoneksi Baru	Total Interkoneksi Dismantle	Utilisasi Rack (%)	Utilisasi Power (%)	SLA Availability (%)
Q3 2025 (Jul–Sep)	42	25	30	18	78%	72%	99,982%

5. Laporan Tahunan

Fokus:

- Rekap semua aktivitas tahunan.
- Analisis pertumbuhan anggota & layanan.
- Rencana kapasitas & pengembangan Data Center.

Parameter:

- Jumlah anggota yang menggunakan layanan Data Center per tahun.
- Jumlah rack & colocation yang digunakan.
- Total perangkat di-install & dismantle.
- Total interkoneksi baru & dismantle.
- Breakdown tipe perangkat.
- Kapasitas Data Center (terpakai vs tersedia).
- SLA tahunan.

Contoh Tabel Tahunan:

Tahun	Anggota Aktif DC	Rack Aktif	Colocation Aktif	Install (Unit)	Dismantle (Unit)	Interkoneksi Baru	Interkoneksi Dismantle	Tipe Perangkat	Utilisasi Rata-rata	SLA Tahunan
2025	62	85	51	180	95	120	80	Router: 95, Switch: 75, Server: 450, Storage: 70, Firewall: 30	Rack: 81%, Power: 77%	99,985%

Konsistensi Format

- **Header** sama di semua periode (anggota, rack, colocation, perangkat, interkoneksi, tipe perangkat).
- **Detail harian & mingguan** → fokus operasional.
- **Bulanan & triwulanan** → fokus tren & utilisasi.
- **Tahunan** → fokus pertumbuhan & kapasitas.

Rekapan Laporan Data Center APJII

1. Rekapan Harian → Mingguan

Input: Data aktivitas harian (install, dismantle, interkoneksi, akses visitor).
Output: Ringkasan mingguan untuk melihat tren & total.

Format Rekap Mingguan:

Minggu Ke-	Total Hari Dicatat	Install (Unit)	Dismantle (Unit)	Interkoneksi Baru	Interkoneksi Dismantle	Jumlah Visitor	Catatan
Minggu 1 (1–7 Sept)	7	10	5	6	2	42	Semua normal

Minggu Ke-	Total Hari Dicatat	Install (Unit)	Dismantle (Unit)	Interkoneksi Baru	Interkoneksi Dismantle	Jumlah Visitor	Catatan
Minggu 2 (8–14 Sept)	7	7	3	4	1	36	1 gangguan listrik singkat

📌 Rumus:

- Install (Unit Mingguan) = Σ Install Harian
- Dismantle (Unit Mingguan) = Σ Dismantle Harian
- Visitor Mingguan = Σ Visitor Harian

2. Rekapan Mingguan → Bulanan

Input: Ringkasan mingguan.
Output: Rekap bulanan utilisasi colocation & rack.

Format Rekap Bulanan:

Bulan	Total Minggu	Install (Unit)	Dismantle (Unit)	Interkoneksi Baru	Interkoneksi Dismantle	Jumlah Visitor	Anggota Aktif DC	Rack Aktif	Colocation Aktif
Sept 2025	4	32	15	18	7	145	54	72	45

📌 Rumus:

- Install (Bulanan) = Σ Install Mingguan
- Dismantle (Bulanan) = Σ Dismantle Mingguan
- Interkoneksi Baru (Bulanan) = Σ Mingguan
- Anggota Aktif DC, Rack Aktif, Colocation Aktif → update dari sistem keanggotaan & kontrak

3. Rekapan Bulanan → Triwulanan

Input: Rekap bulanan 3 bulan berturut-turut.
Output: Analisis tren utilisasi & SLA.

Format Rekap Triwulanan:

Triwulan	Bulan	Install (Unit)	Dismantle (Unit)	Interkoneksi Baru	Interkoneksi Dismantle	Utilisasi Rack (%)	Utilisasi Power (%)	SLA Availability (%)
Q3 2025	Jul	12	7	8	4	75%	70%	99,980%
	Aug	15	10	10	6	76%	71%	99,981%
	Sep	32	15	18	7	78%	72%	99,982%
Total Q3	-	**59**	**32**	**36**	**17**	**76% (avg)**	**71% (avg)**	**99,981% (avg)**

📌 Rumus:

- Total Install (Triwulanan) = Σ Bulanan (3 bulan)
- Utilisasi Rack/Power (Triwulanan) = Rata-rata utilisasi bulanan

4. Rekapan Triwulanan → Tahunan

Input: Rekap triwulanan (Q1 – Q4).
Output: Gambaran tahunan untuk rapat anggota APJII & pengembangan kapasitas.

Format Rekap Tahunan:

Tahun	Triwulan	Install (Unit)	Dismantle (Unit)	Interkoneksi Baru	Interkoneksi Dismantle	Anggota Aktif DC	Rack Aktif	Colocation Aktif	Utilisasi Rack (%)	Utilisasi Power (%)	SLA Tahunan
2025	Q1	40	20	25	10	50	65	41	74%	68%	99,982%
	Q2	45	25	28	15	53	69	43	76%	70%	99,983%
	Q3	59	32	36	17	54	72	45	76%	71%	99,981%
	Q4	36	18	31	12	62	85	51	81%	77%	99,985%
Total 2025	-	**180**	**95**	**120**	**54**	**62**	**85**	**51**	**81% (avg)**	**77% (avg)**	**99,985%**

📌 Rumus:

- Install (Tahunan) = Σ Install Triwulanan (Q1–Q4)
- Anggota Aktif DC, Rack Aktif, Colocation Aktif = data terakhir akhir tahun
- SLA Tahunan = rata-rata SLA availability per triwulan

Alur Konsolidasi Data

1. **Harian** → log operasional (aktivitas teknis & akses).
2. **Mingguan** → rekap total harian per minggu.
3. **Bulanan** → rekap total mingguan + update colocation/rack/anggota.
4. **Triwulanan** → rekap total bulanan + analisis tren & utilisasi.
5. **Tahunan** → rekap total triwulanan + evaluasi tahunan.

LAMPIRAN XXVI
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP MIGITASI RESIKO BENCANA ATAU GANGGUAN DI DC APJII

1. Pendahuluan

Data Center APJII merupakan infrastruktur kritikal nasional yang harus beroperasi dengan tingkat ketersediaan tinggi. Potensi gangguan seperti bencana alam, kebakaran, banjir, kerusuhan, maupun kegagalan teknis dapat mengancam keberlangsungan layanan. Oleh karena itu, diperlukan **SOP Mitigasi Resiko Bencana atau Gangguan** untuk memastikan tindakan pencegahan, penanganan, pemulihan, dan evaluasi berjalan secara terstandar.

2. Tujuan

- Menetapkan langkah-langkah mitigasi untuk mencegah atau meminimalisir dampak bencana/gangguan.
- Menjamin keamanan aset, personel, dan infrastruktur Data Center APJII.
- Menjaga kontinuitas layanan bagi anggota/tenant APJII.
- Menyediakan pedoman evakuasi, pemulihan, dan evaluasi layanan pasca bencana.

3. Dasar & Referensi Standar

- **ISO/IEC 27001** – Information Security Management (kontrol keamanan fisik & lingkungan).
- **ISO 22301** – Business Continuity Management System (BCMS).
- **ISO/IEC 27031** – ICT Readiness for Business Continuity.
- **TIA-942-C** – Data Center Standard Facility (Rated-3/4).
- **NFPA 75/76** – Standard for the Fire Protection of IT Equipment.
- Kebijakan Internal APJII tentang Manajemen Risiko & Keamanan.

4. Definisi Istilah

- **Mitigasi Resiko**: Upaya pencegahan atau pengurangan dampak risiko bencana/gangguan.
- **Disaster Recovery (DR)**: Proses pemulihan layanan pasca gangguan.
- **Business Continuity Plan (BCP)**: Rencana keberlangsungan layanan agar tetap berjalan meskipun terjadi gangguan.
- **Evakuasi**: Proses pemindahan personel dari area berisiko ke tempat aman.

5. Ruang Lingkup

SOP ini mencakup mitigasi risiko bencana/gangguan di Data Center APJII termasuk:

- Pengecekan berkala infrastruktur.
- Pencegahan banjir, kebocoran air, dan arus pendek.
- Mitigasi risiko kerusuhan, kebakaran, dan evakuasi.
- Evaluasi keberlangsungan layanan pasca gangguan.
- Prosedur pemulihan layanan dan minimalisasi risiko.

6. Prosedur Mitigasi Risiko Bencana atau Gangguan

6.1 Pengecekan Berkala

1. **Banjir**
    - Pemasangan **Water Leakage Detection System (WLDS)**.
    - Pemeriksaan pipa drainase PAC setiap **minggu**.
    - Pemasangan pintu kedap air di ruang kritikal.
2. **Kebocoran Air**
    - Pengecekan pipa HVAC/PAC & sistem pendingin setiap **bulan**.
    - Pemasangan sensor kebocoran di bawah raised floor.
3. **Arus Pendek/Konsleting/Short Circuit**
    - Pemeriksaan berkala panel listrik, UPS, PDU setiap **3 bulan**.
    - Pemeriksaan manual untuk deteksi panas berlebih di Rack MMR Bersama.
    - Penerapan grounding & bonding system.

6.2 Mitigasi Risiko Kerusuhan

- Penerapan **akses kontrol ketat** dengan multi-factor authentication.
- Dukungan **CCTV 24/7** dan petugas keamanan/Tim Security.
- Protokol **lockdown facility** saat kerusuhan di sekitar area.
- Koordinasi dengan **Polri/TNI** untuk pengamanan darurat.

6.3 Mitigasi Resiko Kebakaran

- Pemasangan **VESDA/HSSD** untuk deteksi dini asap.
- Penggunaan sistem pemadam otomatis/Fire Suprresion System (non-residual agent).
- Pelatihan fire drill minimal **2 kali setahun**.
- Pemeliharaan tabung APAR di titik strategis.

6.4 Prosedur Evakuasi

1. Aktivasi **alarm evakuasi**.
2. Tim keamanan/Tim Security mengarahkan personel ke **Assembly Point**.
3. Penanggung jawab area memastikan semua personel keluar.
4. Pencatatan jumlah orang yang dievakuasi.
5. Koordinasi dengan pihak pemadam, medis, dan aparat terkait.

6.5 Evaluasi Keberlangsungan Layanan

- Setelah gangguan, dilakukan **assessment dampak layanan** oleh Tim Teknis/NOC & PIC/Penanggung Jawab Operasional DC APJII.
- Identifikasi sistem yang terdampak → prioritisasi pemulihan berdasarkan **RTO (Recovery Time Objective)** & **RPO (Recovery Point Objective)**.
- Penyusunan **Incident Report** lengkap (penyebab, dampak, tindakan, rekomendasi).

6.6 Prosedur Meminimalisir Risiko

- Audit keamanan fisik & lingkungan tiap **6 bulan**.
- Simulasi bencana (fire drill, flood drill, riot drill) minimal **setahun sekali**.
- Review kontrak dengan vendor utility (listrik, air, konektivitas).
- Penempatan **redundancy system** (power, cooling, network).

6.7 Prosedur Pemulihan Layanan (Disaster Recovery)

1. Aktivasi **Disaster Recovery Plan (DRP)**.
2. Failover sistem ke **backup site/DR site** jika layanan utama tidak berfungsi.
3. Restorasi data dari backup sesuai **RPO**.
4. Validasi sistem pasca pemulihan.
5. Komunikasi ke tenant/anggota terkait status layanan.
6. Penyusunan laporan pemulihan ke **Manajemen APJII** & stakeholder terkait.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

Lampiran – Risk Register Mitigasi Resiko Data Center APJII

Legend Skor

- **Probabilitas (P):**
  1 = Sangat Rendah | 2 = Rendah | 3 = Sedang | 4 = Tinggi | 5 = Sangat Tinggi
- **Dampak (D):**
  1 = Minor (tidak ada gangguan layanan)
  2 = Rendah (gangguan kecil, cepat pulih)
  3 = Sedang (gangguan terbatas, ada downtime singkat)
  4 = Tinggi (downtime beberapa jam, gangguan layanan signifikan)
  5 = Kritis (downtime panjang, layanan tidak tersedia)
- **Level Risiko (R):**
  R = P × D
  - 1–5 = Rendah
  - 6–12 = Sedang
  - 13–25 = Tinggi

Tabel Risk Register

No	Risiko	Probabilitas (P)	Dampak (D)	Level Risiko (R)	Mitigasi
1	**Banjir**	3 (Sedang)	4 (Tinggi)	12 (**Sedang**)	- Pemasangan **WLDS** & pompa air otomatis - Inspeksi drainase mingguan - Pintu di ruang kritikal
2	**Kebocoran Air (pipa/HVAC)**	4 (Tinggi)	3 (Sedang)	12 (**Sedang**)	- Sensor kebocoran di raised floor - Inspeksi pipa bulanan - Maintenance rutin HVAC
3	**Arus Pendek/Konsleting**	3 (Sedang)	5 (Kritis)	15 (**Tinggi**)	- Cek Manual tiap 1 bulan - Preventive maintenance panel listrik & UPS - Sistem grounding & bonding

No	Risiko	Probabilitas (P)	Dampak (D)	Level Risiko (R)	Mitigasi
4	**Kerusuhan / Akses Ilegal**	2 (Rendah)	5 (Kritis)	10 (**Sedang**)	- **Akses kontrol ketat** (biometrik, kartu) - CCTV 24/7 & armed security - Protokol lockdown & koordinasi aparat
5	**Kebakaran**	2 (Rendah)	5 (Kritis)	10 (**Sedang**)	- VESDA/HSSD untuk deteksi dini - Gas Fire Suppression System - Fire drill 2x setahun
6	**Gangguan Listrik PLN**	4 (Tinggi)	4 (Tinggi)	16 (**Tinggi**)	- Redundansi genset 2N (Disediakan oleh Pengelola Gedung Cyber-1 - Preventive maintenance bulanan - Stock BBM minimal 72 jam (Disediakan oleh pihak Pengelola Gedung Cyber-1)
7	**Gangguan Pendingin (PAC/CRAC)**	3 (Sedang)	4 (Tinggi)	12 (**Sedang**)	- Redundansi N+1 system di unit PAC - Monitoring suhu & kelembaban 24/7 - Spare parts disediakan oleh Vendor
8	**Evakuasi Darurat (kebakaran/kerusuhan)**	2 (Rendah)	4 (Tinggi)	8 (**Sedang**)	- Jalur evakuasi jelas & teruji - Assembly point aman - Simulasi evakuasi minimal 1x/tahun
9	**Gangguan Jaringan / Interkoneksi**	3 (Sedang)	5 (Kritis)	15 (**Tinggi**)	- Backup Routing - Monitoring NOC 24/7 - Failover
10	**Gangguan Sistem Security (akses kontrol/CCTV)**	2 (Rendah)	3 (Sedang)	6 (**Sedang**)	- Backup sistem keamanan - Inspeksi & test bulanan - Security manual fallback

No	Risiko	Probabilitas (P)	Dampak (D)	Level Risiko (R)	Mitigasi
11	**Gangguan Personel (human error/absen massal)**	3 (Sedang)	3 (Sedang)	9 (**Sedang**)	- SOP detail & training rutin - On-call team 24/7 - Cross-skill antar tim
12	**Pandemi/Wabah**	2 (Rendah)	4 (Tinggi)	8 (**Sedang**)	- Shift split team - Remote access untuk NOC - Protokol kesehatan & disinfektan, serta mengikuti kebijakan pemerintah

Analisis Singkat

- **Risiko Tinggi (R ≥ 13):**
  - Arus pendek / konsleting (15)
  - Gangguan listrik PLN (16)
  - Gangguan jaringan/interkoneksi (15)
    → Fokus mitigasi utama pada **power & network redundancy**.
- **Risiko Sedang (6–12):**
  - Banjir, kebocoran air, pendingin, kerusuhan, kebakaran, evakuasi, sistem keamanan, human error, pandemi.
    → Dikelola dengan **SOP operasional & inspeksi berkala**.
- **Risiko Rendah (≤ 5):**
  - Saat ini tidak ada risiko dengan kategori rendah karena semua potensi di data center minimal **sedang**.

LAMPIRAN XXVII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP SISTEM PENCEGAHAN BAHAYA KEBAKARAN DATA CENTER APJII

1. Pendahuluan

Data Center APJII merupakan fasilitas kritikal yang harus beroperasi secara **24/7** dengan tingkat keamanan dan keandalan tinggi. Salah satu risiko terbesar adalah kebakaran yang dapat mengakibatkan **downtime, kerusakan perangkat, kehilangan data, dan gangguan layanan**. Oleh karena itu, diperlukan SOP yang mengatur pencegahan, deteksi dini, penanggulangan, dan evakuasi bahaya kebakaran di lingkungan Data Center APJII.

2. Tujuan

- Menjamin keselamatan personel, perangkat, dan infrastruktur Data Center dari risiko kebakaran.
- Memberikan pedoman standar dalam penggunaan sistem deteksi, alarm, dan pemadaman kebakaran.
- Menetapkan prosedur evakuasi dan simulasi kebakaran secara berkala.
- Memastikan pemetaan jalur evakuasi tersedia, jelas, dan mudah diakses oleh semua personel.

3. Dasar & Referensi Standar

- **NFPA 75** – Standard for the Fire Protection of Information Technology Equipment.
- **NFPA 2001** – Standard on Clean Agent Fire Extinguishing Systems.
- **ISO/IEC 27002** – Annex A.11 Physical and Environmental Security.
- **TIA-942-C** – Data Center Telecommunications Infrastructure Standard.
- **SNI 03-1746-2000** – Tata Cara Perencanaan Jalur Evakuasi pada Bangunan Gedung.
- Kebijakan Internal APJII mengenai Keselamatan Kerja & Keamanan Data Center.

4. Definisi Istilah

- **Fire Alarm System**: Sistem peringatan dini kebakaran yang mendeteksi asap, panas, atau api.

- **VESDA (Very Early Smoke Detection Apparatus)**: Sistem pendeteksi asap sangat dini berbasis laser.
- **FSS (Fire Suppression System)**: Sistem pemadam kebakaran otomatis berbasis gas (misalnya Novec 1230 / FM-200).
- **Fire Drill**: Latihan simulasi evakuasi dalam kondisi darurat kebakaran.
- **Jalur Evakuasi**: Rute yang ditetapkan untuk evakuasi personel menuju titik kumpul aman.

5. Ruang Lingkup

SOP ini berlaku untuk seluruh fasilitas Data Center APJII, meliputi:

- Ruang Data Hall.
- Ruang UPS & Battery Room.
- Ruang Genset & Panel Listrik.
- Ruang NOC & ruang pendukung.
- Area kantor pendukung di dalam gedung Data Center.

6. Sistem Pencegahan Bahaya Kebakaran

6.1 Pencegahan Utama

- Larangan merokok di seluruh area Data Center.
- Larangan penggunaan perangkat listrik non-standar.
- Pemeriksaan berkala instalasi listrik, panel, UPS, dan genset.
- Penempatan **APAR (Alat Pemadam Api Ringan)** di lokasi strategis (tiap 15 m).
- Pelatihan penggunaan APAR untuk staf teknis & keamanan.

7. Sistem Pendeteksi Bahaya Asap dan Api

- **VESDA (HSSD)** dipasang di ruang data hall untuk mendeteksi asap mikro sebelum terjadi kebakaran.
- **Smoke Detector** & **Heat Detector** dipasang di semua area kritikal.
- Detektor terhubung ke **Fire Alarm Control Panel (FACP)** dan **Building Monitoring System (BMS)**.
- Alarm dikategorikan:
    - **Stage 1 (Early Warning)**: Terjadi indikasi asap awal.
    - **Stage 2 (Fire Alarm)**: Potensi kebakaran, triggering alarm & notifikasi ke NOC.

8. Fire Alarm

- Fire Alarm terintegrasi dengan sistem suara (Public Address/PA) untuk memberi peringatan.
- Alarm dapat berbentuk:
    - **Audible Alarm** (sirine).
    - **Visual Alarm** (lampu strobo merah).

- Alarm langsung mengaktifkan **prosedur evakuasi otomatis** dan notifikasi ke tim keamanan & NOC.

9. Fire Suppression System (FSS)

- Menggunakan **Clean Agent Gas** (Novec 1230 atau FM-200) yang ramah lingkungan dan tidak merusak perangkat elektronik.
- Sistem dilengkapi:
  - **Automatic Release**: Gas dipicu secara otomatis oleh panel deteksi asap & api.
  - **Manual Release**: Tombol manual tersedia di area luar ruangan.
  - **Abort Switch**: Untuk membatalkan pelepasan gas jika kondisi false alarm.
- Setiap pelepasan FSS wajib dibuatkan **incident report** dan analisis penyebab.

10. Prosedur Evakuasi

1. **Alarm Berbunyi**
   - Semua personel segera menghentikan aktivitas.
   - Koordinator Evakuasi (ditunjuk oleh manajemen) memandu evakuasi.
2. **Evakuasi Jalur Aman**
   - Ikuti jalur evakuasi menuju titik kumpul.
   - Jangan membawa barang pribadi yang besar.
   - Jangan gunakan lift.
3. **Titik Kumpul**
   - Berada di lokasi aman yang sudah ditetapkan di luar gedung.
   - Dilakukan **roll call** untuk memastikan seluruh personel aman.
4. **Koordinasi dengan Pemadam**
   - Security APJII menghubungi **Damkar setempat (113)**.
   - Memberikan akses kepada petugas pemadam kebakaran.

11. Fire Drill Simulation

- Fire Drill wajib dilakukan **minimal 2 kali setahun**.
- Melibatkan seluruh staf, tenant, vendor, dan security.
- Skenario mencakup:
  - Aktivasi alarm.
  - Pelepasan simulasi FSS (tanpa gas).
  - Evakuasi ke titik kumpul.
- Evaluasi hasil simulasi dituangkan dalam **Laporan Fire Drill** untuk perbaikan prosedur.

12. Pemetaan Jalur Evakuasi

- Jalur evakuasi ditandai dengan **signage hijau standar internasional (ISO 7010 E001)**.
- Emergency exit dilengkapi **lampu darurat (emergency light)** yang menyala otomatis jika listrik padam.

- Denah evakuasi ditempel di:
    - Pintu masuk utama Data Hall.
    - Koridor utama.
    - Area NOC dan kantor pendukung.
- Peta evakuasi diperbarui minimal **setiap 1 tahun** atau jika ada renovasi/rekonfigurasi ruangan.

13. Dokumentasi & Audit

- Semua aktivitas terkait sistem kebakaran (maintenance, pengujian, drill, insiden) dicatat dalam **Fire Safety Logbook**.
- Audit internal dilakukan **setiap 6 bulan** oleh tim Data Center Operation & Safety Officer.

Alur Respons Kebakaran – Data Center APJII

1. Deteksi Awal

- **VESDA/Smoke Detector** mendeteksi asap → trigger **Early Warning**.
- **Heat Detector** mendeteksi peningkatan suhu → trigger **Fire Alarm Stage 2**.
- Sistem mengirimkan notifikasi ke **Fire Alarm Control Panel (FACP)**, **NOC**, dan **Security**.

2. Alarm Aktif

- **Audible Alarm (sirine)** + **Visual Alarm (lampu strobo merah)** berbunyi.
- **Public Address System** memberikan instruksi evakuasi.
- **Security APJII** segera menginformasikan ke seluruh personel & tenant.

3. Evaluasi Kondisi

- **Stage 1 (Early Warning)** → Koordinator mengecek sumber asap.
- **Stage 2 (Confirmed Fire)** → Sistem siap melepas **Fire Suppression Gas**.
- **Abort Switch** dapat digunakan jika terbukti **false alarm**.

4. Fire Suppression System (FSS)

- **Automatic Release**: Gas (Novec 1230/FM-200) dilepas otomatis jika alarm valid.
- **Manual Release**: Jika api terkonfirmasi, petugas dapat menekan tombol manual release.
- Area terkunci sementara untuk menghindari paparan gas.

5. Prosedur Evakuasi

- Semua personel segera menghentikan aktivitas.
- Ikuti **jalur evakuasi** menuju **titik kumpul**.
- Jangan gunakan lift.
- Koordinator Evakuasi melakukan **roll call** untuk memastikan jumlah personel lengkap.

6. Koordinasi Eksternal

- Security segera menghubungi **Pemadam Kebakaran (113)**.
- Memberikan akses kepada tim pemadam untuk masuk ke area terdampak.
- Koordinasi dengan **Manajemen APJII** untuk eskalasi insiden.

7. Pemulihan (Recovery)

- Setelah area dinyatakan aman:
    - Tim Operasional melakukan **damage assessment**.
    - Dokumentasi insiden dibuat dalam **Incident Report**.
    - Sistem FSS diisi ulang (refill gas).
    - Analisis penyebab & perbaikan prosedur dilakukan (**Root Cause Analysis / RCA**).

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXVIII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP KEBIJAKAN BCP DAN DRP KEJADIAN KAHAR/FORCE MAJEURE DATA CENTER APJII

1. Pendahuluan

Data Center APJII merupakan infrastruktur strategis nasional yang mendukung konektivitas dan interkoneksi internet antar penyelenggara jasa internet (ISP), operator, dan lembaga-lembaga nasional. Dalam menjalankan fungsi kritis tersebut, keberlangsungan operasional (business continuity) dan kemampuan pemulihan pasca bencana (disaster recovery) harus dijamin, termasuk ketika menghadapi **kejadian Kahar (Force Majeure)** yang berada di luar kendali manusia.

SOP Kebijakan Business Continuity dan Disaster Recovery ini disusun untuk memastikan bahwa:

- Operasional Data Center APJII tetap berlanjut atau dapat dipulihkan dengan cepat pasca gangguan besar atau kejadian kahar.
- Dampak kerusakan terhadap layanan kritikal, sistem, data, dan infrastruktur dapat diminimalisir.
- Komunikasi, koordinasi, dan pengambilan keputusan berjalan efektif selama krisis.

Kejadian kahar yang dimaksud mencakup **bencana alam, tindakan manusia, gangguan teknis besar, kebakaran, pandemi/epidemi, serta perintah atau regulasi pemerintah yang tidak dapat dihindari.**

2. Tujuan

Tujuan SOP ini adalah untuk:

1. Menetapkan **prosedur kesiapan dan tanggap darurat** dalam menghadapi kejadian kahar yang mengancam keberlangsungan operasional Data Center APJII.
2. Menjamin **keamanan personel, aset fisik, data, dan sistem** selama dan setelah kejadian kahar.
3. Menyediakan **kerangka kerja sistematis** dalam melakukan aktivasi, pelaksanaan, dan pemulihan operasi kritikal (Disaster Recovery Plan / DRP).
4. Menjamin **komunikasi dan koordinasi** antar tim (Manajemen, Operasional, Network, Electrical, Cooling, Security, Vendor) berjalan secara efisien.

5. Menyusun **strategi pemulihan layanan prioritas** berdasarkan skenario risiko dan tingkat dampaknya.

3. Dasar dan Referensi Standar

SOP ini disusun dengan mengacu pada standar nasional dan internasional berikut:

1. **ISO 22301:2019** – Business Continuity Management System (BCMS)
2. **ISO/IEC 27031:2011** – ICT Readiness for Business Continuity
3. **ISO/IEC 24762:2008** – Guidelines for ICT Disaster Recovery Services
4. **ISO 31000:2018** – Risk Management
5. **TIA-942-C:2023** – Telecommunications Infrastructure Standard for Data Centers (Rated-3/Rated-4 Facility Requirements)
6. **NFPA 75 dan NFPA 76** – Fire Protection of IT Equipment
7. **Peraturan Pemerintah No. 21 Tahun 2008** – Penyelenggaraan Penanggulangan Bencana
8. **Undang-Undang No. 24 Tahun 2007** – Penanggulangan Bencana
9. **Pedoman BNPB** – Klasifikasi dan Penanganan Bencana Alam dan Non-Alam
10. **Kebijakan Internal APJII** – Data Center Operation & Business Continuity Policy

4. Definisi Istilah

1. **Business Continuity (BC)** – Kemampuan organisasi untuk mempertahankan fungsi penting selama dan setelah terjadi gangguan besar.
2. **Disaster Recovery (DR)** – Proses pemulihan sistem IT, data, dan infrastruktur kritikal ke kondisi normal atau fungsional minimum.
3. **Force Majeure / Kejadian Kahar** – Keadaan luar biasa yang tidak dapat dihindari dan di luar kendali manusia, seperti bencana alam, perang, sabotase, kerusuhan, pandemi, atau kebijakan pemerintah.
4. **RTO (Recovery Time Objective)** – Waktu maksimum yang diperbolehkan untuk memulihkan sistem atau layanan kritikal setelah terjadi gangguan.
5. **RPO (Recovery Point Objective)** – Tingkat kehilangan data maksimum yang dapat diterima diukur dari waktu sebelum kejadian gangguan.
6. **Hot Site / DR Site** – Lokasi cadangan operasional yang digunakan untuk menjalankan fungsi kritikal bila site utama tidak dapat digunakan.
7. **BCM Team (Business Continuity Management Team)** – Tim lintas fungsi yang bertanggung jawab dalam pelaksanaan kebijakan BC/DR selama kejadian kahar.
8. **Incident Commanding Officer (ICO)** – Personel yang ditunjuk untuk memimpin dan mengkoordinasikan seluruh respon tanggap darurat dan pemulihan.

5. Ruang Lingkup

SOP ini mencakup seluruh kegiatan **Business Continuity dan Disaster Recovery (BCP/DRP)** di lingkungan **Data Center APJII**, termasuk fasilitas utama dan lokasi pendukung, dengan ruang lingkup sebagai berikut:

5.1 Jenis Kejadian Kahar / Force Majeure

1. **Bencana Alam**
   - **Banjir:** Kenaikan air hingga merendam area data center atau utilitas pendukung.
   - **Gempa Bumi:** Getaran yang menyebabkan kerusakan struktur, rak server, sistem pendingin, dan catu daya.
   - **Badai / Angin Topan:** Gangguan pada infrastruktur fisik, jaringan utilitas, dan jalur komunikasi.
2. **Tindakan Manusia**
   - Peperangan / Konflik Bersenjata
   - Terorisme / Ledakan / Penyerangan Fasilitas
   - Kerusuhan / Aksi Massa / Pemogokan
   - Sabotase terhadap Infrastruktur Kritis
3. **Gangguan Besar Lainnya**
   - **Pandemi / Epidemi:** Gangguan operasional akibat pembatasan mobilitas personel atau infeksi massal.
4. **Kebakaran**
   - Kebakaran yang terjadi di ruang IT, ruang UPS, genset, fuel tank, atau ruang utilitas lainnya.
5. **Gangguan Teknis Besar**
   - **Sistem Kelistrikan:** Kegagalan sumber daya utama dan cadangan (UPS, PDU).
   - **Sistem Telekomunikasi:** Terputusnya konektivitas lintas ISP, router core, atau switch utama.
   - **Sistem Pendingin (Cooling):** Kegagalan Precision Air Conditioning (PAC), chiller, atau sistem distribusi pendingin.
6. **Kebijakan Pemerintah**
   - **Blokade, lockdown, atau aturan baru** yang membatasi akses atau operasional data center.

6. Strategi Umum BCP/DRP

1. **Identifikasi Layanan Kritis (Critical Services Identification)** Melalui analisis, ditetapkan layanan utama yang harus tetap berjalan: interkoneksi IIX, DNS root, NOC operation, dan infrastruktur backbone.
2. **Redundansi Infrastruktur**
   - Power: Dual UPS System.
   - Network: Dual upstream ISP dan redundant path.
   - Cooling: N+1 configuration PAC system.
3. **Backup dan Replikasi Data**
   - Backup otomatis ke **offsite DR site** minimal sekali sehari.
   - Enkripsi data backup untuk keamanan integritas data.
4. **Lokasi Pemulihan (DR Site)**
   - DR Site di lokasi geografis berbeda dengan konektivitas minimal 1 Gbps secure link.
   - Dapat diaktifkan dalam ≤ 4 jam untuk layanan kritikal (RTO 4h / RPO 15min).
5. **Aktivasi dan Eskalasi**
   - Setiap kejadian kahar diverifikasi oleh Incident Commander.
   - BCM Team melakukan aktivasi **Lockdown Mode**, evakuasi, dan transisi operasional ke DR Site.

6. **Komunikasi Krisis**
    - Menggunakan portal DCIM, WA Group, Email, Teams.
    - Komunikasi eksternal hanya dilakukan oleh **Sekretariat APJII**.
7. **Pemulihan dan Normalisasi**
    - Setelah situasi aman, dilakukan **assessment kerusakan, recovery data, restore sistem, dan verifikasi integritas layanan.**
    - Evaluasi pasca-insiden dilakukan untuk memperbaiki SOP dan strategi DR (Disaster Recovery)/BCM.

7. Struktur Organisasi dan Tanggung Jawab BCM (Business Continuity Management)

Struktur organisasi BCM Data Center APJII dirancang untuk memastikan adanya **rantai komando yang jelas, koordinasi efektif, dan tanggung jawab terdistribusi dengan baik** dalam kondisi darurat atau bencana besar.

7.1 Struktur Tim BCP/DRP

Level / Peran	Jabatan / Unit	Tanggung Jawab Utama
Incident Commanding Officer (ICO)	PIC/Penanggung Jawab Operasional DC APJII	Mengambil keputusan strategis, mengaktifkan BCP/DRP, menetapkan status darurat, dan melapor ke Manajemen APJII.
Tim NOC	Supervisor NOC / Shift Leader Senior	Membantu ICO, memastikan pelaksanaan instruksi di lapangan, dan menjadi pengganti ICO jika berhalangan.
BCM Coordinator	Manajemen APJII	Menyusun, mengkoordinasikan, dan memperbarui seluruh kebijakan dan prosedur BCP/DRP.
IT & Network Recovery Team	Tim NOC	Melakukan pemulihan sistem, jaringan, dan layanan ICT ke DR Site atau sistem cadangan.
Facilities & Power Recovery Team	Tim Teknikal	Menangani pemulihan sistem kelistrikan, pendingin, UPS, PAC, dan fasilitas fisik.
Security	Tim Security	Melaksanakan evakuasi, pengamanan aset, dan penerapan protokol keselamatan personel.
Sekretariat APJII	Tim Sekretariat	Mengelola komunikasi internal dan eksternal, termasuk media, regulator, dan pelanggan.
Logistics & Administration Support	HR/GA & Procurement	Mengatur logistik, peralatan darurat, transportasi, dan akomodasi tim pemulihan.

8. Prosedur Aktivasi dan Implementasi BCP/DRP

Prosedur ini menjelaskan **tahapan aktivasi, pelaksanaan, dan pemulihan** operasional Data Center APJII ketika kejadian kahar terjadi.

8.1 Tahapan Aktivasi

1. **Deteksi dan Identifikasi Kejadian**
    - Setiap personel yang mendeteksi anomali besar (misal: kebakaran, banjir, blackout total, kerusakan sistem) wajib segera melapor ke Tim NOC dan **Incident Commanding Officer (ICO)**.
2. **Penilaian Awal Dampak (Initial Impact Assessment)**
    - **ICO** menilai tingkat keparahan kejadian berdasarkan:
        - Skala kerusakan fasilitas / sistem
        - Dampak terhadap layanan utama
        - Potensi risiko terhadap keselamatan personel
    - Jika dampak **"Major" atau "Catastrophic"**, maka status **BCP/DRP Active Mode** dinyatakan.
3. **Deklarasi Keadaan Darurat / Force Majeure**
    - **ICO** mengumumkan status resmi **"Lockdown Mode"** dan **aktivasi BCP/DRP**.
    - Menginformasikan ke Manajemen APJII dan/atau Anggota/Tenant yang dilakukan melalui kanal resmi APJII.
4. **Evakuasi dan Pengamanan Aset**
    - Tim Security memastikan seluruh personel dievakuasi.
    - Server room, panel listrik, dan area kritikal dikunci untuk mencegah sabotase/pencurian.
5. **Aktivasi DR Site (Disaster Recovery Site)**
    - Jika site utama tidak beroperasi ≥ RTO 4 jam, maka sistem prioritas (DNS, NOC core, IIX route server) dipindahkan ke DR Site.
    - Backup data terakhir dari offsite storage digunakan sebagai baseline pemulihan.

8.2 Tahapan Implementasi

1. **Stabilisasi Awal**
    - Pastikan area aman dari bahaya sekunder (api, air, listrik).
    - Hidupkan power backup sementara (UPS APJII, UPS standalone).
2. **Recovery Sistem IT dan Jaringan**
    - Tim IT melakukan restore dari backup image dan re-route trafik jaringan ke jalur cadangan.
    - Validasi konektivitas antar core dan peering member dilakukan melalui NOC.
3. **Koordinasi Eksternal**
    - Sekretariat APJII mengirimkan laporan status ke regulator (KOMDIGI, IDNIC, member APJII).
    - Komunikasi dengan media hanya dilakukan dengan persetujuan **ICO**.
4. **Monitoring Berkelanjutan**
    - Semua aktivitas pemulihan dimonitor secara real-time melalui sistem monitoring.
    - Update status setiap 1 jam selama fase pemulihan aktif melalui kanal resmi APJII.

9. Prosedur Pemulihan dan Normalisasi

Tahapan ini memastikan sistem dan layanan Data Center APJII kembali beroperasi normal secara aman dan terkendali.

9.1 Langkah Pemulihan

1. **Damage Assessment** – Evaluasi fisik fasilitas, kabel, PAC, UPS, dan sistem IT.
2. **System Validation** – Verifikasi integritas data, konfigurasi jaringan, dan keamanan sistem.
3. **Functional Test** – Uji fungsi tiap layanan utama (power, cooling, network, security system).
4. **Gradual Restoration** – Layanan dikembalikan bertahap dari prioritas tinggi → rendah.
5. **User Acceptance Test (UAT)** – Verifikasi bersama pihak Anggota/Tenant bahwa layanan kembali normal.

9.2 Kriteria Normalisasi

- Tidak ada alarm aktif pada sistem monitoring.
- Semua sistem berjalan pada mode utama, bukan mode darurat.
- Layanan utama stabil ≥ 12 jam berturut-turut.
- **ICO** mendeklarasikan “Operational Normal Mode”.

10. Dokumentasi dan Pelaporan

1. **Incident Logbook**
   - Semua kejadian, waktu, tindakan, dan pihak terlibat dicatat di **Disaster Log Form**.
2. **Post-Incident Report (PIR)**
   - Disusun oleh **ICO**, maksimal 3 hari setelah kejadian.
   - Memuat: kronologi, penyebab, dampak, langkah tanggap darurat, waktu pemulihan, pelajaran yang dipetik.
3. **Regulatory Report**
   - Laporan resmi dikirim ke pihak berwenang (KOMDIGI, IDNIC, Anggota/Tenant).
4. **Document Control**
   - Semua dokumen BCP/DRP diklasifikasikan “Confidential” dan disimpan di **Offsite Archive**.

11. Pelatihan dan Simulasi

1. **Pelatihan Rutin**
   - Dilaksanakan minimal **2 kali setahun** untuk seluruh personel operasional, mencakup:
     - Aktivasi BCP/DRP.
     - Evakuasi dan prosedur ERT.
     - Penggunaan fire suppression.
     - Pengalihan operasi ke DR Site.
2. **Simulasi (Drill)**
   - **Tabletop Exercise:** simulasi koordinasi dan komunikasi antar tim.
   - **Live Exercise:** uji pemindahan sistem ke DR Site dan restore data dari backup.

- **Post-Drill Review:** evaluasi kecepatan respon, ketepatan prosedur, dan koordinasi tim.

3. **Evaluasi Kesiapan**
   - Hasil simulasi dianalisis menggunakan **Key Performance Indicator (KPI)**:
     - RTO dan RPO tercapai.
     - Efektivitas komunikasi.
     - Keamanan data dan personel terjaga.

12. Evaluasi, Audit, dan Review Kebijakan

1. **Evaluasi Pasca-Inisiden (Post-Incident Review)**
   - Dilakukan setelah setiap kejadian kahar, mencakup:
     - Analisis akar penyebab (Root Cause Analysis – RCA)
     - Evaluasi efektivitas SOP
     - Rekomendasi perbaikan sistem dan infrastruktur
2. **Audit Internal & Eksternal**
   - Audit internal tahunan oleh tim APJII.
   - Audit eksternal setiap 2 tahun.
3. **Review Berkala**
   - Dokumen BCP/DRP direview minimal **setahun sekali** atau setelah ada perubahan besar (organisasi, sistem, atau fasilitas).
   - Revisi disetujui oleh **PIC/Penanggung Jawab Operasional DC APJII** dan disosialisasikan ke seluruh unit.
4. **Continuous Improvement**
   - Setiap temuan audit, drill, atau insiden digunakan sebagai masukan untuk peningkatan berkelanjutan SOP Kebijakan BCP dan DRP.

Penutup

Kebijakan ini menjadi pedoman resmi bagi seluruh personel Data Center APJII dalam menjaga keberlangsungan operasional, keselamatan personel, serta keandalan layanan publik di bawah kondisi luar biasa. Kepatuhan terhadap SOP ini bersifat **wajib** bagi seluruh unit dan mitra kerja yang beroperasi di lingkungan Data Center APJII.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXIX
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP LOCKDOWN MODE PADA KEJADIAN KAHAR/FORCE MAJEURE DATA CENTER APJII

1. Pendahuluan

Kejadian Kahar atau *Force Majeure* adalah situasi luar biasa yang berada di luar kendali manusia dan dapat menyebabkan gangguan serius terhadap operasional Data Center APJII. Dalam kondisi demikian, dibutuhkan prosedur khusus berupa **Lockdown Mode**, yaitu tindakan pengamanan dan pembatasan akses fisik maupun operasional untuk menjaga keselamatan personel, perlindungan aset kritis, serta kesinambungan layanan data center.

SOP ini memberikan panduan terperinci bagi seluruh personel dan pihak terkait dalam mengaktifkan, melaksanakan, dan menonaktifkan **Lockdown Mode** pada saat terjadinya kondisi kahar, baik yang disebabkan oleh faktor alam, manusia, teknis, maupun kebijakan pemerintah.

2. Tujuan

Tujuan dari SOP ini adalah:

1. Menetapkan mekanisme penanganan kondisi kahar melalui penerapan **Lockdown Mode** guna menjaga keamanan personel, infrastruktur, dan data pelanggan.
2. Memastikan langkah tanggap darurat dilakukan secara cepat, terkoordinasi, dan aman.
3. Menjamin keberlangsungan layanan vital data center selama dan sesudah kejadian kahar.
4. Menyediakan pedoman pemulihan operasional (normalisasi) secara terstruktur pasca kejadian.
5. Menetapkan tanggung jawab dan wewenang setiap pihak selama periode lockdown berlangsung.

3. Dasar dan Referensi Standar

SOP ini disusun mengacu pada pedoman dan standar berikut:

- **TIA-942-C** – *Telecommunications Infrastructure Standard for Data Centers* (Bagian: Facility, Safety & Operations)
- **ISO 22301:2019** – *Business Continuity Management System (BCMS)*
- **ISO 27001:2022** – *Information Security Management System*

- **ISO 45001:2018** – *Occupational Health & Safety Management System*
- **NFPA 75 & 76** – *Fire Protection for IT & Telecommunications Facilities*
- **Undang-Undang No. 24 Tahun 2007** tentang Penanggulangan Bencana
- **Peraturan Menteri Kominfo** terkait keamanan dan keandalan data center
- **Prosedur BCP & ERP APJII Data Center**

4. Definisi Istilah

Istilah	Definisi
Kejadian Kahar / Force Majeure	Kejadian di luar kendali manusia yang mengakibatkan gangguan besar pada operasional data center, seperti bencana alam, perang, atau kebijakan pemerintah yang tidak dapat dihindari.
Lockdown Mode	Kondisi tertutup penuh di mana seluruh akses fisik dan logistik ke dalam maupun keluar area data center dibatasi atau dihentikan sementara untuk keamanan.
Command Center	Ruang kendali utama yang menjadi pusat koordinasi tanggap darurat dan pengambilan keputusan saat Lockdown Mode diaktifkan.
Incident Commanding Officer (ICO)	Penanggung jawab utama dalam mengelola kejadian kahar dan menentukan status Lockdown Mode.
Critical Personnel	Personel terbatas yang memiliki izin tetap berada di fasilitas selama lockdown berlangsung (misalnya NOC, Tim Teknis, Security).
Recovery Team	Tim pemulihan yang bertugas melaksanakan proses normalisasi operasional pasca kejadian kahar.
Evacuation Zone	Area aman yang ditetapkan sebagai tempat berkumpul apabila evakuasi harus dilakukan.

5. Ruang Lingkup

Ruang lingkup SOP ini mencakup seluruh fasilitas **Data Center APJII**, termasuk namun tidak terbatas pada:

- Area Datahall APJII.
- Seluruh personel internal, vendor, kontraktor, serta tamu yang berada di area fasilitas pada saat kejadian.
- Situasi kejadian kahar yang meliputi:

A. Bencana Alam:

- Banjir, gempa bumi, badai, longsor, petir, atau fenomena alam yang ekstrem lainnya.

B. Tindakan Manusia:

- Peperangan, terorisme, kerusuhan, sabotase, pemogokan, perusakan aset publik.

C. Kesehatan:

- Pandemi, epidemi, penyebaran penyakit menular yang membatasi mobilitas personel.

D. Kebakaran:

- Kebakaran internal atau eksternal yang mengancam keselamatan fasilitas & personel APJII.

E. Gangguan Teknis Besar

- Gangguan besar sistem kelistrikan, sistem pendingin (HVAC), sistem telekomunikasi atau jaringan utama.

F. Kebijakan Pemerintah

- Blokade wilayah, peraturan darurat, atau instruksi otoritas yang membatasi operasional.

6. Aktivasi Lockdown Mode

6.1. Pemicu Aktivasi

Lockdown Mode dapat diaktifkan berdasarkan:

- Deteksi langsung kejadian kahar oleh sensor sistem (fire alarm, water leak, *seismic activity*, dsb).
- Informasi resmi dari otoritas (BMKG, BNPB, TNI/Polri, Pemerintah Daerah) atau pihak pengelola gedung Cyber-1.
- Arahan langsung dari **Incident Commanding Office (ICO)** setelah asesmen risiko darurat.

6.2. Prosedur Aktivasi

1. **ICO** mendeklarasikan status ***Lockdown Mode Activated***.
2. Notifikasi disampaikan ke seluruh personel melalui sistem komunikasi internal (portal DCIM, WA group, dan email broadcast).
3. **Security Team** segera menutup seluruh akses keluar/masuk.
4. **Tim Teknis** mengamankan sistem infrastruktur kritis (shutdown selektif jika perlu).
5. **NOC Team** melakukan pengalihan trafik dan memastikan kelangsungan layanan utama.
6. Penetapan **Critical Personnel** yang diizinkan tetap berada di lokasi.
7. Pencatatan waktu aktivasi dan kondisi awal dilakukan oleh **ICO**.

7. Prosedur Pelaksanaan Lockdown Mode

Tahapan	Tindakan Utama	Penanggung Jawab
Keamanan Akses	Menutup pintu DC APJII dan menghentikan aktivitas keluar/masuk.	Security
Keselamatan Personel	Evakuasi ke titik aman jika diperlukan; memastikan seluruh personel tercatat.	ERT Team
Proteksi Aset Kritis	Menjaga kestabilan UPS, HVAC, fire suppression system.	Tim Teknis
Komunikasi & Koordinasi	Update status ke manajemen, pelanggan, dan otoritas terkait.	ICO & Sekretariat APJII
Monitoring Berkelanjutan	Memantau kondisi lingkungan dan sistem melalui sistem monitoring.	NOC & Tim Teknis
Dukungan Logistik	Menyediakan makanan, air, dan kebutuhan dasar bagi critical personnel.	Sekretariat APJII
Larangan	Tidak diperkenankan membuka akses, melakukan perbaikan, atau menerima tamu eksternal selama lockdown tanpa izin IC.	Semua pihak

8. Komunikasi dan Pelaporan

1. Komunikasi internal dilakukan melalui kanal resmi (portal DCIM, WA Group, Teams, email broadcast).
2. Komunikasi eksternal dengan pelanggan dilakukan hanya oleh pihak berwenang (NOC APJII/Sekretariat APJII).
3. Semua kejadian dan keputusan selama lockdown harus terdokumentasi dalam **Incident Report Log**.
4. Laporan awal **(Initial Incident Report)** wajib disampaikan ke manajemen maksimal 1 jam setelah aktivasi.
5. Laporan lengkap **(*Post Incident Report*)** harus disusun maksimal 48 jam setelah lockdown dicabut.

9. Deaktivasi / Pembatalan Lockdown Mode

1. **ICO** menilai bahwa ancaman telah hilang atau kondisi kembali aman.
2. Melakukan koordinasi dengan otoritas terkait untuk verifikasi keamanan.
3. Menyampaikan pengumuman resmi ***"Lockdown Mode Deactivated"***.
4. Melaksanakan proses **Recovery & Normalization**, meliputi:
    - Pemeriksaan sistem listrik, pendingin, keamanan fisik.
    - Reaktivasi akses kontrol.
    - Evaluasi dampak operasional dan laporan kerusakan.

5. Melakukan *post-incident debriefing meeting* untuk perbaikan SOP ke depan.

10. Evaluasi dan Pembelajaran

- Setelah setiap kejadian lockdown, dilakukan **Post-Incident Review Meeting** dalam waktu maksimal 7 hari.
- Hasil evaluasi menjadi dasar untuk memperbarui SOP, pelatihan personel, serta peningkatan sistem keamanan dan BCP.
- Hasil evaluasi dilaporkan ke manajemen dan unit audit internal.

11. Dokumentasi dan Rekaman

Dokumen yang wajib dibuat:

- Formulir Aktivasi Lockdown
- Daftar Critical Personnel
- Incident Report Log
- Communication Log
- Recovery Checklist
- Post-Incident Report

Semua dokumen harus disimpan minimal **5 tahun** dan menjadi bagian dari arsip **Business Continuity Documentation**.

12. Pelatihan dan Uji Coba (Drill)

- Pelatihan *Lockdown Mode Procedure* dilakukan **minimal 2 kali per tahun**.
- Simulasi gabungan (BCP Drill & ERP Drill) wajib melibatkan seluruh divisi dan vendor utama.
- Evaluasi hasil simulasi harus dituangkan dalam laporan tertulis untuk perbaikan prosedur.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXX
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP LOCKDOWN MODE PADA KEJADIAN KAHAR/FORCE MAJEURE GANGGUAN TEKNIS BESAR (LISTRIK, PENDINGIN, & TELEKOMUNIKASI) DATA CENTER APJII

1. Pendahuluan

Data Center APJII sebagai pusat layanan infrastruktur telekomunikasi nasional harus menjamin **ketersediaan, keamanan, dan keberlangsungan layanan (availability, integrity, continuity)** meskipun terjadi gangguan besar (major disruption) akibat **kejadian kahar atau force majeure teknis**.

Salah satu mekanisme tanggap darurat kritikal adalah **aktivasi "Lockdown Mode"**, yaitu kondisi operasional tertutup dan terbatas, di mana seluruh akses fisik dan operasional dikontrol ketat untuk menjaga stabilitas sistem dan keamanan infrastruktur selama masa gangguan besar.

SOP ini menjadi panduan utama bagi seluruh personel dalam mengelola kondisi Lockdown Mode akibat gangguan teknis besar seperti:

- Kegagalan sistem kelistrikan utama dan cadangan (Power System Failure);
- Gangguan besar sistem telekomunikasi / jaringan utama (Network & Telco Failure);
- Kegagalan sistem pendingin utama dan cadangan (HVAC / Cooling System Failure).

2. Tujuan

Tujuan SOP ini adalah untuk:

1. Menetapkan langkah-langkah operasional dan keamanan selama aktivasi Lockdown Mode akibat gangguan teknis besar.
2. Meminimalkan dampak terhadap layanan data center dan sistem pelanggan.
3. Menjamin keselamatan personel, perangkat, serta data selama situasi kritis.
4. Menyediakan mekanisme komunikasi, pelaporan, dan eskalasi yang terstruktur.
5. Mendukung penerapan **Business Continuity Plan (BCP)** dan **Disaster Recovery Plan (DRP)** Data Center APJII.

3. Dasar dan Referensi Standar

SOP ini disusun berdasarkan standar dan acuan berikut:

- **TIA-942-C**: Telecommunications Infrastructure Standard for Data Centers.
- **ISO 22301:2019** – Business Continuity Management Systems (BCMS).
- **ISO/IEC 27001:2022** – Information Security Management Systems.
- **ISO/IEC 20000-1:2018** – IT Service Management.
- **NFPA 70 & 75** – Electrical & Fire Protection Standards for Data Centers.
- **Kebijakan Internal APJII:**
    - BCP & DRP Policy
    - Emergency Response Plan (ERP)
    - HSE & Security Policy
    - Operational Maintenance SOP PAC, Electrical, dan Network Systems

4. Definisi Istilah

Istilah	Definisi
Lockdown Mode	Kondisi darurat di mana akses fisik, operasional, dan komunikasi Data Center dikendalikan secara penuh oleh Emergency Response Team (ERT) untuk menjaga keamanan sistem dan keselamatan operasional.
Force Majeure Teknis	Gangguan besar yang terjadi karena kegagalan sistem utama atau pendukung (kelistrikan, pendingin, telekomunikasi) di luar kendali operasional normal.
ERT (Emergency Response Team)	Tim tanggap darurat yang terdiri dari perwakilan teknis, keamanan, dan manajemen yang bertanggung jawab selama masa insiden.
BCP (Business Continuity Plan)	Rencana yang menjamin kelangsungan operasional kritis selama gangguan besar.
DRP (Disaster Recovery Plan)	Prosedur pemulihan sistem dan layanan setelah gangguan besar.
Critical Infrastructure	Komponen utama data center seperti UPS, CRAC/CRAH, PDU, Switch Core, dan Network Backbone.
Incident Commanding Officer (ICO)	Penanggung jawab utama pengendalian situasi darurat dan pelaksanaan Lockdown Mode.
Authorized Personnel Only	Status pembatasan akses hanya bagi personel/individu yang ditunjuk dan memiliki izin langsung dari **ICO**.

5. Ruang Lingkup

Ruang lingkup SOP ini mencakup:

1. **Sistem yang Dilindungi:**
    - Sistem Kelistrikan (UPS, panel ACB, busbar, PDU, grounding).

    - Sistem Pendingin (PAC, CRAC Unit).
    - Sistem Telekomunikasi & Jaringan (router core, switch distribution, transmission fiber, MMR).
2. **Fase Operasional:**
    - Deteksi awal gangguan (Early Warning).
    - Aktivasi Lockdown Mode.
    - Pengamanan area kritis dan personel.
    - Koordinasi komunikasi internal & eksternal.
    - Pemulihan operasional dan normalisasi.
3. **Lokasi yang Dicakup:**
    - Seluruh area operasional Data Center APJII termasuk ruang server, MMR, NOC, ruang panel listrik, dan ruang pendingin.
4. **Personel Terlibat:**
    - Emergency Response Team (ERT).
    - Tim NOC.
    - Security.
    - Tim Teknis.
    - Manajemen APJII (untuk eskalasi).

6. Prosedur Umum Aktivasi Lockdown Mode

6.1. Deteksi dan Konfirmasi Gangguan

- Sistem monitoring mendeteksi anomali besar.
- Tim NOC/Tim Teknis yang sedang bertugas melakukan verifikasi cepat (<5 menit).
- Laporan dikirim ke ERT dan Incident Commanding Officer.
- Jika gangguan terverifikasi berdampak pada layanan utama, **ICO** mengumumkan **“Lockdown Mode Activated”**.

6.2. Aktivasi Lockdown Mode

- Akses pintu otomatis dikunci ke mode “Authorized Personnel Only”.
- Pengunjung dan vendor segera dievakuasi ke zona aman.
- Semua kegiatan maintenance, delivery, dan akses fisik ditunda dan diberhentikan.
- Tim teknis tetap di dalam area jika diperlukan untuk menjaga stabilitas sistem kritis.

6.3. Koordinasi dan Komunikasi

- **ICO** memimpin koordinasi melalui saluran komunikasi darurat (WA Group, Portal DCIM, Email).
- Sekretariat APJII menginformasikan kondisi Lockdown kepada Anggota/Tenent dan otoritas sesuai protokol.
- Semua komunikasi eksternal harus disetujui oleh **ICO**.

6.4. Pengamanan Infrastruktur

- Security melakukan perimeter lockdown dan kontrol akses penuh.
- Tim Teknis memastikan isolasi sistem yang terganggu (misalnya bypass UPS atau transfer ke genset).
- Tim Teknis menstabilkan suhu ruangan datahall.

- Network engineer / Tim NOC memindahkan traffic ke jalur redundan bila memungkinkan.

6.5. Pemantauan & Dokumentasi

- Semua aktivitas dicatat dalam **Incident Log Book** (waktu, tindakan, personel, hasil).
- Sistem monitoring snapshot diambil setiap 10 menit selama insiden.
- **ICO** memastikan laporan status dikirim ke manajemen APJII setiap 15 menit.

6.6. Pemulihan dan Normalisasi

- Setelah sistem kritikal stabil lebih dari 2 jam tanpa anomali, **ICO** dapat menyatakan **Lockdown Mode Lifted (dicabut)**.
- Verifikasi pasca-insiden dilakukan untuk setiap sistem (power, cooling, network).
- Hasil evaluasi dicatat dalam laporan resmi ke Manajemen APJII.

7. Dokumentasi dan Pelaporan

- **Incident Report Form (IRF)** – diisi maksimal 12 jam setelah kejadian.
- **Post-Incident Review (PIR)** – disusun maksimal 3 hari setelah statusnya normal.
- **Lessons Learned Report** – disampaikan dalam rapat bulanan.
- Semua dokumen diarsipkan oleh **PIC/Penanggung Jawab Operasional DC APJII** dan diaudit secara berkala.

8. Evaluasi dan Review

- SOP ini direview minimal **1 kali per tahun** atau setelah terjadi insiden besar.
- Uji coba simulasi Lockdown Mode dilakukan minimal **2 kali per tahun** untuk memastikan kesiapan sistem dan personel.
- Evaluasi hasil simulasi dijadikan dasar revisi SOP dan peningkatan prosedur keamanan operasional.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXXI
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP LOCKDOWN MODE PADA KEJADIAN KAHAR/FORCE MAJEURE YANG DIAKIBATKAN OLEH TINDAKAN MANUSIA DATA CENTER APJII

1. Pendahuluan

Kejadian Kahar (Force Majeure) akibat tindakan manusia seperti peperangan, terorisme, kerusuhan, pemogokan, atau sabotase dapat menimbulkan ancaman serius terhadap keselamatan personel, keamanan aset fisik, dan keberlangsungan operasional Data Center APJII.
Untuk mengantisipasi dan meminimalkan risiko tersebut, diterapkan **SOP Lockdown Mode**, yaitu prosedur tanggap darurat yang mengatur pembatasan penuh akses fisik ke seluruh area data center serta pengamanan sistem dan personel di lokasi, serta harus mengaktifkan dengan segera setelah ada potensi ancaman yang terkonfirmasi atau perintah resmi dari Manajemen APJII / pihak berwenang.

2. Tujuan

Tujuan dari SOP ini adalah untuk:

1. Menjamin keselamatan personel yang berada di dalam fasilitas Data Center.
2. Melindungi infrastruktur kritikal seperti sistem IT, jaringan, dan sistem pendukung (HVAC, UPS, dan lain-lain).
3. Mencegah akses ilegal atau perusakan aset akibat ancaman manusia.
4. Menjaga kontinuitas layanan internet dan data center dalam situasi darurat nasional atau sosial.
5. Menetapkan mekanisme komunikasi, komando, dan koordinasi selama mode lockdown.
6. Memastikan pemulihan operasional dapat dilakukan dengan aman setelah situasi terkendali.

3. Dasar dan Referensi Standar

SOP ini mengacu pada standar dan regulasi berikut:

1. **ISO 22301:2019** – Business Continuity Management System (BCMS).
2. **ISO/IEC 27001:2022** – Information Security Management System (ISMS).

3. **TIA-942-C** – Telecommunications Infrastructure Standard for Data Centers (Facility Rated-3/4 Security).
4. **NFPA 1600: Standard on Continuity, Emergency, and Crisis Management.**
5. **Undang-Undang No. 24 Tahun 2007** tentang Penanggulangan Bencana.
6. **Peraturan Pemerintah No. 21 Tahun 2008** tentang Penyelenggaraan Penanggulangan Bencana.
7. **Peraturan Kapolri** tentang Penanganan Keamanan Fasilitas Vital Nasional.
8. **Kebijakan Internal APJII** tentang Keamanan Fasilitas dan Perlindungan Infrastruktur Kritis.

4. Definisi Istilah

Istilah	Definisi
Lockdown Mode	Kondisi darurat di mana seluruh akses masuk dan keluar fasilitas ditutup total, dan semua personel diperintahkan untuk tetap berada di tempat aman sampai situasi dinyatakan terkendali.
Force Majeure (Kejadian Kahar)	Keadaan di luar kendali manusia yang mengakibatkan gangguan signifikan terhadap operasi, termasuk tindakan manusia seperti perang, terorisme, sabotase, atau kerusuhan sosial.
Incident Commanding Officer (ICO)	Personel yang ditunjuk untuk memimpin dan mengoordinasikan seluruh tindakan darurat saat lockdown diaktifkan.
Critical Infrastructure	Sistem vital data center seperti UPS, sistem pendingin (PAC), jaringan backbone, fire suppression, dan sistem keamanan.
Safe Zone	Area di dalam data center yang telah ditentukan sebagai titik aman bagi personel saat lockdown berlangsung.
Evacuation Route	Jalur evakuasi darurat yang hanya digunakan jika situasi mengancam langsung keselamatan jiwa.
Access Control System (ACS)	Sistem keamanan elektronik yang mengatur dan memantau keluar masuknya personel.
Command Center (CC)	Ruang kendali utama yang digunakan oleh tim tanggap darurat untuk mengoordinasikan seluruh tindakan selama lockdown.

5. Ruang Lingkup

Ruang lingkup penerapan SOP Lockdown Mode meliputi:

1. **Fasilitas yang tercakup:**
   - Area Datahall DC APJII
2. **Situasi yang memicu aktivasi Lockdown Mode:**

- **Peperangan:** Aktivitas militer yang mengancam fasilitas.
- **Terorisme:** Ancaman bom, serangan bersenjata, atau penyanderaan di sekitar fasilitas.
- **Kerusuhan:** Massa yang mendekati atau menyerang area data center.
- **Pemogokan:** Aksi mogok yang mengganggu operasional atau mengancam keselamatan petugas.
- **Sabotase:** Upaya perusakan atau penyusupan untuk menghancurkan sistem data center.

3. **Personel yang terlibat:**
   - Seluruh staf operasional (Tim Teknis, Security, NOC).
   - Tim Tanggap Darurat (ERT Team) APJII.
   - Manajemen APJII.
   - Pihak eksternal berwenang (POLRI, TNI, Security kawasan, pemadam kebakaran bila diperlukan).
4. **Tahapan pelaksanaan:**
   - **Deteksi dan Peringatan Dini.**
   - **Aktivasi Lockdown Mode.**
   - **Koordinasi Keamanan dan Komando.**
   - **Komunikasi dan Pelaporan.**
   - **Penanganan Personel dan Aset.**
   - **Pemulihan dan Normalisasi.**

6. Prosedur Pelaksanaan Lockdown Mode

Pelaksanaan Lockdown Mode dilakukan secara sistematis dan terkoordinasi untuk memastikan keselamatan personel dan keamanan infrastruktur data center. Proses ini dibagi menjadi **tujuh tahap utama**:

6.1. Tahap Deteksi dan Peringatan Dini

1. **Deteksi ancaman** dilakukan oleh Security atau NOC melalui sistem CCTV, laporan lapangan, atau informasi dari aparat keamanan.
2. **Jenis ancaman** dikategorikan:
   - Tingkat **Hijau (Siaga Awal):** indikasi potensi gangguan sosial atau keamanan di sekitar lokasi.
   - Tingkat **Kuning (Siaga Tinggi):** terdapat kerumunan, aksi massa, atau pergerakan mencurigakan dekat perimeter.
   - Tingkat **Merah (Lockdown Aktif):** ancaman langsung seperti penyerangan, sabotase, teror, atau kekerasan fisik.
3. Security melaporkan segera ke **ICO**.
4. Jika ancaman mencapai **tingkat Merah**, **ICO** menetapkan status **“Lockdown Mode Aktif”**.

6.2. Tahap Aktivasi Lockdown Mode

1. ICO mengumumkan aktivasi lockdown melalui sistem **portal DCIM, WA Group, Email broadcast**:

"Perhatian seluruh personel/vendor/visitor, kondisi darurat keamanan telah terjadi. **Lockdown Mode telah diaktifkan**. Mohon bantuan untuk semuanya tetap berada di dalam area aman dan menunggu arahan selanjutnya."

2. Sistem **Access Control System (ACS)** otomatis:
    - Mengunci seluruh pintu masuk dan keluar (kecuali jalur evakuasi darurat).
    - Menonaktifkan akses biometrik non-otoritatif.
3. Security berkoordinasi dengan pihak Gedung untuk memastikan tidak ada pergerakan masuk/keluar.
4. Semua personel **wajib tetap berada di Safe Zone** yang telah ditentukan (misalnya ruang NOC, ruang UPS atau shelter area).
5. **Server Room dan MMR** dikunci secara manual dan dipantau melalui CCTV aktif.
6. **ICO** berkoordinasi dengan **Pihak Berwenang (TNI/POLRI)** untuk pengamanan eksternal.

6.3. Tahap Komando dan Koordinasi

1. **ICO** memimpin **Command Center (CC)** untuk koordinasi antara tim internal dan eksternal.
2. Struktur komando internal:
    - **Incident Commanding Officer (ICO):** PIC / Penanggung Jawab Operasional DC APJII.
    - **Security:** Koordinasi pengamanan perimeter dan kontrol akses.
    - **Tim Teknis:** Memastikan sistem kritikal tetap berfungsi (UPS, PAC, jaringan).
    - **Sekretariat APJII:** Mengelola komunikasi internal dan eksternal.
    - **ERT Team / Tim Tanggap Darurat:** Menjamin keselamatan personel dan monitoring kondisi di Safe Zone.
3. Semua keputusan strategis selama lockdown dilakukan oleh **ICO** dengan komunikasi satu pintu.

6.4. Tahap Komunikasi dan Pelaporan

1. Semua komunikasi selama lockdown dilakukan melalui **kanal resmi dan terenkripsi** (radio UHF, internal VoIP, atau jaringan LAN secure).
2. Dilarang menggunakan media sosial pribadi untuk menyebarkan informasi.
3. Sekretariat APJII melakukan langkah-langkah berikut:
    - Mengirim notifikasi resmi ke **Manajemen APJII**.
    - Menghubungi pihak eksternal (Kepolisian, TNI, Pemadam Kebakaran, Otoritas Kawasan).
    - Menyampaikan status terkini setiap **15–30 menit** kepada manajemen.
4. Semua komunikasi dan log aktivitas disimpan dalam **Incident Log Sheet (ILS)**.

6.5. Tahap Penanganan Personel dan Aset

1. **Personel:**
    - Semua staf diwajibkan berlindung di **Safe Zone**
    - Tidak diperkenankan meninggalkan ruangan tanpa izin **ICO**.
    - Jika ada yang terluka, tim tanggap darurat **(ERT Team)** melakukan **first aid** dan melapor ke **ICO**.

2. **Aset & Infrastruktur:**
    - Sistem kelistrikan utama (UPS, ACB) tetap dijaga stabil oleh tim teknis.
    - PAC (Precision Air Conditioning) tetap beroperasi dalam mode efisiensi minimal jika diperlukan.
    - Server dan storage critical tetap online selama aman dari gangguan fisik.
    - Jika risiko potensi kebakaran meningkat, sistem **fire suppression & early warning smoke detection** tetap aktif otomatis.
3. **Keamanan Fisik:**
    - Security melakukan **pemantauan terbatas** di perimeter gedung untuk memastikan tidak ada pelanggaran perimeter.
    - Semua akses pintu darurat hanya dapat dibuka dengan otorisasi ICO.

6.6. Tahap Pemantauan dan Evaluasi Situasi

1. **ICO** memantau perkembangan situasi melalui CCTV eksternal, komunikasi aparat keamanan, dan laporan security.
2. Jika ancaman menurun, **ICO** melakukan koordinasi dengan aparat untuk menentukan **status penurunan ancaman (De-escalation)**.
3. Evaluasi risiko dilakukan setiap **30 menit** selama Lockdown Mode aktif.
4. **ICO** dapat memutuskan:
    - **Tetap Lockdown**, jika ancaman belum aman.
    - **Partial Lockdown**, membuka akses internal tapi tetap menutup perimeter luar.
    - **Normalisasi**, jika otoritas keamanan menyatakan situasi terkendali.

6.7. Tahap Pemulihan dan Normalisasi

1. Setelah situasi aman dan status Lockdown dicabut oleh **ICO**, dilakukan tahapan pemulihan:
    - Pemeriksaan menyeluruh kondisi fisik bangunan dan sistem keamanan.
    - Audit terhadap sistem kelistrikan, pendingin, jaringan, dan server untuk memastikan tidak ada kerusakan atau akses ilegal.
    - Validasi log keamanan dari ACS dan CCTV.
2. Personel diperbolehkan meninggalkan area setelah mendapat instruksi resmi.
3. ICO menyampaikan laporan **Post-Incident Summary** kepada Manajemen APJII dan Divisi BCP.
4. Aktivitas operasional kembali normal sesuai hasil **Post-Lockdown Safety Verification**.

7. Dokumentasi dan Pelaporan

1. Semua kejadian selama Lockdown dicatat dalam **Incident Log Sheet (ILS)** dan **Emergency Situation Report (ESR)**.
2. Dokumen yang wajib dibuat:
    - **Form Aktivasi Lockdown.**
    - **Log Komunikasi dan Keputusan ICO.**
    - **Laporan Personel di Safe Zone.**
    - **Rekaman CCTV dan Akses Elektronik.**
    - **Laporan Koordinasi Eksternal (Polisi/TNI).**
3. Semua laporan dikompilasi oleh Sekertariat APJII dan diserahkan ke Divisi BCP untuk arsip serta analisis lanjutan.

8. Evaluasi Pasca-Inisiden (Post-Incident Review)

1. Setelah situasi normal, dilakukan **rapat evaluasi (After Action Review)** paling lambat **3 hari kerja** setelah insiden.

2. Peserta evaluasi:
    - Manajemen APJII.
    - Incident Commanding Officer dan seluruh fungsi pendukung.
    - Tim Tanggap Darurat / **ERT Team**.
    - NOC & Tim Teknis.
3. Hasil evaluasi mencakup:
    - Efektivitas prosedur lockdown.
    - Respons personel terhadap perintah darurat.
    - Hambatan komunikasi dan koordinasi.
    - Rekomendasi peningkatan prosedur dan pelatihan ulang.
4. Hasil review dituangkan dalam dokumen **Post-Incident Evaluation Report (PIER)**.

9. Pelatihan dan Simulasi

1. Simulasi Lockdown Mode wajib dilakukan minimal **1 kali per tahun**, atau setiap ada perubahan sistem keamanan.
2. Pelatihan mencakup:
    - Aktivasi Lockdown Mode.
    - Prosedur evakuasi darurat.
    - Komunikasi krisis dan koordinasi tim.
    - Penggunaan alat keamanan (Access Control, radio, CCTV).
3. Hasil simulasi dicatat dalam **Training & Drill Report**, untuk evaluasi kesiapan personel.

10. Tanggung Jawab dan Wewenang

Jabatan / Fungsi	Tanggung Jawab
Incident Commanding Officer (ICO)	Mengaktifkan dan menonaktifkan Lockdown Mode, memimpin komando darurat.
Security	Mengamankan perimeter, mengunci akses, berkoordinasi dengan aparat keamanan.
Tim Teknis	Menjaga operasional sistem kritikal (UPS, PAC, genset, jaringan).
Sekretariat APJII	Mengelola komunikasi internal-eksternal, mendokumentasikan semua log.
ERT Team/Tim Tanggap Darurat	Mengawasi keselamatan personel dan menangani kondisi medis darurat.
Manajemen APJII	Memberikan dukungan strategis dan otorisasi tindakan tingkat tinggi.

11. Pengendalian Dokumen
    1. Dokumen SOP ini dikendalikan oleh **Sekretariat APJII**.
    2. Jika ada update SOP terbaru, maka harus disediakan oleh **Sekretariat APJII/ NOC, dan Security Post** dalam bentuk cetak dan digital dan disetujui oleh Manajemen APJII.
    3. Dokumen lama disimpan sebagai arsip selama **5 tahun**.

12. Penutup

SOP Lockdown Mode ini merupakan bagian vital dari sistem ketahanan operasional Data Center APJII dalam menghadapi risiko **tindakan manusia yang ekstrem dan tak terduga**. Implementasinya harus dilakukan dengan disiplin, koordinasi yang ketat, serta komunikasi yang jelas antar tim. Kepatuhan terhadap prosedur ini menjamin **keselamatan personel, keamanan aset nasional digital, serta kontinuitas layanan internet Indonesia**.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXXII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP LOCKDOWN MODE KEJADIAN KAHAR/FORCE MAJEURE PANDEMIC/EPIDEMI/GANGGUAN KESEHATAN MASSAL DATA CENTER APJII

1. Pendahuluan

Dalam operasional Data Center APJII yang berfungsi sebagai pusat infrastruktur internet nasional, kontinuitas layanan merupakan prioritas utama. Gangguan besar terhadap kesehatan masyarakat seperti **pandemi** atau **epidemi** (contoh: COVID-19, SARS, MERS, Avian Flu, dsb.) dapat mengancam keselamatan personel, menurunkan kapasitas operasional, dan berpotensi menyebabkan gangguan layanan.

Oleh karena itu, perlu diterapkan **SOP Lockdown Mode** sebagai langkah pengamanan dan pengendalian operasional Data Center APJII selama periode **Kejadian Kahar (Force Majeure)** terkait kesehatan. SOP ini menjadi pedoman resmi untuk seluruh staf, kontraktor, dan pihak ketiga yang berkegiatan di area Data Center dalam menjaga keberlangsungan layanan dan keselamatan seluruh personel.

2. Tujuan

Tujuan dari SOP ini adalah untuk:

1. Menetapkan mekanisme **Lockdown Mode Operation** dalam menghadapi pandemi atau epidemi yang berpotensi mengganggu keselamatan dan operasi Data Center.
2. Menjamin keselamatan seluruh personel Data Center APJII selama periode wabah.
3. Menjaga kelangsungan layanan (service continuity) Data Center melalui pembatasan akses, pengaturan shift, dan penerapan protokol kesehatan ketat.
4. Menyediakan panduan operasional, komunikasi, dan pemulihan setelah kondisi pandemi mereda.
5. Memastikan koordinasi efektif dengan otoritas kesehatan, regulator, dan klien Data Center.

3. Dasar dan Referensi Standar

SOP ini disusun berdasarkan standar, pedoman, dan regulasi berikut:

1. **ISO 22301:2019** – *Security and Resilience — Business Continuity Management Systems (BCMS)*

2. **TIA-942-C:2024** – *Telecommunications Infrastructure Standard for Data Centers* (clause: Operations & Management)
3. **ISO 45001:2018** – *Occupational Health and Safety Management Systems*
4. **ISO 27001:2022** – *Information Security Management Systems*
5. **Keputusan Menteri Kesehatan RI** tentang Penetapan Status Kedaruratan Kesehatan Masyarakat.
6. **Peraturan Pemerintah No. 21 Tahun 2020** tentang PSBB (Pembatasan Sosial Berskala Besar).
7. **Pedoman WHO dan CDC** terkait pencegahan penularan penyakit menular di fasilitas kerja tertutup.
8. **Kebijakan Internal APJII** terkait manajemen risiko operasional dan BCP Data Center.

4. Definisi Istilah

- **Lockdown Mode:**
  Kondisi operasional Data Center dengan pembatasan akses ketat terhadap personel, vendor, dan tamu; hanya personel penting yang diizinkan masuk untuk menjaga kelangsungan layanan.
- **Pandemi:**
  Wabah penyakit menular yang menyebar secara global dan ditetapkan oleh WHO sebagai pandemi.
- **Epidemi:**
  Wabah penyakit menular yang menyebar secara luas di wilayah tertentu dalam waktu yang relatif singkat.
- **Personel Esensial (Essential Personnel):**
  Tim minimal yang ditunjuk untuk tetap bertugas di lokasi untuk menjaga layanan data center tetap berjalan, meliputi teknisi on-site, operator, dan petugas keamanan.
- **Shift Karantina (Quarantine Shift):**
  Pola kerja di mana personel bertugas dalam periode tertentu (misalnya 14 hari) dengan isolasi di dalam area data center untuk mencegah kontak dengan pihak eksternal.
- **Disinfection Zone / Sanitation Area:**
  Area yang ditetapkan untuk sterilisasi tubuh, pakaian, dan barang sebelum masuk ke area operasional data center.
- **BCP (Business Continuity Plan):**
  Rencana kelangsungan bisnis yang memastikan Data Center tetap beroperasi selama dan setelah kejadian luar biasa.

5. Ruang Lingkup

SOP ini berlaku untuk seluruh kegiatan operasional di **Data Center APJII**, mencakup:

1. **Personel:**
   - Seluruh staf APJII yang bertugas di data center.
   - Kontraktor dan vendor pihak ketiga (maintenance, cleaning, security).
   - Tamu atau auditor yang memiliki izin masuk.
2. **Fasilitas:**
   - Seluruh area operasional (Data Hall, NOC, MMR, Power Room, PAC Room).
   - Area penunjang (ruang istirahat, pantry, gudang, lobi, dan parkir).
   - Jalur evakuasi dan area karantina internal.

3. **Sistem Operasional:**
    - Aktivitas monitoring dan kontrol infrastruktur.
    - Akses kontrol fisik dan sistem keamanan.
    - Proses disinfeksi, logistik, serta pengaturan shift operasional.
    - Komunikasi internal dan eksternal selama Lockdown Mode.
4. **Periode Penerapan:**
    - Saat **status darurat kesehatan** ditetapkan oleh pemerintah atau otoritas kesehatan.
    - Selama fase **respon pandemi aktif**, **pemulihan bertahap**, hingga **normalisasi operasional**.

6. Tanggung Jawab dan Kewenangan

Jabatan / Tim	Tanggung Jawab Utama
Incident Commanding Officer (ICO)	- Mengaktifkan status Lockdown Mode berdasarkan arahan manajemen APJII atau otoritas resmi. - Menentukan tingkat pembatasan akses (Total Lockdown, Partial Lockdown, Limited Access). - Menyetujui daftar personel esensial yang bertugas di lokasi. - Melakukan koordinasi langsung dengan manajemen pusat, tim BCP, dan pihak regulator.
ERT Team (Tim Tanggap Darurat)	- Menjalankan prosedur Lockdown sesuai rencana kontinuitas bisnis. - Memastikan ketersediaan personel pengganti (backup team). - Menyiapkan logistik dasar (makanan, obat, APD, disinfektan). - Mengelola komunikasi internal dan eskalasi insiden. - Menetapkan dan memantau penerapan protokol kesehatan (masker, suhu tubuh, disinfeksi, isolasi). - Melakukan pelaporan kesehatan personel harian. - Bekerja sama dengan otoritas kesehatan bila ada indikasi infeksi.
Security	- Mengatur dan membatasi akses ke area data center sesuai daftar personel esensial. - Melaksanakan screening kesehatan di pos masuk. - Mengamankan perimeter dan mencegah akses tidak sah selama lockdown.
Tim Teknis	- Menjaga keandalan infrastruktur utama (listrik, HVAC, UPS, genset, PAC). - Menjalankan prosedur monitoring jarak jauh bila diperlukan. - Menjamin ketersediaan bahan bakar, cadangan suku cadang, dan sistem pendingin. - Berkoordinasi dengan Vendor

Jabatan / Tim	Tanggung Jawab Utama
Tim NOC	- Melakukan remote monitoring, koordinasi dengan Anggota/Tenant, dan pelaporan insiden secara digital. - Mengatur shift personel on-site dengan minimal kontak fisik. - Menjaga komunikasi antar lokasi operasional (NOC pusat dan site).

7. Prosedur Pelaksanaan Lockdown Mode

Prosedur dijalankan dalam 3 (tiga) fase utama: **Aktivasi, Pelaksanaan, dan Pemulihan.**

7.1. Fase Aktivasi

Dilakukan ketika pandemi/epidemi telah ditetapkan oleh pemerintah atau otoritas resmi sebagai darurat kesehatan.

1. **Pemantauan Awal:**
   ERT Team melakukan penilaian risiko berdasarkan informasi Kemenkes, WHO, atau BNPB.
2. **Rapat Darurat:**
   ICO mengadakan rapat cepat (onsite/virtual) dengan **Manajemen APJII** untuk menentukan level Lockdown.
3. **Deklarasi Lockdown Mode:**
   Diumumkan oleh **Manajemen APJII/ICO** dan disebarkan ke seluruh personel, vendor, dan Anggota/Tenant.
4. **Persiapan Fasilitas:**
   - Sterilisasi seluruh area data center.
   - Penyediaan logistik (masker medis, hand sanitizer, makanan, obat, dan perlengkapan tidur untuk shift isolasi).
   - Pembuatan *Disinfection Zone* di pintu masuk utama.

7.2. Fase Pelaksanaan (Operasional Lockdown Mode)

- **Pembatasan Akses:**
  - Hanya personel esensial dengan izin resmi yang diizinkan masuk.
  - Pengunjung, vendor, dan klien dilarang onsite kecuali dengan izin tertulis dari ICO.
- **Penerapan Protokol Kesehatan Ketat:**
  - Pemeriksaan suhu tubuh dan kesehatan di pos masuk.
  - Kewajiban penggunaan masker dan sarung tangan.
  - Disinfeksi area kerja setiap 4 jam.
  - Pembatasan kapasitas ruang (maks. 1 orang per 4 m^2).
- **Pengaturan Shift Isolasi:**
  - Rotasi kerja dengan pola 14 hari on-site (karantina) dan 14 hari off-site (istirahat rumah).
  - Personel yang on-site tidak boleh keluar area tanpa izin.

- **Pengelolaan Logistik:**
  - Pengantaran makanan dan kebutuhan dilakukan dengan sistem tanpa kontak fisik (*contactless delivery*).
  - Logistik disterilkan sebelum masuk ke zona bersih.
- **Monitoring Kesehatan Harian:**
  - Pengecekan suhu sesuai dengan anjuran pemerintah.
  - Jika ditemukan gejala (demam, batuk, sesak napas), personel segera diisolasi di ruang karantina internal.

7.3. Fase Pemulihan dan Normalisasi

Dilakukan ketika otoritas kesehatan mencabut status darurat atau angka kasus menurun stabil.

- Melakukan disinfeksi total seluruh area.
- Evaluasi seluruh personel yang bertugas selama lockdown.
- Mengembalikan jadwal kerja normal secara bertahap.
- Menyusun laporan evaluasi pelaksanaan Lockdown Mode untuk review manajemen.

8. Protokol Kesehatan dan Keselamatan Kerja

1. **Kebersihan Personel dan Area:**
   - Cuci tangan wajib sebelum masuk area kerja.
   - Gunakan hand sanitizer setiap 2 jam.
   - Penggantian masker setiap 4 jam atau bila lembab.
2. **Ventilasi dan HVAC:**
   - Sistem pendingin (PAC/CRAC) tetap beroperasi dengan filtrasi HEPA/UV jika tersedia.
   - Frekuensi pembersihan filter udara ditingkatkan.
3. **Isolasi dan Evakuasi Kesehatan:**
   - Personel yang sakit langsung diisolasi dan dikoordinasikan ke fasilitas kesehatan.
   - Jalur evakuasi khusus yang ditetapkan oleh pengelola Gedung untuk pasien suspek.
4. **Pencatatan & Pelaporan:**
   - Semua aktivitas kesehatan dicatat oleh HSE Officer.
   - Laporan harian disampaikan ke ICO dan Manajemen APJII. Apabila diperlukan dapat disampaikan ke petugas Pengendali Epidemi.

9. Komunikasi dan Eskalasi

Jenis Komunikasi	Media / Kanal	Tujuan
Internal (Tim On-site & Off-site)	WhatsApp Group, Radio HT, Email Operasional	Koordinasi kegiatan harian dan shift.
Manajemen APJII, ICO, ERT Team	Teleconference, Dashboard Monitoring	Pelaporan status operasional dan personel.

Jenis Komunikasi	Media / Kanal	Tujuan
Anggota / Tenant DC	Email resmi, Portal DCIM	Informasi status layanan dan akses terbatas.
Pemerintah / Otoritas Kesehatan	Surat resmi, Email	Pelaporan kondisi darurat kesehatan dan tindakan pencegahan.

10. Dokumentasi dan Pelaporan

Seluruh kegiatan selama Lockdown Mode wajib terdokumentasi:

1. **Formulir Harian:**
    - Catatan suhu tubuh dan kondisi personel.
    - Laporan shift pergantian dan sanitasi.
2. **Laporan Insiden Kesehatan:**
    - Disusun bila ditemukan kasus positif atau gejala mencurigakan.
3. **Laporan Akhir Lockdown Mode:**
    - Disusun oleh BCP & HSE Team setelah status darurat dicabut.
    - Berisi analisis efektivitas, hambatan, dan rekomendasi perbaikan.
4. **Audit Internal & Review BCP:**
    - Dilakukan pasca-insiden untuk meningkatkan kesiapsiagaan di masa depan.

11. Pelatihan dan Sosialisasi

- **Pelatihan Berkala:**
    - Simulasi prosedur Lockdown dan protokol kesehatan minimal 1x per tahun.
    - Edukasi pencegahan penyakit menular dan penggunaan APD.
- **Sosialisasi:**
    - Informasi disebarkan melalui email, papan pengumuman, dan briefing harian.
- **Evaluasi Kompetensi:**
    - HSE Officer melakukan evaluasi pemahaman seluruh personel setiap kuartal.

12. Evaluasi dan Review Berkala

1. **Evaluasi Rutin:**
    - Dilakukan setiap 6 bulan oleh ERT Team.
    - Meninjau kesiapan fasilitas, APD, dan sistem komunikasi.
2. **Review Pasca-Insiden:**
    - Setelah kejadian pandemi berakhir, dilakukan *After Action Review (AAR)*.
    - Diperbarui jika ada perubahan regulasi kesehatan atau kebijakan nasional.
3. **Dokumentasi Perubahan:**
    - Semua revisi SOP harus disetujui oleh Manajemen APJII.
    - Versi dokumen dikontrol melalui sistem dokumentasi internal.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXXIII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP LOCKDOWN MODE KEJADIAN KAHAR/FORCE MAJEURE BERDASARKAN KEBIJAKAN PEMERINTAH DATA CENTER APJII

1. Pendahuluan

Situasi **Kejadian Kahar (Force Majeure)** dapat terjadi akibat kebijakan atau instruksi resmi pemerintah, seperti **Pembatasan Sosial Berskala Besar (PSBB), Pemberlakuan Pembatasan Kegiatan Masyarakat (PPKM), penetapan status Bencana Non-Alam, hingga penutupan atau blokade akses terhadap kawasan Gedung Cyber-1**.

Kondisi tersebut termasuk dalam kategori **keadaan luar biasa (extraordinary circumstances)** yang berada di luar kendali APJII maupun pihak Anggota/Tenant dan tidak dapat diprediksi sebelumnya, serta dapat menghambat pelaksanaan kewajiban operasional Data Center yang normal.

Untuk menjaga **keselamatan personel**, **keamanan aset dan infrastruktur**, serta **kelangsungan layanan kritikal**, maka diperlukan **prosedur baku (Standard Operating Procedure)** dalam mengaktifkan dan melaksanakan **Lockdown Mode Data Center APJII** berdasarkan kebijakan pemerintah.

2. Tujuan

SOP ini disusun untuk:

1. Menetapkan mekanisme dan tahapan pelaksanaan **Lockdown Mode** di Data Center APJII selama masa Kejadian Kahar berdasarkan kebijakan pemerintah.
2. Memastikan **keamanan operasional, ketersediaan layanan, dan perlindungan aset** selama periode pembatasan aktivitas atau penutupan akses.
3. Memberikan panduan **koordinasi antar unit internal, tenant, serta pihak eksternal** (pemerintah, pengelola gedung, aparat keamanan, dan mitra teknis).
4. Menjaga **kepatuhan terhadap kebijakan pemerintah dan regulasi terkait K3, darurat nasional, serta manajemen BCP/DRP**.
5. Mendukung implementasi **Business Continuity Plan (BCP)** agar layanan tetap berjalan dalam kondisi minimum yang aman.

3. Dasar dan Referensi Standar

Pelaksanaan SOP ini mengacu pada standar dan regulasi berikut:

a. Regulasi Nasional

1. Undang-Undang No. 24 Tahun 2007 tentang Penanggulangan Bencana.
2. Undang-Undang No. 11 Tahun 2008 dan No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.
3. Peraturan Pemerintah No. 21 Tahun 2008 tentang Penyelenggaraan Penanggulangan Bencana.
4. Peraturan Pemerintah No. 23 Tahun 2020 tentang PSBB.
5. Keputusan Presiden dan/atau Instruksi Pemerintah terkait **status darurat nasional, pandemi, atau bencana non-alam.**
6. Pedoman Keselamatan dan Kesehatan Kerja (K3) Kementerian Ketenagakerjaan.
7. Panduan Gugus Tugas Nasional/BNPB tentang Protokol Darurat dan Pembatasan Aktivitas.

b. Standar dan Pedoman Teknis

1. **TIA-942-C**: Telecommunications Infrastructure Standard for Data Centers.
2. **ISO 22301:2019** – Business Continuity Management Systems.
3. **ISO 27001:2022** – Information Security Management.
4. **NFPA 75 & 76** – Fire Protection and Telecommunications Facilities.
5. **K**ebijakan internal APJII terkait keamanan operasional data center.

4. Definisi Istilah

Istilah	Definisi
Kejadian Kahar / Force Majeure	Keadaan luar biasa di luar kendali manusia seperti bencana alam, kebijakan pemerintah, perang, kerusuhan, pandemi, atau kejadian lain yang menyebabkan gangguan signifikan terhadap operasi.
Lockdown Mode	Kondisi operasional terbatas di mana seluruh atau sebagian aktivitas fisik di Data Center dibatasi, hanya personel esensial yang diizinkan masuk, dan sistem dioperasikan secara remote.
PSBB/PPKM/Bencana Non-Alam	Kebijakan resmi pemerintah untuk membatasi pergerakan manusia dalam rangka mitigasi risiko atau bahaya non-alam lainnya.
Anggota/Tenant	Pihak pengguna layanan Data Center APJII, termasuk penyewa rak, cage, atau konektivitas jaringan.

Istilah	Definisi
Tim Operasional Kritis (Critical Operation Team - COT) / Tim Teknis	Tim terbatas yang bertugas menjaga kelangsungan operasional vital (power, cooling, network, security) selama masa Lockdown.
Gedung Cyber-1 Management	Pihak pengelola gedung yang bertanggung jawab terhadap akses fisik, keamanan umum, dan kebijakan fasilitas bersama.
BCP/DRP	Business Continuity Plan dan Disaster Recovery Plan, panduan untuk menjaga kelangsungan layanan dan pemulihan setelah gangguan besar.

5. Ruang Lingkup

SOP ini mencakup seluruh tahapan dan area operasional yang terkait dengan pengelolaan Data Center APJII di **Gedung Cyber-1**, antara lain:

1. **Area Cakupan Operasional:**
   - Data Hall APJII yang berlokasi di Gedung Cyber-1.
2. **Jenis Kejadian yang Dicakup:**
   - **Kebijakan Pemerintah:** PSBB, PPKM, Lockdown wilayah, pembatasan perjalanan, atau penutupan sementara kawasan.
   - **Bencana Non-Alam:** pandemi, epidemi, atau kontaminasi biologis yang mengancam keselamatan staf.
   - **Gangguan Akses Fasilitas:** blokade jalan, isolasi kawasan, atau larangan masuk ke Gedung Cyber-1 akibat kebijakan pemerintah atau keamanan nasional.
3. **Aspek Pengelolaan yang Diatur:**
   - Aktivasi dan de-aktivasi **Lockdown Mode.**
   - Pengendalian akses dan izin kerja untuk **personel esensial.**
   - Pengaturan ***remote operation*** sistem monitoring dan helpdesk.
   - Komunikasi internal-eksternal serta pelaporan kepada manajemen dan regulator.
   - Pelaksanaan prosedur **keselamatan kerja (K3) dan protokol kesehatan.**
   - Koordinasi dengan pihak **pengelola gedung, keamanan, dan tenant**

6. Tanggung Jawab dan Kewenangan

6.1. Manajemen APJII.

- Menetapkan kebijakan resmi aktivasi dan de-aktivasi Lockdown Mode.
- Berkoordinasi dengan instansi pemerintah, BNPB, pengelola Gedung Cyber-1, dan aparat keamanan.
- Mengeluarkan surat tugas atau izin khusus bagi personel yang harus tetap bekerja on-site.
- Menjamin implementasi standar keselamatan kerja dan keamanan data selama masa Lockdown.
- Melakukan review dan evaluasi pasca-aktivasi Lockdown Mode.

6.2. PIC/Penanggung Jawab Operasional DC APJII.

- Memastikan seluruh sistem infrastruktur (power, cooling, fire, network) beroperasi stabil dalam mode terbatas.
- Melakukan penjadwalan rotasi personel shift kritis untuk menghindari kelelahan dan paparan risiko.
- Mengaktifkan sistem remote monitoring (BMS, NMS, CCTV) dari lokasi alternatif.
- Menetapkan komunikasi reguler (briefing, laporan status) ke manajemen setiap 6–12 jam.
- Menjamin kepatuhan terhadap protokol kesehatan, kebersihan, dan sterilisasi area kerja.

6.3. Tim Teknis.

- Menjaga kesinambungan fungsi utama Data Center: daya listrik, pendingin, jaringan, keamanan, dan pemantauan sistem.
- Melaksanakan pemeriksaan rutin sesuai jadwal terbatas.
- Melaporkan setiap anomali atau insiden segera ke Operation Manager dan BCP Team.
- Membatasi interaksi fisik dengan pihak eksternal, kecuali yang diizinkan secara resmi.

6.4. Security (Access Control Team).

- Mengontrol akses fisik ke area Data Center, hanya memperbolehkan personel dengan izin Lockdown Pass.
- Mencatat seluruh pergerakan masuk/keluar di logbook digital dan manual.
- Memastikan sistem keamanan (CCTV, alarm, akses biometrik) tetap aktif 24/7.
- Menjalin koordinasi langsung dengan pengelola Gedung Cyber-1 dan aparat keamanan setempat.

6.5. Anggota/Tenant.

- Menghormati kebijakan Lockdown Mode dan mematuhi prosedur pembatasan akses.
- Berkomunikasi dengan Sekretariat APJII untuk komunikasi darurat dan remote coordination.
- Melakukan kegiatan operasional secara remote kecuali mendapat izin khusus untuk on-site emergency.
- Bertanggung jawab menjaga keamanan data dan sistem mereka melalui akses jarak jauh yang aman.

7. Prosedur Pelaksanaan Lockdown Mode

7.1. Pemantauan dan Peringatan Dini

- PIC/Penanggung Jawab Operasional DC APJII memonitor situasi dan mengumpulkan informasi resmi dari pemerintah, BNPB, dan pengelola gedung.
- Apabila status darurat atau pembatasan resmi diberlakukan, maka disusun *Lockdown Risk Assessment Report*.
- Manajemen APJII menentukan status eskalasi:
    - **Level 1:** Kewaspadaan (situasi potensial, belum berdampak langsung).
    - **Level 2:** Pembatasan terbatas (akses fisik dikurangi, sistem remote aktif).
    - **Level 3:** Lockdown penuh (hanya Tim Teknis diizinkan masuk, layanan re-mote-only).

7.2. Aktivasi Lockdown Mode

- Keputusan resmi dikeluarkan oleh Manajemen APJII melalui memo internal dan komunikasi email resmi.
- Tim Teknis diberi arahan melalui briefing singkat secara daring.
- Pengelola Gedung Cyber-1 dan Anggota/Tenant diinformasikan secara tertulis.
- Akses fisik dibatasi sesuai level Lockdown.
- Sistem remote access dan sistem monitoring diaktifkan.
- Seluruh personel wajib mematuhi protokol kesehatan dan logistik (APD, sanitizer, disinfektan, konsumsi mandiri).

7.3. Operasional Selama Lockdown

- Tim Teknis bekerja dengan rotasi shift (maksimal 12 jam/shift) untuk mengurangi risiko kelelahan dan paparan.
- Pemeriksaan vital sistem dilakukan minimal 2 kali per hari:
    - Status UPS, genset, CRAC/CRAH, suhu dan kelembapan ruang, serta status jaringan backbone.
- Layanan helpdesk tetap aktif 24/7 melalui kanal remote.
- Semua kegiatan operasional dicatat di **Lockdown Operation Logbook** digital.
- Material dan logistik dikirim melalui titik drop-off yang disetujui oleh pengelola gedung.

7.4. Komunikasi dan Koordinasi

- Komunikasi internal dilakukan melalui kanal resmi: email, Teams, atau WhatsApp Group APJII.
- Update kondisi dikirim setiap 12 jam kepada manajemen APJII.
- Komunikasi eksternal ke Anggota/Tenant dilakukan melalui portal DCIM (ticketing system) dan broadcast email.
- Semua komunikasi harus terdokumentasi dengan baik (timestamp, pengirim, penerima, isi pesan).

7.5. Pengelolaan Keamanan dan Akses

- Sistem keamanan fisik (CCTV, alarm intrusion, access control) diaudit secara rutin oleh tim Security.
- Tidak ada tamu, vendor, atau kontraktor yang diizinkan masuk tanpa izin tertulis dari manajemen APJII.
- Jika perbaikan darurat dibutuhkan, vendor wajib mengikuti protokol ketat:
    - Surat tugas resmi dari perusahaan.
    - Screening kesehatan.
    - Pengawasan langsung oleh personel Tim Teknis.
    - Area isolasi pasca pekerjaan selesai.

8. Prosedur De-Aktivasi Lockdown Mode

- Keputusan pencabutan status Lockdown dikeluarkan oleh Manajemen APJII setelah:
    1. Pemerintah mencabut pembatasan atau status darurat.
    2. Gedung Cyber-1 kembali membuka akses normal.

3. Evaluasi keamanan dan kesiapan operasional dinyatakan aman.

Langkah-langkah de-aktivasi:

1. Mengumumkan resmi kepada semua tenant dan pihak eksternal.
2. Melakukan pembersihan menyeluruh (disinfeksi, sanitasi, pemeriksaan sistem).
3. Melakukan uji operasional penuh seluruh infrastruktur sebelum membuka kunjungan normal.
4. Mengarsipkan seluruh catatan operasional Lockdown (logbook, laporan status, foto, surat izin).
5. Melakukan briefing internal pasca-aktivasi untuk pembelajaran (lessons learned).

9. Protokol Kesehatan dan Keselamatan (K3) Selama Lockdown

1. Semua personel wajib mengenakan masker medis dan pelindung tambahan sesuai risiko.
2. Dilakukan pengecekan suhu tubuh dan log kesehatan sebelum dan sesudah shift.
3. Menyediakan ruang istirahat isolasi sementara bagi personel on-site.
4. Menjaga kebersihan tangan dan area kerja dengan disinfeksi rutin.
5. Menyediakan APAR dan emergency kit di setiap area penting.
6. Melaksanakan pelatihan singkat mengenai prosedur evakuasi darurat di tengah kondisi Lockdown.

10. Dokumentasi dan Pelaporan

1. Setiap kegiatan Lockdown dicatat dalam **Log Operasional Harian**.
2. Setiap insiden, gangguan, atau temuan dicatat dalam **Incident Report Form** dan dilaporkan ke Operation Manager.
3. Laporan periodik harian dikompilasi menjadi **Weekly Lockdown Report** untuk manajemen APJII.
4. Dokumentasi foto/video dilakukan hanya untuk kepentingan audit internal.
5. Semua dokumen disimpan minimal selama 3 tahun sebagai bukti pelaksanaan BCP/Force Majeure.

11. Evaluasi Pasca-Incident dan Pembaruan SOP

- Setelah masa Lockdown berakhir, dilakukan **Post-Incident Review** oleh PIC/Penanggung Jawab Operasional DC APJII untuk:
    - Mengevaluasi efektivitas prosedur Lockdown.
    - Mengidentifikasi kendala, risiko baru, dan peluang perbaikan.
    - Memperbarui SOP Lockdown berdasarkan hasil evaluasi dan perubahan kebijakan pemerintah.
- Hasil evaluasi dituangkan dalam **Laporan Evaluasi dan Rekomendasi Perbaikan** yang disetujui oleh Manajemen APJII.

12. Distribusi dan Pengendalian Dokumen

- Dokumen SOP ini termasuk dokumen **terkendali (Controlled Document)**.
- Salinan resmi didistribusikan ke:
    - PIC/Penanggung Jawab Operasinal DC APJII.

    - Tim Teknis &Tim NOC.
    - Security (Access Control Team).
    - Manajemen APJII.
    - Anggota/Tenant Representative (salinan terbatas)
- Setiap revisi diberi nomor versi dan tanggal efektif baru, serta disosialisasikan melalui komunikasi resmi APJII.

Penutup

SOP Lockdown Mode ini menjadi pedoman utama bagi seluruh personel dan tenant Data Center APJII dalam menghadapi situasi darurat non-alam akibat kebijakan pemerintah atau keadaan kahar lainnya. Dengan pelaksanaan yang disiplin dan terstruktur, diharapkan layanan Data Center tetap **aman, andal, dan berkelanjutan (Resilient & Secure Operation)** di tengah keterbatasan operasional.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXXIV
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP LOCKDOWN MODE KEJADIAN KAHAR/FORCE MAJEURE BENCANA ALAM DATA CENTER APJII

1. Pendahuluan

Data Center Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) merupakan fasilitas strategis nasional yang berfungsi sebagai pusat layanan infrastruktur internet dan data komunikasi nasional.
Dalam situasi **Kejadian Kahar (Force Majeure)** seperti **bencana alam (banjir, gempa bumi, badai, longsor, petir, atau fenomena alam ekstrem lainnya)**, keberlangsungan operasi Data Center harus dijaga dengan memastikan **keselamatan personel, keamanan infrastruktur, dan perlindungan aset kritikal**.

Untuk itu, diperlukan prosedur **Lockdown Mode**, yaitu mekanisme penghentian sementara seluruh akses eksternal dan pembatasan pergerakan internal secara terkontrol guna **meminimalisir risiko kerusakan, kebocoran keamanan, dan memastikan stabilitas operasional Data Center selama kondisi darurat berlangsung.**

2. Tujuan

SOP ini bertujuan untuk:

1. Menetapkan mekanisme aktivasi **Lockdown Mode** pada Data Center APJII selama terjadinya Kejadian Kahar / Force Majeure bencana alam.
2. Menjamin keselamatan seluruh personel di dalam fasilitas Data Center.
3. Melindungi peralatan IT, infrastruktur pendukung (listrik, pendingin, jaringan, keamanan), dan aset vital dari potensi kerusakan.
4. Mengatur proses komunikasi, koordinasi, dan otorisasi selama periode Lockdown.
5. Memastikan seluruh aktivitas yang dilakukan selama Lockdown tetap sesuai dengan standar keamanan dan keselamatan kerja.
6. Mempercepat proses pemulihan (recovery) setelah kondisi darurat berakhir.

3. Dasar dan Referensi Standar

SOP ini disusun berdasarkan pedoman dan standar berikut:

1. **TIA-942-C**: Telecommunications Infrastructure Standard for Data Centers — klausul mengenai *Physical Security, Monitoring, and Facility Management*.
2. **ISO 22301:2019** — Business Continuity Management Systems (BCMS).
3. **ISO 27001:2022** — Information Security Management Systems (ISMS).
4. **ISO 22320:2018** — Emergency Management — Guidelines for Incident Management.
5. **NFPA 1600** — Standard on Disaster/Emergency Management and Business Continuity Programs.
6. **Peraturan Pemerintah RI No. 24 Tahun 2007** tentang Penanggulangan Bencana.
7. **Peraturan Menteri Kominfo** terkait keamanan dan keandalan infrastruktur data.
8. **Kebijakan Internal APJII** tentang keamanan fisik, keselamatan kerja, dan kelangsungan bisnis (BCP/DRP Policy).

4. Definisi Istilah

Istilah	Definisi
Kejadian Kahar / Force Majeure	Peristiwa luar biasa di luar kendali manusia yang menyebabkan terganggunya operasional Data Center, seperti bencana alam, perang, terorisme, atau gangguan besar lain.
Lockdown Mode	Kondisi penguncian operasional fisik Data Center yang membatasi seluruh akses keluar-masuk, baik personel maupun pihak eksternal, serta menonaktifkan aktivitas non-esensial demi menjaga keamanan dan keselamatan.
Incident Commanding Officer (ICO)	Personel yang ditunjuk sebagai penanggung jawab utama saat situasi darurat/lockdown berlangsung.
Critical Systems	Sistem vital Data Center seperti UPS, CRAC/PAC, jaringan backbone, access control, CCTV, dan sistem monitoring.
Safe Zone	Area aman diluar dai Data Center yang digunakan sebagai tempat berlindung sementara selama kondisi bencana.
Emergency Shutdown (ESD)	Prosedur penghentian operasional sistem tertentu secara manual atau otomatis untuk mencegah kerusakan lebih lanjut.
All-Clear Signal	Pernyataan resmi dari Incident Commander bahwa kondisi darurat telah berakhir dan Lockdown Mode dapat dicabut.

5. Ruang Lingkup

SOP Lockdown Mode ini mencakup:

1. **Jenis Kejadian Kahar / Force Majeure**:
    - **Bencana Alam**: banjir, gempa bumi, badai, petir, tanah longsor, kebakaran akibat alam, atau fenomena cuaca ekstrem lainnya.

2. **Lokasi yang termasuk dalam cakupan Lockdown**:
    - Area Datahall DC APJII
3. **Personel yang terlibat**:
    - Petugas Operasional Data Center (NOC, Tim Teknis, PIC / Penanggung Jawab Operasional)
    - Tim Keamanan dan Keselamatan (Security & HSE)
    - Manajemen APJII dan Tim Tanggap Darurat (ERT)
    - Vendor kritikal jika diperlukan (atas izin ICO)
4. **Sistem yang dikendalikan selama Lockdown**:
    - Sistem kelistrikan utama & cadangan (UPS, ACB/MCCB, MDB)
    - Sistem pendingin (PAC/CRAC)
    - Sistem keamanan (CCTV, Access Control, Alarm, Intrusion Detection)
    - Sistem pemadam kebakaran (Fire Suppression & Early Warking Smoke Detection)
    - Sistem komunikasi dan jaringan backbone.
5. **Tahapan operasional yang diatur**:
    - Aktivasi Lockdown Mode
    - Pembatasan akses dan pergerakan
    - Pemantauan sistem dan kondisi lingkungan
    - Komunikasi dan pelaporan ke manajemen
    - Evaluasi pasca-incident dan pencabutan Lockdown.

6. Prinsip Umum Pelaksanaan Lockdown Mode

1. **Keselamatan manusia adalah prioritas utama.**
   Semua keputusan operasional harus mengutamakan keselamatan personel di dalam fasilitas.
2. **Stabilitas infrastruktur vital harus dijaga.**
   Sistem pendingin, sistem kelistrikan & sistem telekomunikasi harus tetap beroperasi pada level minimum yang aman.
3. **Tidak ada akses eksternal tanpa izin.**
   Semua pintu utama dikunci otomatis dan hanya dapat dibuka oleh Incident Commander.
4. **Komunikasi internal harus terjaga.**
   Gunakan radio komunikasi, telepon satelit, atau sistem komunikasi darurat jika jaringan utama terganggu.
5. **Dokumentasi wajib dilakukan.**
   Semua kejadian, tindakan, dan waktu harus dicatat dalam *Incident Log Book*.

7. Aktivasi Lockdown Mode

- **Trigger:** Alarm bencana alam, laporan otoritas (BMKG, BNPB), atau kondisi nyata di sekitar fasilitas.
- **Otorisasi:** Incident Commander (IC) dengan persetujuan Manajer Data Center.
- **Langkah awal:**
    1. Umumkan “Lockdown Mode” melalui sistem PA (Public Address) dan grup komunikasi internal.
    2. Kunci seluruh pintu masuk & aktifkan perimeter lockdown (security gate).
    3. Pindahkan personel ke area **Safe Zone**.
    4. Nonaktifkan aktivitas non-esensial dan hentikan pekerjaan lapangan/vendor.
    5. Monitor sistem listrik, pendingin, dan keamanan dari ruang kontrol.

8. Prosedur Pelaksanaan Lockdown Mode

8.1. Aktivasi Awal

1. **Deteksi Kejadian**
   - Sistem monitoring lingkungan (BMS, sensor banjir, seismic detector, atau peringatan BMKG) mendeteksi kondisi abnormal.
   - Security atau teknisi yang pertama kali mengamati kejadian wajib segera melaporkan ke **Incident Commander (ICO)** melalui jalur komunikasi darurat.
2. **Penilaian Awal (Initial Assessment)**
   - ICO menilai tingkat ancaman dan dampaknya terhadap fasilitas dan personel.
   - Jika kondisi berpotensi membahayakan keselamatan, IC **mengaktifkan Lockdown Mode**.
3. **Deklarasi Lockdown**
   - ICO mengumumkan melalui sistem **Public Address (PA)** atau komunikasi radio:

     "Perhatian, seluruh personel. Dinyatakan Lockdown Mode akibat kondisi darurat [jenis bencana]. Semua personel segera menuju area aman (Safe Zone)."

4. ***Oto*risasi**
   - Lockdown Mode hanya dapat diaktifkan oleh **ICO** atau **Ketum APJII** setelah mendapat konfirmasi dari minimal dua sumber terpercaya (sistem deteksi, otoritas, atau pengamatan langsung).

8.2. Tindakan Saat Lockdown Aktif

Area	Tindakan	Penanggung Jawab
Akses Fisik & Perimeter	- Kunci seluruh pintu utama dan sekunder secara otomatis melalui sistem access control. - Nonaktifkan sistem visitor management. - Aktifkan perimeter lockdown (pintu utama dan sekunder ditutup manual atau otomatis).	Security
Personel & Keselamatan	- Pindahkan seluruh personel ke *Safe Zone* yang telah ditetapkan. - Pastikan absensi personel di daftar hadir darurat. - Jika ada cedera, aktifkan protokol P3K dan hubungi fasilitas medis terdekat.	ERT Team
Sistem Kelistrikan	- Amankan sistem listrik utama. - Aktifkan mode *fail-safe* UPS dan genset. - Nonaktifkan beban non-kritis jika diperlukan untuk mencegah overheat.	Tim Teknis

Area	Tindakan	Penanggung Jawab
Sistem Pendingin (PAC/CRAC)	- Jalankan sistem pendingin pada mode minimum yang menjaga suhu optimal server (≤ 28°C). - Matikan unit non-esensial jika diperlukan untuk efisiensi daya.	Tim Teknis
Sistem Keamanan (CCTV, Alarm, Access Control)	- Pastikan seluruh CCTV tetap aktif dengan catu daya cadangan. - Pantau perimeter melalui Control Room.	NOC
Sistem Pemadam & Fire Suppression	- Pastikan sistem HSSD/VESDA aktif penuh. - Pastikan gas fire suppression siap digunakan.	Tim Teknis
Komunikasi Internal	- Gunakan radio HT, sistem PA, atau saluran komunikasi darurat. - Hindari penggunaan jaringan internet umum jika jaringan utama terganggu.	ICO/Sekretariat APJII

8.3. Monitoring Selama Lockdown

- Seluruh sistem vital dimonitor melalui BMS dan CCTV secara terus-menerus.
- Catat semua kejadian (waktu, kondisi, tindakan) ke dalam **Incident Log Sheet**.
- Update situasi kepada manajemen APJII minimal setiap **30 menit**.
- Dilarang membuka akses fisik tanpa izin ICO.

8.4. Kriteria Pencabutan Lockdown

Lockdown hanya dapat dicabut jika:

1. BMKG atau otoritas terkait menyatakan kondisi aman.
2. Tidak ada ancaman residual terhadap keselamatan personel dan infrastruktur.
3. Seluruh sistem kritikal dalam kondisi stabil.
4. ICO menyatakan **All Clear Signal** dan mendapatkan persetujuan **Manajer Data Center APJII**.

9. Struktur Tanggung Jawab dan Komando

Jabatan	Tanggung Jawab
Incident Commanding Officer (ICO)	Pengambil keputusan tertinggi selama Lockdown. Mengkoordinasikan semua tim dan komunikasi internal/eksternal.

Jabatan	Tanggung Jawab
PIC / Penanggung Jawab Operasional	Memberikan otorisasi formal atas aktivasi dan pencabutan Lockdown Mode.
Security	Menjamin penguncian perimeter, kontrol akses, dan keamanan fisik personel.
ERT Team	Menjamin keselamatan personel, evakuasi ke Safe Zone, dan pengawasan area berisiko.
Tim Teknis	Menjaga kestabilan sistem kelistrikan, UPS, genset, PAC/CRAC, serta melakukan shutdown aman jika perlu.
NOC/Sekretariat APJII	Menjaga komunikasi internal dan eksternal, termasuk pelaporan kepada manajemen APJII dan pihak berwenang.
Sekretariat APJII	Mencatat seluruh kronologi kejadian, log sistem, dan laporan pasca-insiden.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXXV
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP LOCKDOWN MODE KEJADIAN KAHAR/FORCE MAJEURE KEBAKARAN & PROSEDURAL PANIC MODE BUTTON DATA CENTER APJII

1. Pendahuluan

Kebakaran merupakan salah satu bentuk kejadian kahar (force majeure) yang memiliki potensi mengakibatkan kerusakan serius terhadap infrastruktur, sistem kelistrikan, dan data center secara keseluruhan. Dalam konteks operasional Data Center APJII, sistem **Lockdown Mode** dan **Panic Mode Button** berfungsi sebagai langkah tanggap darurat untuk memastikan keselamatan personel, melindungi aset kritis, serta meminimalkan risiko penyebaran api dan kerusakan sistem vital.

SOP ini menjelaskan secara rinci mekanisme pengaktifan **Lockdown Mode**, prosedur operasional **Panic Mode Button**, serta tata letak (placement) tombol darurat di area data center sesuai dengan standar keselamatan dan keamanan fasilitas data center kelas nasional.

2. Tujuan

Tujuan penyusunan SOP ini adalah untuk:

1. Menetapkan langkah-langkah operasional tanggap darurat saat terjadi kebakaran dalam lingkungan Data Center APJII.
2. Memastikan pelaksanaan **Lockdown Mode** dan **Panic Mode** berjalan terstruktur dan terkendali.
3. Melindungi personel, perangkat IT, dan infrastruktur fisik dari risiko kebakaran dan kontaminasi asap.
4. Menjamin koordinasi efektif antar personel keamanan, teknisi, dan manajemen tanggap darurat.
5. Mendukung penerapan **Business Continuity Plan (BCP)** dan **Disaster Recovery Plan (DRP)** pada kondisi force majeure.

3. Dasar dan Referensi Standar

SOP ini disusun mengacu pada standar dan pedoman berikut:

- **ISO 22301:2019** – Business Continuity Management System (BCMS)

- **ISO 27001:2022** – Information Security Management System (ISMS)
- **TIA-942-C** – Telecommunications Infrastructure Standard for Data Centers
- **NFPA 75** – Standard for the Fire Protection of Information Technology Equipment
- **NFPA 76** – Standard for the Fire Protection of Telecommunications Facilities
- **NFPA 101 (Life Safety Code)** – Panduan keselamatan penghuni dan evakuasi
- **SNI 03-1746-2000** – Tata Cara Perencanaan dan Pemasangan Sistem Deteksi dan Alarm Kebakaran pada Bangunan Gedung
- **Peraturan Menteri Tenaga Kerja No. PER.04/MEN/1980** – Tentang syarat-syarat pemasangan dan pemeliharaan sistem proteksi kebakaran
- **Peraturan Pemerintah No. 50 Tahun 2012** – Tentang Penerapan Sistem Manajemen K3

4. Definisi Istilah

Istilah	Definisi
Kejadian Kahar / Force Majeure	Peristiwa yang terjadi di luar kendali manusia seperti kebakaran, banjir, gempa bumi, atau peristiwa besar lain yang menyebabkan terganggunya operasional data center.
Lockdown Mode	Kondisi sistem keamanan fisik di mana semua akses masuk/keluar data center dikunci secara otomatis (fail-safe), untuk mencegah penyebaran bahaya dan menjaga keamanan area.
Panic Mode Button	Tombol darurat manual yang digunakan untuk memicu Lockdown Mode dan/atau alarm evakuasi saat kondisi berbahaya terdeteksi atau disaksikan oleh personel.
Fire Suppression System	Sistem otomatis penekan bahaya kebakaran yang diintegrasikan dengan detektor asap, panas, dan sistem alarm.
BMS (Building Management System)	Sistem terintegrasi yang mengontrol dan memonitor kondisi fasilitas (termasuk sistem HVAC, listrik, alarm, dan proteksi kebakaran).
Incident Commanding Officer (ICO)	Personel tanggung jawab utama dalam penanganan insiden darurat dan koordinasi tim tanggap darurat (ERT).
ERT (Emergency Response Team)	Tim internal yang dilatih khusus untuk melakukan tanggap darurat, evakuasi, dan pengamanan aset saat insiden terjadi.

5. Ruang Lingkup

SOP ini mencakup seluruh area dan sistem Data Center APJII, antara lain:

1. **Ruang lingkup area:**
    - Data Hall utama

2. **Ruang lingkup sistem dan kegiatan:**
    - Aktivasi Lockdown Mode otomatis & manual
    - Penggunaan dan lokasi Panic Mode Button
    - Prosedur koordinasi keamanan & evakuasi
    - Integrasi dengan sistem alarm & fire suppression
    - Komunikasi ke command center & pihak eksternal (pemadam, PLN, vendor maintenance)
    - Post-incident inspection & reporting

6. Penempatan Panic Mode Button

Penempatan tombol **Panic Mode Button** harus mengikuti prinsip **"visible, accessible, and protected"**, yaitu mudah dilihat, mudah dijangkau, namun terlindung dari aktivasi tidak sengaja.

A. Area dan Lokasi Penempatan:

1. **Ruang Data Hall** – 1 unit di setiap pintu keluar utama, dekat reader access control.

B. Karakteristik Teknis Panic Mode Button:

- Jenis: Push Button "Emergency Break Glass Type" dengan pelindung transparan.
- Warna: Merah (RAL 3020).
- Label: "Panic Mode / Emergency Lockdown".
- Tinggi pemasangan: 1,2 – 1,4 meter dari lantai.
- Terhubung langsung ke sistem monitoring dan ACS (Access Control System).
- Memiliki redundansi koneksi (fail-safe) dan status termonitor pada sistem monitoring.

7. Prosedur Pengaktifan Panic Mode Button

7.1 Kondisi Aktivasi

- Terjadi kebakaran yang terdeteksi secara visual atau oleh sistem smoke/heat detector.
- Terdapat ancaman langsung terhadap keselamatan personel atau peralatan.
- Alarm kebakaran otomatis aktif namun diperlukan penguncian manual area tertentu.

7.2 Langkah-langkah Operasional

1. **Tekan tombol Panic Mode Button** terdekat hingga terdengar bunyi klik dan alarm aktif.
2. Sistem akan mengirimkan sinyal ke **sistem monitoring dan Access Control System** untuk mengaktifkan **Lockdown Mode**.
3. **Pintu akses masuk akan terkunci otomatis**, sementara **pintu keluar darurat tetap terbuka secara fail-safe (exit push bar active)**.
4. Alarm audio-visual (sirine & strobe light) akan menyala di area yang terdampak.
5. **Fire Suppression System** akan masuk ke mode *pre-discharge* (delay 10–30 detik) menunggu konfirmasi otomatis dari sistem detektor kedua.
6. Personel di area terdampak segera **melakukan evakuasi** sesuai **jalur evakuasi yang ditentukan**.
7. **ERT dan Security** melakukan verifikasi lokasi api, memastikan semua personel keluar dengan aman.

8. Setelah situasi terkendali, **Incident Commanding Officer (ICO)** dapat menonaktifkan Lockdown Mode melalui panel kontrol.

8. Prosedur Lockdown Mode (Terintegrasi Sistem)

Tahap	Deskripsi Kegiatan	Tindakan Sistem
1. Deteksi Awal	Alarm asap/panas atau Panic Button aktif	Alarm lokal aktif, notifikasi ke sistem monitoring
2. Aktivasi Lockdown	Akses ke area tertutup dikunci (auto-lock)	ACS menutup seluruh akses masuk
3. Evakuasi Aman	Jalur keluar darurat terbuka fail-safe	Door release aktif hanya untuk exit
4. Isolasi Area Bahaya	Sistem HVAC otomatis shutdown di area terdampak	Mencegah sirkulasi asap ke area lain
5. Pemadaman Otomatis	Fire Suppression System discharge aktif	Pemadaman api berlangsung
6. Verifikasi & Normalisasi	ICO, ERT & Security lakukan inspeksi pasca insiden	Lockdown dinonaktifkan manual

9. Komunikasi dan Koordinasi

- **Level 1 (Internal):** ERT, Security, NOC, ICO.
- **Level 2 (Manajemen):** PIC/Penanggung Jawab Operasional DC APJII.
- **Level 3 (Eksternal):** Pemadam kebakaran, PLN, Vendor Fire System, dan pihak asuransi.

Semua komunikasi menggunakan jalur radio, telepon darurat, email, portal DCIM dan pesan prioritas sistem monitoring.

10. Post-Incident Recovery

1. Pastikan area dinyatakan aman oleh tim DAMKAR & **ICO**.
2. Lakukan **pemeriksaan sistem Lockdown dan Panic Mode Button** untuk memastikan fungsinya normal kembali.
3. Catat setiap kejadian, waktu aktivasi, personel penekan tombol, dan waktu pemulihan sistem.
4. Lakukan **evaluasi insiden** (post-incident review) untuk pembaruan SOP dan pelatihan ***Fire-Drill*** berikutnya.

11. Evaluasi dan Pelatihan

- Pelatihan ***Fire-Drill*** dilakukan **setiap 6 bulan sekali**.
- Uji fungsi Panic Mode Button dan Lockdown Mode dilakukan **setiap bulan** dalam jadwal pemeliharaan rutin.
- Evaluasi tahunan dilakukan untuk memastikan kesesuaian dengan update standar TIA-942-C dan NFPA terbaru.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXXVI
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PUBLIKASI INFORMASI DAN SOSIALISASI (AWARENESS) DATA CENTER APJII

1. Pendahuluan

Data Center APJII sebagai infrastruktur kritikal nasional membutuhkan manajemen komunikasi yang terstruktur dalam menyampaikan informasi kepada tenant, anggota, staf internal, maupun pihak eksternal. Publikasi informasi serta kegiatan sosialisasi (awareness) harus dilakukan secara terkontrol, akurat, dan sesuai standar keamanan informasi. Untuk itu, dibutuhkan SOP yang mengatur prosedur publikasi dan sosialisasi agar tidak menimbulkan kebingungan, kebocoran informasi, maupun risiko reputasi.

2. Tujuan

- Menjamin **informasi resmi Data Center APJII** disampaikan secara akurat, konsisten, dan tepat waktu.
- Memberikan **kesadaran (awareness)** kepada Anggota/Tenant, staf, dan pihak terkait mengenai kebijakan, prosedur, atau perubahan penting.
- Mengatur **koordinasi internal** antara Data Center Operation dengan **Humas APJII** dalam publikasi eksternal.
- Mengurangi risiko misinformasi, kebocoran informasi, dan gangguan operasional akibat publikasi tidak resmi.

3. Dasar & Referensi Standar

- **ISO/IEC 27001** – Information Security Management System (A.7, A.13 – Awareness & Communications).
- **ISO/IEC 27002** – Controls for communication security.
- **ISO 22301** – Business Continuity (komunikasi dan awareness dalam situasi darurat).
- **TIA-942-C** – Data Center Facility Standard (bagian terkait operational procedures & documentation).
- **Kebijakan Internal APJII** mengenai tata kelola komunikasi & publikasi.

4. Definisi Istilah

- **Publikasi Informasi**: Penyampaian informasi resmi melalui media cetak, elektronik, email, portal, atau media sosial APJII.

- **Sosialisasi (Awareness)**: Kegiatan penyuluhan, pelatihan singkat, atau komunikasi terjadwal yang bertujuan meningkatkan pemahaman anggota/tenant/staf terkait kebijakan atau prosedur Data Center.
- **Sekretariat APJII**: Divisi resmi yang bertanggung jawab atas komunikasi eksternal, media relations, dan publikasi resmi organisasi.
- **Internal Memo**: Informasi resmi yang hanya ditujukan untuk lingkup internal staf Data Center APJII.
- **External Communication**: Informasi resmi yang disampaikan ke tenant, anggota APJII, atau publik luas.

5. Ruang Lingkup

SOP ini berlaku untuk:

- Semua bentuk **publikasi informasi** terkait operasional Data Center APJII wajib mendapatkan persetujuan dari Manajemen APJII.
- Proses **sosialisasi (awareness)** terkait kebijakan, prosedur, SLA, dan insiden.
- Media komunikasi: email resmi, portal DCIM, laporan berkala, media sosial resmi APJII (dikoordinasikan dengan pihak Sekretariat APJII).
- Pihak internal (staf APJII) dan eksternal (tenant, anggota, vendor, regulator).

6. Klasifikasi Informasi

1. **Internal Only** – Informasi terbatas pada divisi terkait dan meminta persetujuan dari Manajemen APJII.
2. **Anggota/Tenant Communication** – Informasi untuk tenant/anggota (contoh: jadwal maintenance, perubahan SLA, upgrade layanan, permintaan layanan baru).
3. **Public Communication** – Informasi untuk publik/regulator/media, **harus melalui Sekretariat APJII** dan sudah disetujui oleh Manajemen APJII.

7. Prosedur Publikasi Informasi

1. **Identifikasi Informasi**
    - Tim Teknis mengajukan kebutuhan publikasi (misalnya: jadwal maintenance, update kebijakan, laporan insiden).
2. **Drafting Konten**
    - Draft disusun oleh tim Tim Teknis.
    - Konten harus jelas, ringkas, bebas dari istilah ambigu.
3. **Review Internal**
    - Diverifikasi oleh **PIC/Penanggung Jawab Operasional DC APJII**.
    - Informasi diklasifikasikan (internal, tenant, publik).
4. **Koordinasi dengan Sekretariat APJII**
    - Untuk komunikasi eksternal/publik → wajib koordinasi dengan **Sekretariat APJII**.
    - Humas APJII melakukan editing, branding, dan menentukan media publikasi.
5. **Distribusi/Penyebaran**
    - Internal → memo/email/portal DCIM.
    - Anggota/Tenant → email resmi, portal DCIM, WhatsApp group resmi (jika ada).
    - Publik → media sosial resmi APJII, pres-release, atau website APJII.
6. **Arsip & Dokumentasi**
    - Semua publikasi disimpan di repository internal (dokumen + log distribusi).

- Penyimpanan arsip & dokumentasi, minimal **3 tahun**.

8. Prosedur Sosialisasi (Awareness)

1. **Perencanaan**
   - Tim Teknis/NOC membuat rencana awareness (bulanan/kuartalan) terkait kebijakan, keamanan, dan layanan baru.
2. **Materi**
   - Materi disiapkan dalam bentuk presentasi, video singkat, info singkat (infografis) atau flyer.
   - Disesuaikan dengan audiens (anggota/tenant, staf, vendor).
3. **Pelaksanaan**
   - Awareness dilakukan melalui:
     - Training singkat untuk staf.
     - Webinar/Meeting Online/Training untuk anggota/tenant.
     - Bulletin email berkala.
4. **Koordinasi dengan Sekretariat APJII**
   - Jika awareness perlu disampaikan ke media/regulator → wajib melalui Sekretariat APJII.
5. **Evaluasi**
   - Feedback dikumpulkan dari peserta.
   - Laporan hasil awareness disimpan oleh pihak PIC/Penanggung Jawab Operasional DC APJII.

9. Prosedur Koordinasi dengan Sekretariat APJII

- **Semua publikasi eksternal** (press release, berita media, posting sosial media) harus **disetujui oleh Manajemen APJII dan dirilis oleh Sekretariat APJII**.
- Sekretariat APJII menjadi satu-satunya pintu komunikasi resmi ke media dan publik.
- PIC/Penanggung Jawab Operasional DC APJII hanya menyampaikan data teknis/operasional untuk diproses oleh Sekretariat APJII.

10. Aturan Tambahan

- Tidak diperkenankan Tim Internal APJII melakukan publikasi di media sosial pribadi terkait insiden, maintenance, atau data anggota/tenant.
- Semua publikasi harus menggunakan **logo, format, dan bahasa resmi APJII**.
- Informasi yang bersifat **confidential** tidak boleh dipublikasikan tanpa izin Manajemen APJII.

11. Catatan & Dokumentasi

- Setiap publikasi & sosialisasi wajib dicatat dalam **Log Publikasi Sekretariat APJII**.
- Evaluasi efektivitas publikasi & awareness dilakukan **setiap 6 bulan sekali**.

12. Alur Proses Publikasi & Sosialisasi

1. **Internal Initiation**
   - Tim Teknis / PIC / Penanggung Jawab Operasional DC APJII mengidentifikasi kebutuhan publikasi/sosialisasi (contoh: maintenance schedule, awareness training, kebijakan baru).
   - Draft konten awal dibuat oleh staf terkait/Tim Teknis.
2. **Review & Approval Internal**
   - Draft diverifikasi oleh **PIC/Penanggung Jawab Operasional DC APJII**.
   - Menentukan klasifikasi informasi: Internal, Anggota/Tenant, atau Publik.
3. **Koordinasi dengan Sekretariat APJII**
   - Jika informasi bersifat **eksternal/publik** → dikirim ke Sekretariat APJII.
   - Humas APJII melakukan editing & branding untuk media komunikasi resmi dari APJII.
4. **Distribusi / Sosialisasi**
   - **Internal** → memo/email/portal DCIM.
   - **Anggota/Tenant** → email resmi, portal DCIM, grup komunikasi resmi.
   - **Publik** → siaran pers, website resmi, media sosial APJII (oleh Sekretariat).
5. **Arsip & Dokumentasi**
   - Semua publikasi disimpan dalam **Log Publikasi Sekretariat APJII**.
   - Disertakan tanggal, isi konten, target audiens, dan media distribusi.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXXVII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENGALIHAN KEPEMILIKAN ASET DAN LAYANAN DATA CENTER APJII

1. Pendahuluan

Dalam operasional Data Center APJII, terdapat aset berupa perangkat ICT maupun layanan yang dikelola oleh anggota/tenant. Pada kondisi tertentu, aset atau layanan tersebut perlu dialihkan, baik karena berakhirnya kontrak layanan, akuisisi antar anggota, pemindahan layanan, maupun hibah. Proses pengalihan harus dilakukan secara terstruktur, terdokumentasi, dan sesuai kebijakan agar tidak menimbulkan sengketa hukum maupun risiko operasional.

2. Tujuan

- Menetapkan prosedur yang jelas terkait pengalihan kepemilikan aset & layanan.
- Melindungi kepentingan APJII, anggota, dan pihak ketiga dalam proses pengalihan.
- Memastikan keamanan fisik, logis, dan legal dari aset dan layanan yang dialihkan.
- Menjadi acuan resmi bagi staf APJII dalam menangani permohonan pengalihan.

3. Dasar & Referensi Standar

- **ISO/IEC 27001** – Information Security Management (Kontrol Aset & Akses).
- **ISO/IEC 20000-1** – IT Service Management (Service Transition & Asset Management).
- **TIA-942-C** – Data Center Standard (Facility & Security).
- **ISO 22301** – Business Continuity Management.
- Kebijakan Internal APJII tentang Pengelolaan Aset dan Layanan.
- Peraturan Perundangan terkait Hak Kekayaan dan Kepemilikan Aset di Indonesia.

4. Definisi Istilah

- **Aset**: Perangkat keras (server, switch, router, storage, dll.) atau perangkat lunak milik anggota/tenant yang ditempatkan di Data Center APJII.
- **Layanan**: Fasilitas yang diberikan APJII kepada anggota, misalnya colocation, interkoneksi, atau layanan Smarthand.
- **Pengalihan Kepemilikan**: Proses perpindahan hak kepemilikan perangkat/layanan dari satu pihak ke pihak lain dengan dokumen resmi.
- **Hibah**: Penyerahan aset atau layanan tanpa biaya dari satu pihak ke APJII atau pihak lain, dengan persetujuan tertulis.

- **Tenant Lama**: Anggota/instansi yang sebelumnya memiliki aset/layanan.
- **Tenant Baru**: Anggota/instansi penerima aset/layanan hasil pengalihan.

5. Ruang Lingkup

SOP ini berlaku untuk:

1. Pengalihan kepemilikan perangkat anggota APJII yang tidak diambil setelah berakhirnya layanan.
2. Pengalihan kepemilikan aset antar anggota APJII/instansi lain (misal akuisisi).
3. Pengalihan layanan antar anggota atau tenant.
4. Penerimaan hibah aset atau layanan.

6. Prosedur Pengalihan Kepemilikan Perangkat Anggota yang Tidak Diambil

1. **Pemberitahuan Resmi**
    - APJII mengirimkan surat resmi kepada anggota terkait pengambilan perangkat setelah kontrak berakhir (minimal **30 hari** sebelum tanggal efektif).
2. **Masa Tenggang**
    - Tenant diberikan waktu maksimal **30 hari kalender** setelah berakhirnya layanan untuk mengambil perangkatnya.
3. **Jika Tidak Diambil**
    - APJII mengeluarkan **Surat Pernyataan Surat Tidak Bertuan** terhadap aset yang tidak diambil, maka perangkat dianggap **Tidak Bertuan**.
4. **Tindakan APJII**
    - Aset yang **Tidak Bertuan**, maka akan menjadi hak milik APJII untuk ditentukan penggunaannya kemudian oleh APJII.
    - Semua tindakan didokumentasikan melalui **Berita Acara Aset**.

7. Prosedur Pengalihan Kepemilikan Aset antar Anggota/Institusi (Akuisisi)

1. **Pengajuan Permohonan**
    - Anggota/Tenant lama mengajukan surat resmi pengalihan kepemilikan perangkat kepada APJII.
    - Anggota/Tenant baru memberikan **Surat Pernyataan Penerimaan Aset**.
2. **Verifikasi APJII**
    - APJII memverifikasi legalitas kedua pihak.
    - Dilakukan pemeriksaan fisik aset.
3. **Dokumentasi Pengalihan**
    - Dibuat **Berita Acara Pengalihan Aset** yang ditandatangani kedua belah pihak dan APJII sebagai penghubung saja.
4. **Update Data**
    - Sistem manajemen kepemilikan dan layanan diperbaharui di portal DCIM APJII.
    - Kartu akses anggota/tenant lama terkait kepemilikan tersebut dicabut.

8. Prosedur Pengalihan Layanan

1. **Permohonan Resmi**
   - Anggota/Tenant lama mengajukan surat permohonan pengalihan layanan ke Anggota/Tenant baru.
   - Anggota/Tenant baru melampirkan dokumen legal perusahaan dan kebutuhan teknis.
   - Anggota/Tenant lama wajib menyelesaikan status outstanding finansialnya di APJII, dan Anggota/Tenant baru akan memverifikasi status outstanding tersebut.
2. **Analisis & Persetujuan**
   - Tim Admin NOC mengecek kontrak tenant lama & outstanding billing.
   - Tim Teknis/NOC mengecek ketersediaan kapasitas teknis.
   - Persetujuan diberikan oleh **PIC/Penanggung Jawab Operasional DC APJII**.
3. **Implementasi**
   - Layanan diputuskan dari tenant lama & dialihkan ke tenant baru sesuai jadwal.
   - UAT (User Acceptance Test) dilakukan bersama tenant baru.
4. **Dokumentasi**
   - Dibuat **Berita Acara Pengalihan Layanan** yang ditandatangani oleh tenant lama, tenant baru, dan PIC/Penanggung Jawab Operasional DC APJII.
   - Billing & SLA diperbaharui sesuai tenant baru.

9. Prosedur Penerimaan Hibah Permanen

1. **Pengajuan Hibah Permanen**
   - Pihak pemberi hibah permanen (anggota/tenant atau pihak luar) mengajukan surat resmi kepada APJII.
   - Disertai daftar aset/layanan yang akan dihibahkan secara permanen.
2. **Evaluasi APJII**
   - Tim Teknis/NOC melakukan pemeriksaan fisik perangkat.
   - Tim Kebendaharaan mencatat dan memverifikasi potensi implikasi biaya pengiriman (termasuk pajak) dari luar negeri ke Indonesia.
   - Tim Legal mengecek potensi implikasi hukum (jika ada).
3. **Persetujuan Manajemen**
   - Manajemen APJII memutuskan apakah hibah permanen ini akan diterima/ditolak.
4. **Dokumentasi Hibah Permanen**
   - Dibuat **Berita Acara Serah Terima Hibah Permanen** yang ditandatangani kedua belah pihak.
   - Aset masuk ke inventaris resmi APJII.

10. Catatan & Dokumentasi

- Semua dokumen pengalihan (surat permohonan, berita acara, surat persetujuan, log teknis) harus diarsipkan minimal **5 tahun**.
- Pencatatan dilakukan pada **Sistem Asset Management & Service Management APJII**.

Alur Proses Pengalihan Kepemilikan Aset & Layanan Data Center APJII

1. Prosedur Aset Tidak Diambil Setelah Layanan Berakhir

Alur:

1. **Notifikasi Pertama** – APJII mengirimkan surat pemberitahuan ke tenant 30 hari sebelum kontrak berakhir.
2. **Berakhirnya Kontrak** – Tenant diwajibkan mengambil aset dalam waktu 30 hari kalender.
3. **Masa Tenggang** – Jika belum diambil, APJII kirim **Surat Teguran Kedua**.
4. **Status Abandoned Asset** – Jika tetap tidak diambil → aset dianggap ditinggalkan.
5. **Tindakan APJII**:
    - Opsi A → Pengalihan ke APJII (digunakan kembali/inventaris).
    - Opsi B → Dimusnahkan dengan berita acara resmi.
6. **Dokumentasi** – Semua tindakan dicatat dalam **Berita Acara Pengalihan/Pemusnahan**.

2. Prosedur Pengalihan Aset antar Anggota/Institusi (Akuisisi)

Alur:

1. **Pengajuan Resmi** – Tenant lama mengirim surat permohonan pengalihan aset.
2. **Surat Penerimaan** – Tenant baru mengirim **Surat Pernyataan Penerimaan Aset**.
3. **Verifikasi APJII** – Legalitas kedua pihak & kondisi fisik perangkat diverifikasi.
4. **Approval** – Persetujuan Data Center Manager.
5. **Dokumentasi** – Dibuat **Berita Acara Pengalihan Aset** (tenant lama + tenant baru + APJII).
6. **Update Sistem** – Data kepemilikan diperbarui di sistem manajemen aset.
7. **Revokasi Akses** – Akses tenant lama terhadap perangkat tersebut dicabut.

3. Prosedur Pengalihan Layanan

Alur:

1. **Permohonan Resmi** – Tenant lama mengajukan permintaan pengalihan layanan → tenant baru melengkapi dokumen legal & teknis.
2. **Evaluasi Administrasi** – Tim CS mengecek kontrak & billing tenant lama.
3. **Evaluasi Teknis** – Tim Operasional mengecek ketersediaan kapasitas.
4. **Persetujuan** – Disetujui oleh Data Center Manager.
5. **Implementasi Teknis** – Pemutusan layanan dari tenant lama → aktivasi ke tenant baru (sesuai jadwal/maintenance window).
6. **Testing (UAT)** – Pengujian bersama tenant baru.
7. **Dokumentasi** – Dibuat **Berita Acara Pengalihan Layanan**.
8. **Update Sistem** – Billing & SLA dialihkan ke tenant baru.

4. Prosedur Penerimaan Hibah Permanen

Alur:

1. **Pengajuan Hibah** Permanen– Pihak pemberi mengirimkan surat resmi ke APJII.
2. **Daftar Aset/Layanan** – Lampiran detail barang/jasa yang dihibahkan permanen.
3. **Evaluasi Teknis** – Tim Teknis/NOC memeriksa kondisi fisik/perangkat.
4. **Evaluasi Legal** – Tim Legal mengecek implikasi hukum kepemilikan.
5. **Approval Manajemen** – Manajemen APJII memutuskan terima/tolak hibah.

6. **Dokumentasi** – Dibuat **Berita Acara Serah Terima Hibah Permanen**.
7. **Update Sistem** – Aset masuk ke inventaris resmi APJII.

Ringkasan Flow (Singkat dalam 1 Tabel)

Prosedur	Start	Pihak Terlibat	Dokumen Akhir
Aset Tidak Diambil/Aset Tidak Bertuan	Notifikasi ke Anggota/Tenant	Anggota/Tenant, Tim Teknis/NOC & Tim Legal APJII	BA Pengalihan (Tidak Bertuan)
Pengalihan Aset (Akuisisi)	Surat Anggota/Tenant Lama	Anggota/Tenant lama, Anggota/Tenant baru, Tim Legal, Tim Kebendaharaan	BA Pengalihan Aset (Akuisisi)
Pengalihan Layanan	Surat Anggota/Tenant lama & Anggota/Tenant baru	Anggota/Tenant lama, Anggota/Tenant baru, Tim Legal, Tim Kebendaharaan	BA Pengalihan Layanan
Penerimaan Hibah Permanen	Surat Hibah Permanen	Pemberi Hibah Permanen, Tim Legal, Tim Kebendaharaan	BA Serah Terima Hibah Permanen

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXXVIII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENYELESAIAN PEKERJAAN MANAJEMEN TIKET DATA CENTER APJII

1. Pendahuluan

Manajemen tiket (Ticket Management) merupakan proses penting dalam operasional Data Center APJII untuk memastikan setiap insiden, permintaan layanan (service request), perubahan (change request), atau gangguan teknis tercatat, ditangani, dan diselesaikan sesuai dengan prosedur standar.

SOP ini menjadi panduan resmi dalam pengelolaan tiket mulai dari pembukaan (Opened Ticket), penanganan (Handling Ticket), hingga penutupan (Closed Ticket), termasuk proses eskalasi dan dokumentasi penyelesaian.

Penerapan sistem Ticket Management ini bertujuan untuk menjamin **traceability**, **accountability**, dan **continuous improvement** dalam pengelolaan layanan data center, baik untuk pelanggan internal maupun eksternal.

2. Tujuan

Tujuan dari SOP ini adalah:

1. Menetapkan prosedur yang terstandarisasi dalam proses pencatatan, penanganan, dan penyelesaian tiket di lingkungan Data Center APJII.
2. Menjamin bahwa setiap tiket ditindaklanjuti sesuai SLA (Service Level Agreement) dan OLA (Operational Level Agreement) yang berlaku.
3. Menyediakan dokumentasi lengkap untuk keperluan audit, evaluasi performa, dan peningkatan layanan berkelanjutan.
4. Menurunkan risiko kegagalan layanan akibat tidak terpantau atau terlambatnya penanganan insiden.
5. Meningkatkan efisiensi koordinasi antar tim (Tim Teknis/NOC, Tim Security, Tim Vendor Support) melalui sistem tiket yang terintegrasi.

3. Dasar dan Referensi Standar

SOP ini disusun berdasarkan pada standar dan pedoman berikut:

1. **ISO/IEC 20000-1:2018** – Information Technology – Service Management System (ITSM).
2. **ISO/IEC 27001:2022** – Information Security Management System.
3. **ISO/IEC 27035-1:2016** – Information Security Incident Management.
4. **TIA-942-C** – Telecommunications Infrastructure Standard for Data Centers (Operation & Management).
5. **ITIL v4 Framework** – Service Operation & Continual Service Improvement.
6. **Kebijakan Operasional dan Pemeliharaan Data Center APJII.**
7. **Peraturan Internal APJII terkait Incident dan Problem Management.**

4. Definisi Istilah

Istilah	Definisi
Ticket	Catatan elektronik dalam sistem manajemen insiden yang mencatat setiap gangguan, permintaan, perubahan, atau kegiatan layanan.
Opened Ticket	Status tiket ketika insiden atau permintaan baru pertama kali dicatat dan diverifikasi oleh Tim NOC.
Assigned Ticket	Status tiket ketika telah ditugaskan kepada personel atau tim tertentu untuk ditindaklanjuti.
In-Progress Ticket	Status tiket yang sedang dalam proses penyelesaian oleh tim teknis.
Pending Ticket	Status tiket yang tertunda karena menunggu konfirmasi anggota/tenant, persetujuan perubahan, atau material/sparepart.
Resolved Ticket	Status tiket ketika penyelesaian telah dilakukan dan menunggu konfirmasi atau validasi dari pihak pelapor.
Closed Ticket	Status akhir tiket yang menandakan bahwa tiket telah diverifikasi penyelesaiannya dan dinyatakan selesai.
Re-Opened Ticket	Tiket yang dibuka kembali karena masalah yang sama muncul kembali dalam periode waktu tertentu.
SLA (Service Level Agreement)	Perjanjian tingkat layanan antara penyedia layanan (APJII) dan Anggota/Tenant terkait waktu respons dan waktu penyelesaian.
OLA (Operational Level Agreement)	Kesepakatan internal antar tim dalam organisasi untuk mendukung pemenuhan SLA.
Helpdesk APJII	Unit yang bertanggung jawab untuk menerima dan penanganan awal terhadap insiden, request, change, problem serta melakukan eskalasi ke bagian terkait.
Incident	Gangguan tak terduga yang mempengaruhi atau berpotensi mempengaruhi layanan normal.

Istilah	Definisi
Service Request	Permintaan layanan yang bersifat rutin, seperti permintaan akses, backup, atau laporan.

5. Ruang Lingkup

SOP ini berlaku untuk seluruh kegiatan pengelolaan tiket di lingkungan **Data Center APJII dan telah terintegrasi di dalam portal DCIM**, mencakup:

1. **Jenis tiket yang dikelola:**
    - Incident Ticket (Tiket Insiden)
    - Service Request Ticket (Tiket Permintaan Layanan)
    - Change Request Ticket (Tiket Permintaan Perubahan Layanan)
    - Maintenance/Activity Ticket (Tiket Permintaan Pemeliharaan)
    - Problem Ticket (Tiket Masalah)
2. **Kanal resmi:** Portal Pusat Layanan APJII
3. **Pihak yang terlibat:**
    - Tim Teknis/NOC Data Center APJII
    - Vendor eksternal/kontraktor terkait
    - Anggota/Tenant (member APJII)
4. **Sistem yang digunakan:**

    Sistem Ticketing berbasis aplikasi di Portal Pusat Layanan APJII.

5. **Proses yang tercakup:**
    - Pembuatan dan klasifikasi tiket
    - Penugasan dan eskalasi
    - Pemantauan progres dan komunikasi
    - Verifikasi penyelesaian
    - Penutupan tiket
    - Analisis pasca-penutupan (Post Ticket Review)

6. Tanggung Jawab dan Kewenangan

Pihak/Tim	Tanggung Jawab Utama
Helpdesk	- Berfungsi sebagai Single Point of Contact (SPOC). - Menerima laporan awal mengenai insiden, permasalahan, permintaan & perubahan. - Mendistribusikan laporan tersebut atau melakukan eskalasi ke pihak terkait. - Melakukan pembuatan/update status: opened ticket & closed ticket.

Pihak/Tim	Tanggung Jawab Utama
Tim Teknis/ NOC (Network Operation Center)	- Menerima laporan dari Helpdesk atau laporan yang telah dibuat oleh Anggota/Tenant melalui portal DCIM. - Melakukan verifikasi awal terkait infrastruktur (listrik, pendingin, fire system, PAC, UPS, Sistem Monitoring), jaringan, server, storage, keamanan sistem, dan aplikasi, keamanan fisik, akses masuk, dan pelanggaran kebijakan keamanan. - Mengklasifikasikan kategori tiket (incident, request, change, problem). - Melakukan proses penanganan tiket dan update progres ke dalam sistem. - Memberikan laporan penyelesaian teknis dan evidence. - Melakukan analisis akar penyebab untuk insiden yang berulang.
PIC/Penanggung Jawab Operasional DC APJII	- Melakukan review dan approval terhadap tiket yang telah diselesaikan. - Melakukan validasi SLA dan eskalasi bila diperlukan. - Menyusun laporan mingguan dan bulanan terkait performa tiket.

7. Prosedur Pelaksanaan (Flow Proses Ticket Management)

7.1 Alur Umum Penanganan Tiket

1. **Pembuatan Tiket (Ticket Logging)**
    - Tiket dapat dibuat oleh:
        - Helpdesk.
        - Anggota/Tenant (melalui portal DCIM/email)
        - Tim Teknis (hasil inspeksi rutin)
    - Informasi wajib: Nomor tiket, tanggal/waktu, pelapor, kategori, deskripsi masalah, & lokasi.
2. **Klasifikasi dan Prioritas (Classification & Prioritization)**
    - Tim Teknis/NOC akan mengklasifikasikan kategori tiket.
    - Tiket dikategorikan berdasarkan jenis dan dampak terhadap layanan:
        - **Critical** (menyebabkan downtime service)
        - **High** (menyebabkan degradasi kinerja)
        - **Medium** (berpengaruh minor)
        - **Low** (informasi atau permintaan minor).

3. **Penugasan (Assignment)**
    - Laporan tiket akan ditugaskan ke tim teknis yang relevan oleh Tim Teknis/NOC APJII.
    - Waktu penugasan maksimum: **5 menit** setelah tiket dibuat (untuk critical ticket).
4. **Penanganan (Investigation & Resolution)**
    - Tim Teknis/NOC melakukan investigasi awal.
    - Melakukan tindakan perbaikan sementara (workaround) bila perlu.
    - Update status tiket menjadi *In Progress*.
5. **Eskalasi (Escalation Management)**
    - **Hierarkis:** apabila melewati batas waktu SLA penanganan tiket.
    - Semua eskalasi harus tercatat di sistem tiket.
6. **Verifikasi dan Validasi (Resolution Verification)**
    - Setelah tindakan dilakukan dan masalah telah diselesaikan, tim teknis menandai tiket menjadi *Resolved*.
    - Tim Teknis/NOC melakukan validasi hasil pekerjaan dan memastikan layanan telah normal.
7. **Penutupan Tiket (Closure)**
    - Tiket dinyatakan *Closed* jika:
        - Layanan telah kembali Normal.
        - Pelapor/Anggota/Tenant memberikan konfirmasi, jika pelapor/anggota/tenant tidak memberikan konfirmasi, maka ticket akan ditutup secara otomatis.
        - PIC/Penanggung Jawab Operasional DC APJII menyetujui penutupan.
    - Semua data evidence (foto, log, laporan pekerjaan) harus dilampirkan.
8. **Analisis Pasca-Insiden (Post Ticket Review)**
    - Dilakukan untuk tiket **major incident** atau **repeated issue**.
    - Bertujuan mencari akar penyebab dan menyusun tindakan pencegahan (Preventive Action).

8. Standar Waktu Layanan (SLA Ticket Management)

Kategori Tiket	Prioritas	Waktu Respon Maksimal	Waktu Penyelesaian Maksimal
Incident – Critical	P1	≤ 5 menit	≤ 2 jam
Incident – High	P2	≤ 15 menit	≤ 4 jam
Incident – Medium	P3	≤ 30 menit	≤ 8 jam
Incident – Low	P4	≤ 1 jam	≤ 24 jam
Service Request	Normal	≤ 1 jam	≤ 1 hari kerja
Change Request	Planned	Berdasarkan jadwal CRB	Berdasarkan window maintenance

Kategori Tiket	Prioritas	Waktu Respon Maksimal	Waktu Penyelesaian Maksimal
Problem Ticket	Analytical	≤ 4 jam	Berdasarkan RCA Completion (≤ 3 hari kerja)

9. Dokumentasi dan Pelaporan

1. **Dokumentasi Setiap Tiket Harus Memuat:**
   - Nomor tiket dan tanggal waktu.
   - Identitas pelapor dan penanggung jawab.
   - Kategori dan prioritas tiket.
   - Deskripsi permasalahan dan tindakan yang dilakukan.
   - Hasil penyelesaian dan bukti (foto, log, laporan teknis).
   - Waktu penyelesaian dan SLA compliance.
2. **Pelaporan Harian oleh NOC:**
   - Daftar tiket terbuka (opened).
   - Daftar tiket kritikal aktif.
   - Tiket yang melewati SLA.
   - Tiket yang telah diselesaikan.
3. **Pelaporan Mingguan/Bulanan oleh PIC/Penanggung Jawab Operasional DC APJII:**
   - Total tiket per kategori.
   - SLA achievement rate.
   - Repeated issue summary.
   - Analisis tren gangguan dan rekomendasi perbaikan.

10. Evaluasi dan Tindakan Perbaikan

1. **Evaluasi Kinerja Tiket** dilakukan minimal setiap bulan melalui:
   - Review SLA achievement.
   - Analisis tren tiket yang berulang.
   - Kepuasan Kinerja Tim Teknis/NOC/Helpdesk (*Customer Feedback*).
   - Audit internal terhadap kepatuhan prosedur.
2. **Tindakan Perbaikan (Corrective Action):**
   - Dilakukan bila ditemukan deviasi dari prosedur atau pelanggaran SLA.
   - Dicatat dalam *Corrective Action Log* dan dipantau hingga penyelesaian.
3. **Tindakan Pencegahan (Preventive Action):**
   - Dilakukan berdasarkan analisis RCA untuk insiden yang berulang.
   - Melibatkan update SOP, peningkatan pelatihan teknisi, atau penambahan alat monitoring.

11. Pengendalian Dokumen dan Rekaman

1. Semua tiket yang dibuat, diubah, atau ditutup disimpan dalam sistem ticketing minimal selama **3 tahun** sebagai arsip audit.
2. Laporan bulanan dikompilasi dan disimpan dalam folder resmi Tim Teknis/NOC.
3. Setiap revisi terhadap SOP ini harus disetujui oleh PIC/Penanggung Jawab Operasional DC APJII dan dicatat dalam **Daftar Revisi Dokumen**.

12. Lampiran

12.1 Contoh Struktur Nomor Tiket

[Tahun][Bulan][Kategori][Nomor Urut]
Contoh: 2025-10-INC-00125 → Incident bulan Oktober 2025.

12.2 Contoh Formulir Penutupan Tiket

Field	Keterangan
Nomor Tiket	2025-10-INC-00125
Pelapor	Member APJII / NOC
Deskripsi Masalah	Alarm suhu tinggi di Rack A7
Tindakan	Pembersihan filter PAC & reset sensor
Waktu Respon	3 menit
Waktu Penyelesaian	1 jam 15 menit
Status	Closed
Evidence	Foto sensor & log BMS
Disetujui oleh	Supervisor DC Facility

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XXXIX
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP DESAIN DAN TATA RUANG DATA CENTER APJII

1. Pendahuluan

Data Center APJII merupakan infrastruktur kritikal yang mendukung layanan interkoneksi anggota. Untuk menjaga keamanan, ketersediaan, dan efisiensi operasional, diperlukan prosedur baku dalam desain dan tata ruang Data Center yang mencakup aspek kelistrikan, pendinginan, tata letak rak, hingga sistem keamanan fisik. Prosedur ini disusun untuk memastikan konsistensi standar desain, tata kelola ruang, serta mendukung sertifikasi TIA-942 dan ISO 27001.

2. Tujuan

- Menetapkan standar desain tata ruang Data Center APJII yang aman, efisien, dan sesuai best practice.
- Memberikan panduan teknis dalam perencanaan, pembangunan, serta pengelolaan tata ruang Data Center.
- Memastikan operasional Data Center tetap handal dengan pengaturan optimal pada kelistrikan, pendinginan, dan tata letak perangkat.

3. Dasar & Referensi Standar

- **TIA-942-C**: Telecommunications Infrastructure Standard for Data Centers.
- **ISO/IEC 27001 & ISO/IEC 27002**: Information Security Management System.
- **ASHRAE TC 9.9**: Thermal Guidelines for Data Processing Environments.
- **SNI terkait bangunan & kelistrikan** (PUIL 2011).

4. Definisi Istilah

- **Rack**: Lemari perangkat ICT untuk server, storage, dan perangkat jaringan.
- **Cold Aisle**: Jalur udara dingin yang dihasilkan PAC, diarahkan ke intake perangkat.
- **Hot Aisle**: Jalur udara panas yang keluar dari exhaust perangkat.
- **PAC (Precision Air Conditioning)**: Sistem pendingin presisi untuk data center.
- **Raised Floor**: Lantai tambahan untuk distribusi udara dingin, kabel, dan jalur kelistrikan.

5. Ruang Lingkup

SOP ini mencakup desain dan tata ruang Data Center APJII, termasuk:

- Tata letak rak & perangkat.
- Sistem pendinginan dan pengaturan suhu.
- Desain jalur Cold-Aisle & Hot-Aisle.
- Desain kelistrikan, backup power, dan grounding.
- Standarisasi ukuran, kapasitas, dan beban.
- Prosedur pemeliharaan terkait fasilitas fisik.

6. Prosedur Desain dan Tata Ruang

6.1 Pemetaan Posisi Rack

- Rak disusun dalam konfigurasi **Hot-Aisle / Cold-Aisle**.
- Cold aisle selalu berhadapan satu sama lain, hot aisle saling membelakangi.
- Jarak minimal antar rak depan-belakang: **120 cm** untuk akses perawatan.
- Jarak sisi samping rak minimal **80 cm**.
- Akses evakuasi harus tersedia sesuai standar **NFPA & K3**.

6.2 Standarisasi Ukuran

- **Ukuran Rack**: 42U–48U (600mm x 1000mm) atau sesuai standar TIA-942.
- **Cable Tray**: minimal lebar **300 mm** untuk backbone, **100–200 mm** untuk distribusi.
- **Ducting kabel power & data harus dipisah** (minimum clearance 30 cm).
- **Raised Floor**: tinggi minimum **60 cm** untuk sirkulasi udara dingin.

6.3 Maksimal Beban Rack & Perangkat

- Beban maksimum per rack: **1.000–1.200 kg** (tergantung spesifikasi lantai).
- Beban listrik maksimum per rack: **2.2 kW** (sesuai perhitungan kapasitas Data Center APJII).
- Jumlah perangkat per rack disesuaikan dengan **perhitungan cooling load & kapasitas listrik**.

6.4 Suhu & Sirkulasi

- **Suhu ruangan ideal**: 22°C ± 2°C.
- **Suhu udara dingin (supply PAC)**: 18–20°C.
- **Suhu udara panas (return PAC)**: 28–32°C.
- **Kelembaban relatif (RH)**: 45–55%.
- Evaluasi cooling load dilakukan minimal **setiap 6 bulan**.
- **Perawatan PAC**: harian (cek alarm & filter), bulanan (cek refrigerant, sensor, kapasitor), tahunan (overhaul unit) yang dilakukan oleh vendor/pihak ketiga.

6.5 Jalur Hot-Aisle & Cold-Aisle

- **Cold aisle containment** digunakan untuk efisiensi pendinginan.
- Pintu masuk Cold Aisle dilengkapi **magnetic door** untuk menjaga tekanan udara.
- Hot aisle dialirkan langsung ke return PAC melalui ceiling plenum atau ducting.

6.6 Desain & Topologi Kelistrikan

1. **Pemetaan Jalur Kelistrikan**
    - Dual power path (**2N/N+1 system**) untuk Rack MMR.
    - Distribusi listrik via **PDUs (Power Distribution Unit)** di setiap rak Anggota/Tenant menggunakan UPS stand-by alone di masing-masing Rack Anggota/Tenant .
2. **Sistem Backup Kelistrikan**
    - UPS dengan minimum runtime **15 menit** sebelum genset aktif.
3. **Sistem Grounding**
    - Semua rack, PAC, dan panel listrik wajib terhubung ke grounding busbar.
    - Nilai resistansi grounding **<= 1 ohm** (mengacu PUIL 2011 & TIA-942).
4. **Pembagian Beban Kelistrikan**
    - Setiap rack diberi kapasitas listrik sesuai kontrak Anggota/Tenant sebesar **2.2 kW**.
    - Overload protection menggunakan **circuit breaker per rack**.
    - Monitoring beban listrik real-time menggunakan **iPDU (intelligent PDU) khusus di Rack MMR**.

7. Catatan & Dokumentasi

- Semua desain tata ruang, layout rack, kapasitas listrik, dan pendinginan harus terdokumentasi dalam **As-Built Drawing** dan portal **DCIM (Data Center Infrastructure Management System)**.
- **As-Built Drawing** yang direvisi wajib mendapatkan persetujuan dari manajemen APJII.
- Evaluasi desain dilakukan minimal **1 kali setahun** atau saat ada perubahan yang signifikan.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XL
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP INFRASTRUKTUR JARINGAN DATA CENTER APJII

1. Pendahuluan

SOP Infrastruktur Jaringan ini disusun untuk memastikan seluruh kegiatan perencanaan, pemasangan, pengelolaan, pemeliharaan, dan pembongkaran (dismantle) infrastruktur jaringan di Data Center APJII berjalan secara aman, terstandarisasi, serta sesuai dengan praktik terbaik industri. Infrastruktur jaringan merupakan komponen kritikal dalam menjaga kontinuitas layanan interkoneksi, IIX, peering, dan layanan kolokasi.

SOP ini berlaku bagi seluruh Tim Teknis/NOC, Anggota/Tenant, Kontraktor, maupun pihak ketiga yang melakukan pekerjaan terkait instalasi dan penanganan kabel jaringan, baik fiber optic maupun UTP, di area Data Center APJII.

2. Tujuan

SOP ini disusun untuk mencapai tujuan-tujuan berikut:

1. Menjamin standar penataan kabel yang rapi, aman, dan sesuai best practice data center.
2. Mengatur proses desain, instalasi, pengetesan, labeling, dokumentasi, dan pemeliharaan kabel.
3. Mencegah gangguan layanan akibat salah pemasangan, kabel rusak, atau interferensi fisik.
4. Menetapkan batasan serta prosedur penanganan kabel dari luar (incoming cable) dan internal.
5. Memastikan seluruh pekerjaan mengikuti prosedur izin kerja (Work Permit) dan keamanan APJII.
6. Menyediakan acuan bagi audit internal dan eksternal untuk memastikan kepatuhan standar.

3. Dasar dan Referensi Standar

SOP Infrastruktur Jaringan mengacu pada standar dan pedoman berikut:

3.1 Standar Internasional

- **TIA-942-C**: Telecommunications Infrastructure Standard for Data Centers
- **TIA/EIA-568**: Structured Cabling Standard
- **ISO/IEC 11801**: Generic Cabling for Customer Premises
- **ISO/IEC 14763-2**: Testing & Operation of Cabling
- **ANSI/TIA-606-B**: Cable Labeling & Administration
- **IEC 60364**: Electrical Installation & Safety

3.2 Regulasi APJII

- SOP Akses Masuk dan Keluar Data Center APJII
- SOP Interkoneksi

4. Definisi Istilah

4.1 Infrastruktur Jaringan

Seluruh elemen fisik dan nonfisik yang digunakan untuk membangun konektivitas jaringan antar perangkat tenant, IIX, backbone operator, dan perangkat internal APJII.

4.2 Cable Tray

Media jalur kabel berbahan metal yang ditempatkan di atas, pada ceiling, atau di bawah raised floor untuk mengatur routing kabel.

4.3 Shaft Cable

Ruang vertikal (ducting) untuk jalur kabel dari lantai ke lantai.

4.4 Raised-Floor Cable Path

Jalur kabel yang diletakkan pada ruang kosong di bawah raised floor khusus untuk kabel data atau power (dengan segregasi).

4.5 Backbone Cable

Link kabel utama penghubung antara MMR, OTB, Core Network, dan Data Hall.

4.6 Cross-Connect Cable

Kabel penghubung antara rak tenant ke panel IIX/APJII atau antar tenant.

4.7 OTB (Optical Termination Box)

Kotak terminasi serat optik untuk sambungan backbone dan distribusi.

4.8 Fibre Patch Panel

Panel terminasi fiber untuk patching antar perangkat.

4.9 Cable Management

Aksesori perapihan kabel seperti horizontal/vertical organizer, velcro, ladder tray, dll.

4.10 Work Permit

Izin kerja resmi untuk melakukan aktivitas instalasi, pemeliharaan, atau dismantle.

5. Ruang Lingkup

Ruang lingkup SOP ini mencakup seluruh aktivitas berikut:

5.1 Struktur Kabel & Aksesoris Penunjang

5.1.1 Jalur Cable Tray

- Semua kabel horizontal dan backbone wajib melalui tray yang telah ditentukan.
- Pemisahan jalur tray untuk jalur **kabel data** dan jalur **kabel listrik** adalah wajib (minimum 60 cm).
- Dilarang menggunakan tray tanpa label atau jalur melewati area yang tidak diperbolehkan.

5.1.2 Jalur Shaft

- Kabel backbone dari operator wajib masuk melalui shaft khusus backbone.
- Setiap operator harus menggunakan ruang shaft yang telah diberikan secara tertib dan sesuai layout.

5.1.3 Raised Floor

- Digunakan untuk jalur kabel fibre/UTP dari rack ke rack.
- Harus mengikuti tray yang telah dipasang di bawah raised floor.
- Dilarang meletakkan kabel langsung ke lantai tanpa tray.

5.2 Desain & Layout Jaringan

Poin yang wajib ditetapkan sebelum instalasi:

- **Topologi jaringan tenant**: star, mesh, atau ring.
- **Penempatan OTB & patch panel** di MMR.
- **Penomoran tray** dan **zona pendistribusian kabel**.
- **Rencana kapasitas** dalam 1 tray (fill ratio maksimal 80%).
- **Labeling path** dari titik awal ke titik akhir.
- **Routing diagram** yang wajib disetujui NOC APJII sebelum penarikan kabel.

5.3 Jenis Kabel dan Standarisasi

5.3.1 Backbone Cable

- Fibre SM 12 core, 24 core, 48 core, atau sesuai kebutuhan operator.
- Mengikuti standar G.652D / G.657A2.

5.3.2 Cross-Connect Cable

- Fibre patch cord: LC-LC, SC-LC, atau sesuai port standar APJII.
- Copper: UTP/STP Cat6A.

5.3.3 Topologi Kabel

- MMR → OTB → Rack Tenant → Equipment
- Routing wajib mengikuti jalur terpendek namun tetap menjaga radius bending.

5.3.4 Cable Management

- **Horizontal Cable Manager** wajib digunakan tiap 1U/2U pada patch panel.
- **Vertical Cable Manager** digunakan di sisi kiri-kanan rack.
- Pengikat kabel wajib menggunakan **velcro**, bukan cable tie plastik.

5.4 Prosedur Kabel Masuk dari Luar Data Center (Incoming Cable)

1. Setiap operator wajib memberitahu APJII minimal **3 hari sebelumnya**.
2. Kabel masuk hanya melalui **MMR** dan **shaft yang ditentukan**.
3. Pemeriksaan dilakukan oleh NOC:
    - Jenis kabel
    - Panjang kabel
    - Penempatan OTB
    - Routing di area Data Center
4. Tidak diperbolehkan membawa masuk **kemasan**, **karton**, **bubble wrap**, atau material packaging lainnya (zero packaging policy).
5. Instalasi dilakukan oleh engineer operator dengan supervisi Tim Teknis/NOC APJII.
6. Semua terminasi wajib dilakukan pada OTB/patch panel yang telah disediakan.
7. Tes OTDR wajib dilakukan untuk backbone.
8. Hasil tes diserahkan ke APJII sebagai dokumen serah terima.

5.5 Testing & Maintenance

5.5.1 Pengujian Kabel

- **Fiber**: OTDR + Power Meter Test
- **Copper**: Fluke DSX Certification (Cat6A/7 Standard)
- Semua hasil test disimpan sebagai arsip APJII.

5.5.2 Pemeliharaan Berkala

- Inspeksi tray setiap 3 bulan.
- Audit patch panel: patching yang berantakan wajib diperbaiki.
- Audit labeling minimal 6 bulan sekali.
- Pembersihan MMR & OTB area dilakukan sesuai SOP kebersihan DC.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XLI
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

PERSYARATAN BAGI ANGGOTA/TENANT DALAM MENEMPATKAN STANDALONE UPS DI BAWAH RACK DATA CENTER APJII

1. Pendahuluan

UPS (Uninterruptible Power Supply) Standalone yang ditempatkan di bawah rack tenant berfungsi sebagai lapisan proteksi tambahan untuk peralatan IT (server, switch, router, storage) terhadap gangguan daya sesaat, *voltage drop*, *spike*, atau *brownout*.

Dalam konteks **Data Center APJII**, penempatan UPS di bawah rack tenant **harus memenuhi persyaratan keselamatan, efisiensi daya, dan integrasi infrastruktur listrik data center** agar tidak mengganggu sistem distribusi utama (power path A/B) dan tidak menimbulkan risiko terhadap lingkungan bersama (shared data hall).

2. Persyaratan Umum UPS Standalone di Bawah Rack Tenant

2.1. Spesifikasi Teknis Minimum

Parameter	Persyaratan Teknis
Kapasitas Daya	2.2 kW – 7 kW (single phase 230 V atau 208 V)
Topologi UPS	Online Double Conversion (VFI-SS-111) sesuai IEC 62040-3
Efisiensi	≥ 93% pada mode online; ≥ 97% pada ECO mode
Faktor Daya Output (PF)	≥ 0.9 lagging; disarankan unity (1.0)
Input Power Factor	≥ 0.99 dengan THDi ≤ 5%
Battery Type	Lithium-Ion (disarankan) atau VRLA (AGM) dengan flame-retardant casing UL94-V0
Communication Interface	SNMP, Modbus TCP, USB, dry contact

Parameter	Persyaratan Teknis
Bypass	Automatic & manual maintenance bypass (bypass internal atau eksternal optional)
Cooling	Forced air cooling, ventilasi bawah-rack minimal 50 cm dari obstruction
IP Rating	Minimal IP20 (indoor rack space)
Certifications	CE, UL, IEC 62040-1/2, RoHS, dan memenuhi TIA-942 Safety Guideline
Noise Level	≤ 55 dB(A) pada 1 meter
Form Factor	Tower atau rackmount (2U–6U) dengan clearance udara memadai
Monitoring	Real-time status, temperature, battery health via DCIM/BMS integration

3. Persyaratan Penempatan dan Instalasi di Data Center APJII

3.1. Lokasi & Tata Letak

- UPS hanya boleh ditempatkan di bawah rack tenant (bukan di koridor hot aisle/cold aisle).
- Tidak boleh menghalangi aliran udara pendingin (cold air intake).
- Harus ada **clearance minimum 10 cm di setiap sisi** dan 30 cm di belakang untuk ventilasi udara.
- Rak tenant wajib dilengkapi **perangkat deteksi panas lokal (termal sensor)** yang terintegrasi ke BMS.

3.2. Koneksi Daya

- UPS **tidak boleh langsung dihubungkan ke panel utama data hall**, melainkan melalui **PDU tenant yang sudah disediakan** (PDU/Circuit Breaker yang terproteksi).
- Kabel power UPS harus menggunakan **kabel standar IEC 60320 atau IEC 60309**, sesuai kapasitas arusnya.
- Sistem Grounding wajib terhubung ke **common grounding bar (CGB)** di bawah raised floor atau tray grounding rack.

3.3. Proteksi & Keamanan

- UPS wajib memiliki:
  - **Circuit breaker internal dan fuse proteksi.**
  - **Thermal sensor** untuk memutus arus saat overheating.
  - **Overload dan short circuit protection.**
- **Tidak diperkenankan** menggunakan UPS yang casing-nya berlubang, rusak, atau memiliki kebocoran baterai.

- **Tidak diperkenankan** menggunakan UPS Rakitan.
- **Label identifikasi tenant** dan **kapasitas daya maksimum** harus ditempel jelas di unit UPS.

4. Preventive Maintenance (PM) – Metode dan Frekuensi

4.1. Jadwal Preventive Maintenance Yang Dilakukan oleh Anggota/Tenant

Frekuensi	Kegiatan Utama
Harian	- Periksa indikator LED/alarm pada UPS. - Pastikan suhu sekitar < 30 °C.
Mingguan	- Cek ventilasi udara dan kebersihan area bawah rack. - Pastikan komunikasi SNMP ke monitoring aktif.
Bulanan	- Lakukan simulasi uji transfer beban (*load transfer test*). - Catat log runtime dan kapasitas baterai.
Triwulanan (3 Bulan)	- Bersihkan kipas dan grill ventilasi. - Periksa tegangan baterai per sel. - Tes fungsi auto-bypass dan auto-recovery.
Tahunan	- Kalibrasi sensor suhu & tegangan. - Uji beban penuh (load bank test 100%). - Ganti filter udara jika ada. - Uji proteksi overload/short circuit.

5. Penggantian Komponen dan Umur Pakai oleh Anggota/Tenant

Komponen	Umur Teknis	Tindakan Penggantian
Baterai VRLA	3–5 tahun	Ganti saat kapasitas < 80% dari nominal
Baterai Lithium-Ion	8–10 tahun	Ganti saat cycle count tercapai atau degradasi > 15%
Kipas pendingin	3–4 tahun	Ganti preventif untuk hindari overheating
Kapasitor DC/AC	5–7 tahun	Ganti bila terjadi swelling atau drop tegangan signifikan
Kontaktor/Relay	5 tahun	Periksa fungsi mekanis & ganti bila ada keausan
Firmware UPS	Setiap update vendor	Lakukan pembaruan dengan teknisi bersertifikat

6. Prosedur Penanganan UPS Jika Terbakar / Overheating

6.1. Tanda Awal

- Bau gosong dari bawah rack.
- Suhu UPS > 60 °C.
- Alarm “Over Temperature” atau “Battery Fault”.
- Asap tipis di area bawah rack.

6.2. Tindakan Darurat

1. **Segera tekan tombol EPO (Emergency Power Off)** pada rack atau zona terkait.
2. **Putuskan sumber daya (input breaker)** UPS secara manual.
3. **Jangan gunakan air!** Gunakan **APAR jenis CO_2 atau clean agent**.
4. Laporkan ke **Tim NOC/Teknis APJII dan ICO (Incident Commanding Officer)**.
5. Dokumentasikan insiden, ambil foto, dan isolasi area UPS selama minimal 1 jam untuk pendinginan.
6. Lakukan **analisa akar penyebab (Root Cause Analysis)** sebelum unit diganti atau dipasang kembali.

7. Mitigasi Risiko

Risiko	Dampak	Mitigasi
Overheating / kebakaran baterai	Kerusakan aset dan potensi kebakaran	- Gunakan baterai bersertifikasi UL94-V0 - Tambah sensor suhu bawah rack - Lakukan PM rutin
Korsleting internal UPS	Trip pada PDU / breaker tenant	- Gunakan internal fuse proteksi - Periksa kabel & konektor
Battery leakage (VRLA)	Korosi & kontaminasi udara	- Gunakan tray pelindung dan bahan tahan asam - Bersihkan area setiap bulan
Ketidakseimbangan beban antar fasa	Overload salah satu jalur distribusi	- Pantau load per phase melalui DCIM - Distribusi daya seimbang
Kegagalan transfer beban	Downtime server tenant	- Tes simulasi transfer load setiap 3 bulan - Gunakan UPS dengan double conversion
Interferensi elektromagnetik (EMI)	Gangguan perangkat IT	- Gunakan UPS dengan EMI filter internal - Pisahkan kabel power dan data

8. Dokumentasi dan Pelaporan

- Setiap UPS tenant wajib terdaftar di **Asset Management DC APJII** dengan:
  - Nomor seri, kapasitas, tenant, dan lokasi rack.
  - Log preventive maintenance dan penggantian baterai.
  - Catatan hasil uji tahunan (*load test report*).
- Semua kegiatan PM dan insiden harus dilaporkan ke **PIC/Penanggung Jawab Operasional DC APJII/ICO** dalam format *Preventive Maintenance Report* dan *Incident Report*.

10. Kesimpulan

UPS standalone tenant di bawah rack **harus memenuhi standar keselamatan (IEC 62040 & TIA-942)**, menggunakan **topologi online double conversion**, **baterai bersertifikasi flame-retardant**, dan **terhubung ke sistem monitoring APJII**.

Preventive maintenance yang disiplin dan wajib dilakukan oleh Anggota/Tenant serta prosedur tanggap darurat yang jelas di DC APJII menjadi sangat penting untuk mencegah **overheating, kebakaran, dan gangguan layanan**.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XLII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENGELOLAAN EKSTERNAL VENDOR DATA CENTER APJII

1. PENDAHULUAN

Dalam operasional Data Center APJII yang berlokasi di Gedung Cyber-1, berbagai kegiatan pemeliharaan, instalasi, dan dukungan teknis melibatkan pihak ketiga (vendor eksternal), seperti kontraktor PAC/CRAC/CRAH, UPS, Baterai, keamanan fisik, kebersihan, dan sistem jaringan. Untuk menjamin keamanan, keselamatan, dan keberlangsungan layanan Data Center, diperlukan pengelolaan yang ketat terhadap seluruh aktivitas vendor eksternal yang masuk, bekerja, dan keluar dari area Data Center.

SOP ini mengatur proses administratif, teknis, dan keamanan terkait pengelolaan eksternal vendor agar setiap aktivitas yang dilakukan oleh pihak luar berjalan sesuai standar operasional, tidak menimbulkan risiko terhadap infrastruktur, data, maupun personel di lingkungan Data Center APJII.

2. TUJUAN

Tujuan dari SOP Pengelolaan Eksternal Vendor ini adalah untuk:

1. Menjamin seluruh kegiatan vendor eksternal dilakukan sesuai kebijakan keamanan dan keselamatan kerja Data Center APJII.
2. Menetapkan prosedur izin masuk, pengawasan, dan evaluasi vendor.
3. Mengendalikan akses fisik vendor ke area terbatas Data Center (white area, grey area, utility area).
4. Menjamin kegiatan vendor tidak menimbulkan gangguan terhadap operasional sistem kritikal Data Center.
5. Menegakkan akuntabilitas dan dokumentasi atas seluruh aktivitas pihak eksternal.
6. Memastikan vendor memahami dan mematuhi ketentuan keamanan fisik, lingkungan, serta standar HSE (Health, Safety, and Environment) / K3 Umum yang berlaku di Gedung Cyber-1 dan APJII.

3. DASAR DAN REFERENSI STANDAR

SOP ini disusun berdasarkan pedoman dan standar berikut:

1. **ISO/IEC 27001:2022** – Information Security Management System (ISMS)

- Klausul 7.4, 8.1, 8.2, dan Annex A.5.19 – *Supplier Relationships & Access Control*

2. **ISO 22301:2019** – Business Continuity Management Systems (BCMS)
   - Klausul 8.4 – *Continuity of Supply Chain*
3. **TIA-942-C:2023** – Telecommunications Infrastructure Standard for Data Centers
4. **SOP Keamanan Fisik DC APJII & SOP Akses Masuk/Keluar DC APJII**.
5. **Peraturan Gedung Cyber-1 Management** – tentang akses, keselamatan, dan penggunaan fasilitas bersama.
6. **Peraturan Ketenagakerjaan dan K3 (Kesehatan & Keselamatan Kerja)** – Permenaker No. PER.05/MEN/1996 dan KEP.463/MEN/1993.
7. **Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)** – aspek keamanan informasi.

4. DEFINISI ISTILAH

Istilah	Definisi
Vendor Eksternal	Pihak ketiga yang dipekerjakan untuk memberikan layanan teknis, pemeliharaan, atau dukungan kepada fasilitas Data Center APJII.
Tim Teknis/NOC/Security	Tim internal APJII yang bertanggung jawab atas operasional, keamanan fisik, dan pemeliharaan Data Center.
Permit to Work (PTW)	Dokumen izin kerja resmi yang diberikan kepada vendor eksternal untuk melaksanakan pekerjaan di area tertentu dalam jangka waktu tertentu.
Work Permit Officer (WPO)	PIC/Penanggung Jawab Operasional DC APJII yang berwenang mengeluarkan, memverifikasi, dan menutup PTW.
Petugas Pendamping	Petugas Pendamping dari internal APJII yang mendampingi vendor selama bekerja di area terbatas (white area).
Visitor/Vendor Access Log	Catatan elektronik atau manual yang berisi data identitas, waktu masuk/keluar, area kerja, dan keperluan kunjungan vendor.
White Area	Area Data Hall, Rack MMR (Meet Me Room) Bersama, atau ruang yang berisi peralatan IT kritikal dan memiliki pembatasan akses tinggi.
Grey Area	Area utilitas seperti ruang listrik, ruang PAC, ruang UPS, dan ruang mekanikal.
Black Area	Area umum yang tidak terbatas, seperti loading dock, lift servis, dan koridor umum yang dimiliki oleh Pengelola Gedung Cyber-1.

5. RUANG LINGKUP

SOP ini mencakup seluruh tahapan kegiatan pengelolaan vendor eksternal yang terlibat dalam aktivitas di lingkungan **Data Center APJII yang berlokasi di Gedung Cyber-1**, meliputi:

1. **Tahapan Administratif**
   - Seleksi dan registrasi vendor.
   - Verifikasi dokumen legal, sertifikasi teknis, dan asuransi kerja.
   - Penandatanganan NDA (Non-Disclosure Agreement) dan SLA kontraktual.
2. **Tahapan Operasional**
   - Pengajuan izin kerja (Work Permit/PTW) minimal 3x24 jam sebelum pelaksanaan.
   - Pemeriksaan peralatan dan material yang akan dibawa masuk.
   - Briefing prosedur K3 Umum sebelum pekerjaan dimulai.
   - Pengawalan vendor selama berada di area terbatas.
3. **Tahapan Keamanan dan Keselamatan**
   - Penerapan sistem akses kontrol (Access Control System, Visitor Card).
   - Larangan membawa kamera, flashdisk, atau perangkat perekam tanpa izin tertulis.
   - Kepatuhan terhadap protokol ESD (Electrostatic Discharge) di ruang IT.
   - Penegakan aturan K3 Umum selama pekerjaan berlangsung.
4. **Tahapan Evaluasi dan Dokumentasi**
   - Pemeriksaan hasil pekerjaan.
   - Penutupan izin kerja (PTW Closure).
   - Evaluasi vendor (Vendor Performance Evaluation).
   - Dokumentasi dan pelaporan ke Manajer Data Center.
5. **Tahapan Khusus (Force Majeure atau Emergency Work)**
   - Mekanisme izin darurat dengan notifikasi kepada PIC/Penanggung Jawab Operasional DC APJII.
   - Pengawalan ketat selama tindakan pemulihan dilakukan.
   - Pencatatan lengkap dalam *Emergency Work Logbook*.

6. TANGGUNG JAWAB DAN KEWENANGAN

Jabatan / Pihak	Tanggung Jawab dan Kewenangan
PIC/Penanggung Jawab Operasional DC APJII	- Menyetujui vendor yang akan melakukan pekerjaan di area Data Center. - Menyetujui dokumen Permit to Work (PTW) untuk pekerjaan berisiko tinggi. - Mengawasi kepatuhan vendor terhadap kebijakan keamanan dan keselamatan. - Menyusun evaluasi tahunan performa vendor. - Mengambil tindakan korektif jika vendor melanggar ketentuan.
Work Permit Officer (WPO) / Penanggung Jawab Operasional DC APJII	- Memproses pengajuan izin kerja vendor. -Memastikan seluruh dokumen vendor lengkap dan valid. -Melakukan safety briefing dan penjelasan area kerja.

Jabatan / Pihak	Tanggung Jawab dan Kewenangan
	-Menerbitkan, menandatangani, dan menutup PTW.
Petugas Security (Cyber-1 dan APJII)	- Melakukan verifikasi identitas vendor di pos keamanan. - Memeriksa barang dan peralatan yang dibawa masuk dan keluar. - Mengawal vendor hingga bertemu dengan petugas pengawas. - Menolak vendor tanpa izin kerja resmi atau tanpa pendamping APJII. - Mengisi dan menjaga log akses vendor.
Escort Officer / Petugas Pendamping APJII	- Mendampingi vendor selama berada di area terbatas (white/grey area). - Memastikan vendor bekerja sesuai prosedur dan tidak mengganggu sistem kritikal. - Menegur langsung jika ditemukan pelanggaran. - Melaporkan hasil pendampingan kepada WPO.
Vendor Eksternal / Kontraktor	- Mematuhi seluruh kebijakan keamanan dan K3 APJII. - Mengajukan izin kerja sesuai jadwal yang ditentukan. - Menghadiri safety briefing sebelum bekerja. - Melakukan pekerjaan sesuai PTW dan tidak melebihi area yang diizinkan. - Membersihkan area kerja setelah selesai.

7. PROSEDUR PELAKSANAAN

7.1. Pra-Kegiatan

1. Vendor mengajukan permohonan izin kerja (PTW) minimal **3x24 jam** sebelum pelaksanaan melalui email resmi dan/atau portal DCIM.
2. Lampirkan dokumen berikut:
    - Surat Tugas resmi dari perusahaan vendor.
    - Daftar nama personel dan nomor identitas (KTP/SIM).
    - Sertifikat kompetensi teknis (jika relevan).
    - Asuransi tenaga kerja (BPJS Ketenagakerjaan/Asuransi proyek).
    - Deskripsi pekerjaan dan risiko kegiatan.
    - Daftar alat dan material yang akan dibawa masuk.
3. WPO melakukan pemeriksaan kelengkapan dokumen dan memberikan **pre-approval**.
4. Jika pekerjaan melibatkan sistem kritikal (listrik, PAC, UPS, fire system), maka wajib dilakukan **review teknis dan risk assessment** terlebih dahulu.

5. Vendor wajib mengikuti **safety briefing** dan menandatangani *Acknowledgement Form* bahwa telah memahami SOP APJII.

7.2. Saat Pekerjaan Berlangsung

1. Vendor melakukan registrasi di **meja Tim Security DC APJII** dengan menunjukkan:
    - ID resmi, surat tugas, dan salinan PTW yang disetujui.
2. Security melakukan pemeriksaan fisik terhadap peralatan dan mencatat dalam **Visitor/Vendor Logbook**.
3. Vendor diberikan **Visitor/Vendor ID Card** dan wajib dikembalikan saat keluar.
4. Vendor wajib didampingi oleh **Petugas Pendamping APJII** selama berada di area white/grey.
5. Semua kegiatan vendor harus tercatat dalam **Work Log Sheet** termasuk waktu mulai, jenis pekerjaan, dan status progres.
6. Jika vendor membutuhkan downtime atau isolasi sistem (contoh: pemadaman panel, uji UPS & baterai, bypass PAC), maka harus ada **approval tertulis** dari PIC/Penanggung Jawab Operasional DC APJII.
7. Dilarang:
    - Mengambil foto/video tanpa izin tertulis.
    - Mengakses rak pelanggan, Rack MMR bersama, atau server tanpa petugas pendamping.
    - Menggunakan Wi-Fi internal atau port jaringan APJII.
8. Vendor wajib menjaga kebersihan, tidak meninggalkan sisa material, dan membuang limbah sesuai prosedur K3.

7.3. Pasca-Pekerjaan

1. Vendor menyerahkan hasil pekerjaan kepada **WPO** untuk verifikasi.
2. Jika pekerjaan selesai sesuai rencana dan area bersih, WPO menandatangani **PTW Closure**.
3. Petugas Pendamping memastikan seluruh alat dan material vendor dibawa keluar dan diverifikasi oleh Security.
4. Semua dokumen (PTW, foto before/after, laporan teknis) disimpan dalam arsip digital **Data Center Maintenance Record**.
5. Vendor wajib menyerahkan **Laporan Pekerjaan (Work Completion Report)** dalam waktu 1x24 jam.

8. DOKUMENTASI DAN PELAPORAN

Dokumentasi wajib yang harus disimpan:

Jenis Dokumen	Keterangan	Retensi
Formulir Permit to Work (PTW)	Berisi data izin kerja, jenis kegiatan, dan waktu pelaksanaan	2 tahun
Risk Assessment / Safety Checklist	Analisis risiko pekerjaan vendor	2 tahun

Jenis Dokumen	Keterangan	Retensi
Work Log Sheet	Catatan aktivitas harian vendor	1 tahun
Vendor Evaluation Form	Evaluasi performa vendor	1 tahun
Foto Before/After Work	Bukti pelaksanaan pekerjaan	1 tahun
Emergency Work Logbook	Pekerjaan darurat vendor	2 tahun

Semua dokumen harus diunggah ke **dalam portal DCIM** dengan akses terbatas untuk tim Teknis/NOC dan PIC/Penanggung Jawab Operasional DC APJII.

9. PENGAWASAN DAN PENGENDALIAN

1. **CCTV Monitoring:** seluruh aktivitas vendor dipantau 24 jam melalui sistem CCTV dengan rekaman disimpan minimal 90 hari.
2. **Patroli Security:** dilakukan setiap 2 jam sekali selama pekerjaan berlangsung.
3. **Audit Internal:** dilakukan secara berkala oleh tim ISMS APJII untuk memastikan kepatuhan SOP.
4. **Vendor Violation Report:** dibuat jika vendor melanggar ketentuan (contoh: tidak memakai APD, akses tanpa izin, merusak peralatan).
5. **Sanksi:** pelanggaran berat dapat berakibat pada:
    - Pencabutan izin kerja.
    - Blacklist vendor selama periode tertentu.
    - Pemutusan kontrak kerja sama.

10. EVALUASI KINERJA VENDOR

Evaluasi dilakukan minimal **setiap 6 bulan** oleh PIC/Penanggung Jawab Operasional DCO APJII berdasarkan kriteria berikut:

Kriteria	Parameter Penilaian	Bobot (%)
Kepatuhan terhadap SOP	Disiplin, dokumentasi lengkap, penggunaan APD	25
Kualitas pekerjaan	Kerapihan, hasil kerja sesuai standar	25
Ketepatan waktu	Penyelesaian pekerjaan sesuai jadwal	20
Responsivitas & komunikasi	Kerjasama dan koordinasi dengan tim APJII	15
Kepatuhan terhadap HSE	Kecelakaan nol, kepatuhn K3	15

Catatan: **Bobot Nilai yang kurang dari 70% akan dikategorikan sebagai Vendor Berisiko dan dapat dievaluasi ulang atau diganti**.

11. PELATIHAN DAN SOSIALISASI

1. Semua vendor wajib mengikuti **Induksi K3 Umum Data Center APJII** sebelum melaksanakan pekerjaan pertama.
2. Pelatihan diberikan oleh tim Teknis/NOC, mencakup:
    - Pengenalan area dan level akses Data Center.
    - Aturan keamanan informasi dan kontrol fisik.
    - Prosedur K3 (alat pelindung diri, evakuasi, bahaya listrik, ESD).
    - Protokol darurat (fire alarm, power failure, lockdown).
3. APJII akan melakukan **refreshment training** setiap 12 bulan untuk seluruh vendor aktif.
4. Vendor yang tidak mengikuti pelatihan tidak diperbolehkan mengajukan izin kerja.

12. TINJAUAN DAN PEMBARUAN SOP

1. SOP ini ditinjau **setiap 12 bulan sekali** atau apabila terdapat:
    - Perubahan kebijakan manajemen APJII.
    - Pembaruan standar ISO/TIA yang relevan.
    - Perubahan aturan dari pengelola Gedung Cyber-1.
2. Revisi SOP dilakukan oleh **Tim Konsultan APJII** dan disetujui oleh **PIC/Penanggung Jawab Operasional DC APJII**.
3. Versi terbaru SOP akan didistribusikan ke seluruh staf APJII, vendor terdaftar, dan pengelola gedung.
4. Seluruh versi terdahulu disimpan dalam arsip kebijakan dengan penandaan “OBSOLETE”.

13. PENUTUP

SOP ini merupakan pedoman resmi yang wajib dipatuhi oleh seluruh pihak internal dan eksternal yang beraktivitas di area Data Center APJII Cyber-1. Pelanggaran terhadap ketentuan ini dapat berdampak pada sanksi administratif maupun terminasi kerja sama.
Dengan penerapan SOP ini, diharapkan keamanan, keselamatan, dan keberlangsungan operasional Data Center APJII dapat terjaga sesuai standar tertinggi industri.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XLIII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENYELENGGARAAN LAYANAN INTERNET EXCHANGE APJII

1. Pendahuluan

Dokumen ini menjelaskan Standar Operasional Prosedur (SOP) penyelenggaraan layanan Internet Exchange (IXP), khususnya IIX (Internet Exchange Indonesia). SOP ini berfungsi sebagai panduan resmi yang mengatur semua aspek layanan, mulai dari administrasi, operasi jaringan, penanganan insiden, hingga tata kelola (governance).

2. Tujuan

Tujuan SOP ini adalah:

2.1 Memberikan panduan yang jelas dan terstruktur terkait administrasi layanan dan operasi jaringan IIX.
2.2 Memastikan konsistensi dalam penanganan gangguan (insiden) dan respons keamanan.
2.3 Menjamin keandalan (reliability), skalabilitas (scalability), dan keamanan platform IIX.
2.4 Mendukung praktik terbaik (best practices) yang diadopsi dari IXP Internasional (AMS-IX, DE-CIX, LINX, Euro-IX, dan SGIX).

3. Definisi & Referensi Standar

Kategori	Deskripsi
IIX/IXP	Internet Exchange Point, platform yang memfasilitasi pertukaran traffic internet antar anggota (peer).
Referensi IXP	**AMS-IX, DE-CIX, LINX, Euro-IX, SGIX (Singapore Internet Exchange)**.
Standar & Protokol	BGP (Border Gateway Protocol), IRR (Internet Routing Registry), RPKI (Resource Public Key Infrastructure), L2 ACLs (Layer 2 Access Control Lists), RFC 9234 (ASPA Validation).

4. Definisi Istilah

Istilah	Definisi
Anggota/Member	Perusahaan atau entitas yang terhubung dan melakukan *peering* di IIX.
Route Server	Perangkat BGP yang memfasilitasi *multilateral peering* untuk efisiensi *peering*.
Flapping	Port jaringan yang berulang kali (lebih dari 3x dalam 5 detik) berubah status dari Up ke Down.
Prefix Leak	Kesalahan *propagasi* rute BGP di luar cakupan yang seharusnya atau yang disepakati.
Hijacking	Routing BGP secara tidak sah untuk mengalihkan *traffic*.
Spoofing	Memalsukan alamat IP sumber untuk tujuan penyerangan atau penyembunyian.
NMS	Network Management System, sistem pengendalian dan monitoring jaringan terpusat.
RCA	Root Caused Analysis, analisis penyebab utama suatu insiden.
RTBH	Remote Triggered Blackhole, teknik mitigasi DDoS menggunakan BGP *community*.
PKS	Perjanjian Kerja Sama.

5. Ruang Lingkup

SOP ini berlaku untuk semua personel dan pihak terkait yang bertanggung jawab atas penyelenggaraan, pengoperasian, pemeliharaan, dan tata kelola layanan IIX, termasuk:

1. Administrasi Layanan dan Anggota.
2. Operasi dan Monitoring Jaringan.
3. Penanganan Gangguan dan Keamanan Jaringan.
4. Manajemen Infrastruktur Fisik.

6. Prosedur Operasional Inti (Core SOP)

6.1 Administrasi Layanan

Prosedur	Detail Pelaksanaan
Permohonan, Perubahan, dan Pemutusan Layanan	Semua permintaan interkoneksi, *upgrade/downgrade* port, maupun penghentian layanan harus diajukan secara **resmi** melalui **formulir** (email/sistem online) dan disetujui Pengelola IIX.
Prosedur Isolasi/Staging Peering Baru	Anggota baru akan ditempatkan pada **jaringan isolasi** untuk **uji coba** sebelum masuk ke jaringan produksi/IXP.
Prosedur Alokasi IP IIX	Alamat IP dialokasikan berdasarkan **kebijakan *numbering plan* IXP**. Setiap anggota hanya diperbolehkan menggunakan IP yang diberikan.
Prosedur Alokasi Port IIX	Penentuan port dilakukan berdasarkan **ketersediaan kapasitas**, kebutuhan anggota, dan **perencanaan kapasitas jangka panjang**.

Prosedur Upgrade Port IIX	Port dapat di-*upgrade* dari 10G secara bertahap (2x10G, 40G/100G, Nx100G) jika utilisasi harian mencapai **70%** selama 7 hari berturut-turut.
Prosedur Penggunaan Aggregate Port	Untuk Port **10G** maksimal hanya sampai 2 x 10G. Jika lebih dari 20G, diarahkan ke 40G/100G. Port 100G tidak memiliki batasan agregasi saat ini.
Ketentuan untuk Pengguna Khusus	Pengguna dengan *outbound traffic* (kontribusi konten) dominan **1:5 (20%)** dapat terhubung ke IIX secara **gratis** (tidak dikenakan biaya *cross connect* 100G) dengan syarat ber-PKS dengan APJII.

6.2 Penanganan Gangguan

Gangguan diklasifikasikan berdasarkan *severity* (dampak) dengan tindakan dan mitigasi yang berbeda:

Severity Level	Tindakan NOC (Network Operations Center)	Jenis Gangguan	Mitigasi yang Diterapkan
Low	Diberikan **Notifikasi** hingga Anggota melakukan perbaikan.	Broadcast Flood	Sistem akan mendeteksi dan membatasi *broadcast traffic* abnormal.
		Network/Port Flapping	Port *flapping* diisolasi otomatis **minimal** 3×24 **jam**. Jika berulang, diisolasi **minimal 30 hari**.
Medium	Dilakukan **Soft Block** dan akan dibuka kembali setelah Anggota melakukan perbaikan.	Route/Prefix Leak	*Route server* melakukan **filtering IRR/RPKI** untuk mencegah *prefix leak*.
		Looping (L2/L3)	*Monitoring* akan mendeteksi anomali *looping* L2/L3.
High	Dilakukan **Shutdown Port** sampai dilakukan Rapat Klarifikasi.	Hijacking	**Validasi RPKI & IRR** digunakan untuk mencegah *prefix hijacking*.
		Spoofing	**Port security (L2 ACLs)** diterapkan untuk mengurangi *spoofing*.

6.3 Prosedur Pencegahan Gangguan

Prosedur	Detail Pencegahan dan Mitigasi
Isolasi Member Bermasalah	Anggota yang menyebabkan gangguan serius dapat **diisolasi sementara** hingga **shutdown port** sampai masalah terselesaikan.

Mitigasi Resource Availability	Jika terjadi *overload*, *traffic* akan **di-redistribute** ke port cadangan atau *backup switch*.
Port Congestion (Anggota)	Diberikan **Surat Peringatan (SP)** secara bertahap kepada anggota yang menyebabkan *port congestion*: **SP1** (1 bulan), **SP2** (2 bulan), dan **SP3** (jika 3 bulan berturut-turut tidak ada aksi).

6.4 Monitoring & Pelaporan

Prosedur	Detail Pelaksanaan
Pengendalian Jaringan Terpusat	**NMS** memantau semua perangkat, port, dan trafik secara *real-time*. (Contoh *tools*: Observium).
Pencatatan & Pelaporan Rutin	Laporan mencakup: Jumlah anggota, port terpakai & tersedia, *traffic* per anggota, jumlah gangguan bulanan, laporan aset & inventori, laporan perubahan layanan, dan pencatatan insiden (hardware failure, dll).
Penanganan Port Congestion (Proaktif)	Surat Pemberitahuan dikirimkan dari NOC-APJII kepada Anggota yang pemakaian Port-nya telah melebihi **80%**.
	Anggota diberikan kesempatan *upgrade interface* selambat-lambatnya dalam jangka waktu **6 bulan**.
	Jika dalam 6 bulan tidak di-*upgrade*, dilakukan **soft block** berdasarkan pemberitahuan, diikuti oleh **pencabutan kabel** dari Port (untuk dimanfaatkan anggota lain).

7. Kebijakan Peering

Prosedur	Detail Pelaksanaan & Mitigasi Keamanan
Prosedur Bilateral Peering	Anggota dapat melakukan *bilateral peering* langsung antar-router dengan persetujuan kedua pihak (tanpa komunikasi melalui APJII).
Prosedur Multilateral Peering	Anggota dapat bergabung melalui **Route Server** untuk efisiensi *peering*.
Mitigasi Network Loops (Port Security)	Implementasi **Layer 2 Access Control Lists (L2 ACLs)** membatasi MAC address yang diizinkan pada port (hanya MAC address router Anggota).
Penanganan MAC Address Changes	Perubahan MAC address dapat dilakukan melalui **web portal** (direkomendasikan beberapa jam sebelumnya) atau kontak NOC IIX dalam keadaan darurat.
Port Flap Dampening	Jika port transisi Up/Down/Up lebih dari **tiga kali dalam lima detik**, port akan dinonaktifkan (*disabled*) dan diaktifkan kembali secara otomatis setelah sepuluh detik.

8. Infrastruktur & Perawatan

Prosedur	Detail Pelaksanaan
Perawatan Berkala	Meliputi pembersihan, **update *firmware***, dan pengecekan koneksi optik.
Manajemen Fasilitas Fisik	DC harus memiliki sistem **pendingin, UPS, dan generator cadangan** yang memadai.
Prosedur Pergantian Perangkat Rusak	Jika ada *switch/transceiver* rusak, harus diganti maksimal **4 jam** sejak insiden.
Hardware Lifecycle Policy	Perangkat diganti setiap **5 tahun** untuk menjamin keandalan operasional.
Spares & N+1 Plan	Tersedia *spare* **switch, transceiver, PSU, dan *linecard*** dengan spesifikasi yang sama (redundansi N+1).
Cross-Connect Policy	Semua koneksi ke IIX *fabric* harus melalui **patch panel resmi** sesuai standar.

9. Desain & BGP Policy

Prosedur	Detail Pelaksanaan
Topologi Jaringan IIX	Menggunakan **core-switch redundant** dengan distribusi ke *edge-switch*.
IXP Network Scalability	Kapasitas direncanakan untuk pertumbuhan **3-5 tahun**. Pengadaan *hardware* baru jika ketersediaan port tersisa kurang dari **10%**.
Redudansi & Failover	Semua jalur kritis memiliki **backup otomatis** (*failover*).
Peering Policy (Route Server)	*Default*: semua prefix **ditolak** kecuali yang **valid IRR/RPKI**.
BGP Community	Disediakan *community* standar untuk *control* (**blackhole, prepend, selective announce**).
Route/Prefix Filtering	Prefiks diverifikasi **max-length, IRR, dan RPKI**.
Validasi IRR DB & Route Object	Semua prefix harus memiliki *route object* dan *as-set* yang valid.
Validasi ROA & RPKI	Prefix yang diumumkan harus **ROA valid**.
Prefix Limit	Setiap *member* wajib menetapkan batasan **max prefix** untuk mencegah *overload*.

10. Security & Abuse Handling

Prosedur	Detail Pelaksanaan
RTBH (Remote Triggered Blackhole)	Disediakan BGP *community* khusus untuk melakukan **blackhole prefix** yang diserang (DOS/DDoS *attack*).
Abuse Handling	Semua laporan *abuse* (*spam, malware, botnet*) diterima dan ditindaklanjuti oleh kontak **abuse-c**.

Traffic Policing	*Broadcast* & *unknown unicast flood* akan diberikan **rate-limit** untuk menjaga stabilitas jaringan.

11. Transparansi & Publikasi

- **Realtime Looking Glass:** Tersedia portal publik untuk pengecekan **routing & BGP session** secara *real-time*.
- **Publik Traffic Graph:** Statistik *traffic* IXP tersedia di **website resmi** untuk transparansi.

12. Governance (Tata Kelola)

Prosedur	Detail Pelaksanaan
Change Management Procedure	Semua perubahan jaringan (*maintenance, upgrade*) harus melalui proses **Change Request (CR)** terstruktur.
Incident Management Framework	Insiden dikategorikan berdasarkan *severity*, dilaporkan dengan detail, dan disertai **RCA (Root Cause Analysis)**.
Disaster Recovery Plan (DRP)	Prosedur pemulihan layanan (termasuk *failover* infrastruktur) jika terjadi **bencana besar**.
Business Continuity Plan (BCP)	Menjamin ketersediaan layanan (*waktu aktif*) meskipun ada gangguan signifikan pada infrastruktur utama.
Membership Agreement & SLA	Kontrak resmi berisi hak & kewajiban anggota, termasuk **SLA (Service Level Agreement)** terkait platform ketersediaan layanan.

13. Penutup

Dokumen Standar Operasional Prosedur (SOP) ini merupakan panduan wajib bagi seluruh personel NOC/Operasi IIX dan seluruh Anggota/Tenant yang terhubung dengan platform IIX.

Kepatuhan terhadap semua prosedur, kebijakan routing, dan ketentuan keamanan yang tercantum dalam dokumen ini adalah **mandatory** untuk menjaga stabilitas, keamanan, dan keandalan layanan *Internet Exchange*.

SOP ini akan **ditinjau dan diperbarui secara berkala** (minimal setiap tahun) atau sewaktu-waktu jika terjadi perubahan signifikan pada teknologi, regulasi, atau kebutuhan operasional. Dengan demikian, semua pihak diwajibkan untuk selalu mengacu pada versi dokumen yang paling mutakhir.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XLIV
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP SDM BIDANG DATA CENTER APJII

1. Pendahuluan

Sumber Daya Manusia (SDM) merupakan aset terpenting dalam menjaga keberlangsungan operasi Data Center APJII. Keandalan, keamanan, serta profesionalisme layanan sangat ditentukan oleh kualitas, kedisiplinan, dan kompetensi SDM. SOP ini menjadi pedoman standar bagi pengelolaan SDM agar selaras dengan best practice operasional data center, standar internasional, dan kebutuhan organisasi.

2. Latar Belakang

Data Center APJII berfungsi sebagai pusat interkoneksi, pertukaran trafik internet, serta penyimpanan data penting. Untuk memastikan kontinuitas layanan, diperlukan manajemen SDM yang terstruktur dan berstandar tinggi, mencakup aspek kompetensi teknis, manajemen shift, pengembangan karir, hingga perencanaan suksesi. SOP ini disusun agar SDM Data Center APJII dapat mendukung pencapaian target organisasi, memenuhi standar TIA-942, ISO 22301, ISO 27001, serta praktik terbaik industri.

3. Tujuan SOP

- Menetapkan pedoman pengelolaan SDM Data Center APJII.
- Menjamin konsistensi dan kontinuitas operasional.
- Meningkatkan kompetensi dan profesionalisme SDM.
- Mengatur sistem kerja, rotasi, dan shift handover.
- Mendukung compliance terhadap standar global.

4. Obyektif SOP

- Memberikan panduan formal terkait peran, tanggung jawab, dan prosedur SDM.
- Mengatur mekanisme pengembangan karir, pelatihan, dan sertifikasi.
- Mengidentifikasi kebutuhan skills & resource matriks.
- Membangun sistem manajemen performa berbasis KPI.
- Menjamin ketersediaan SDM dalam kondisi normal maupun kontingensi.

5. Dasar & Referensi Standar

- **TIA-942-C** (Telecommunications Infrastructure Standard for Data Centers).
- **ISO 27001** (Information Security Management System).
- **ISO 22301** (Business Continuity Management).
- **ISO 20000** (IT Service Management).
- Regulasi ketenagakerjaan Indonesia.
- Kebijakan internal APJII.

6. Definisi & Istilah

- **SDM Data Center**: Seluruh staf yang bertugas mengelola operasi data center.
- **Shift Handover**: Proses serah terima tugas antar shift.
- **Skills Matrix**: Pemetaan kompetensi teknis dan manajerial setiap staf.
- **Resource Matrix**: Ketersediaan personil per shift/posisi.
- **Succession Planning**: Rencana kaderisasi posisi strategis.

7. Ruang Lingkup

SOP ini berlaku untuk seluruh personil SDM yang bekerja di Data Center APJII, mencakup:

- PIC/Penanggung Jawab Operasional DC APJII
- Staff operasional (Helpdesk, Tim NOC/Teknis, Tim Security, Tim Support Pengaturan Kebersihan/Perapihan).
- Tenaga pendukung (Admin, Sekretariat, Humas, Legal).

8. Tanggung Jawab & Organisasi

- **PIC/Penanggung Jawab Operasional DC APJII**: Manager IIX dan Data Center yang bertanggung jawab penuh atas operasional dan kebijakan SDM.
- **Divisi SDM**: HRD APJII yang mengelola rekrutmen, jadwal pelatihan, program pengembangan dan evaluasi SDM.
- **Supervisor**: Memastikan jadwal shift, melakukan shift handover, memastikan kepatuhan SOP
- **Tim Teknis/NOC**: menangani operasional harian, troubleshooting, dan maintenance.
- **Tim Security**: Menjaga keamanan fasilitas Data Center.

9. Kebijakan SDM Bidang Data Center APJII

- Sangat disarankan memiliki sertifikasi minimal **CDCP** (Certified Data Centre Professional) dari **EPI** untuk Tim Teknis/NOC.
- Wajib mengikuti pelatihan **BCP/DRP** setiap tahun.
- Kedisiplinan shift 24/7 wajib dipatuhi.
- Penerapan **Code of Conduct** (etika, integritas/kepatuhan, kerahasiaan).

10. Prosedur SDM Bidang Data Center APJII

1. Standarisasi SDM
    a. Hierarki SDM
    b. Peningkatan kualitas SDM

c. Prosedur tenaga SDM kontrak
d. Governance dan Manajemen Organisasi
e. Prosedur evaluasi SDM

2. Perekrutan, Tingkat Perputaran, dan Pemberhentian SDM
   a. Prosedur rekrutmen yang jelas;
   b. Prosedur mutasi yang jelas;
   c. Rasio perekrutan dan pemberhentian SDM;
3. Peraturan dan Kepatuhan
   a. Membuat, mensosialisasikan, dan menerapkan Peraturan SDM Data Center yang jelas
   b. Menyediakan ruang pengaduan atau pelaporan untuk setiap dugaan pelanggaran terhadap Peraturan SDM Data Center
   c. Sanksi terhadap setiap tindakan pelanggaran yang dilakukan oleh SDM Data Center
4. Kepemimpinan/promosi SDM
   a. Membuat *readiness test* berkala setiap tahun.
   b. Menggunakan hasil *readiness test* sebagai salah satu parameter untuk promosi/demosi.
   c. Menciptakan SDM pemimpin yang bertanggung jawab terhadap iklim kerja yang kondusif.
   d. Menciptakan SDM pemimpin yang menjaga keberlangsungan layanan.
5. Budaya Organisasi
   a. Menilai dan mengelola norma serta perilaku SDM.
   b. Mengatur serta menilai cara bekerja dan berinteraksi SDM.
   c. Survei karyawan yang mengukur antara lain : kepuasan kerja, hubungan dengan atasan, hubungan antar SDM, kejelasan peran/*jobdesk*.
6. Kesehatan dan Keselamatan Kerja (K3)
   a. Pemahaman K3 bagi SDM Data Center;
      i. Pelatihan K3 Umum
      ii. Evaluasi kepatuhan K3 Umum secara berkala
   b. Tingkat kecelakaan kerja;
      i. Pencegahan terjadinya kecelakaan kerja;
      ii. Prosedur penanganan kecelakaan kerja.
   c. Tingkat kehadiran SDM;
      i. Sebagai indikator produktivitas SDM
7. Produktivitas
   a. Key Performance Indicator (KPI)/Produktivitas SDM;
   b. Rotasi Shift
8. Kompetensi, Keterampilan, dan Kapabilitas
   a. Pelatihan SDM;
   b. Evaluasi kompetensi berkala;
   c. Sertifikasi.
9. Ketersediaan tenaga kerja
   a. Memastikan layanan tetap berjalan dan menghindari resiko kekosongan SDM;
   b. Pengaturan rasio jadwal shifting dan libur

1. **Rekrutmen**: melalui seleksi teknis & psikotes.
2. **Onboarding**: induction training, familiarisasi fasilitas.
3. **Shift Management**: 3 shift (06.30–15.30, 14.30–23.30, 22.30–07.30).
4. **Shift Handover**: logbook, verbal briefing, pending issues.
5. **Pelaporan**: semua kegiatan dicatat pada sistem monitoring.

6. **Evaluasi**: review kinerja per 3 bulan.

11. Program Pengembangan Karir & Pelatihan

- **Basic**: Training internal (SOP, Keamanan Fisik, K3 Umum).
- **Intermediate**: Sertifikasi CDCP, ITIL Foundation, Network+.
- **Advanced**: CDCS, ISO 27001 LA, CDFOS, CDFOM.
- **Leadership Track**: Manajemen proyek, manajemen risiko, coaching.

12. Skills Matriks SDM Bidang Data Center

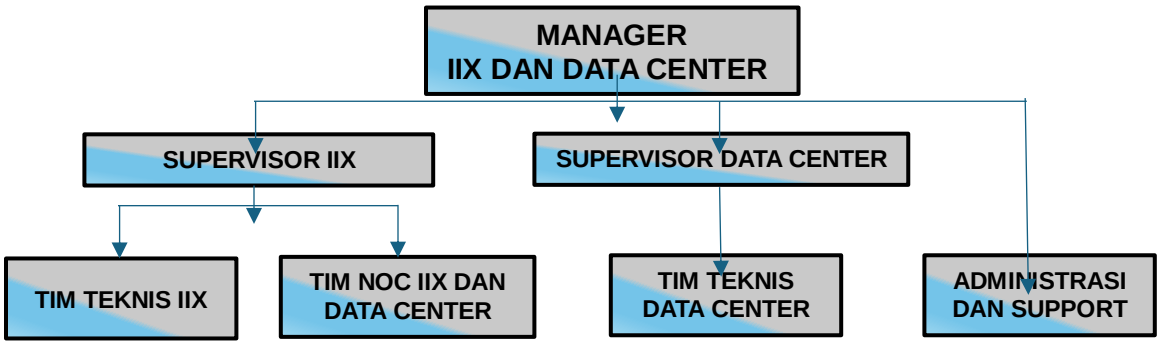
Contoh format (✓ = Menguasai, △ = Perlu Pelatihan, – = Tidak Relevan):

Skills	Tim NOC	Tim Teknis	Security	Supervisor Tim NOC/Teknis	PIC/Penanggung Jawab DC Operasional APJII
Tim NOC Operasional DC	✓	–	–	✓	✓
Power, Cooling, Telecommunication (Tim Teknis)	△	✓	–	✓	✓
ISO 27001	△	△	△	✓	✓
K3 Umum/ HSE	✓	✓	✓	✓	✓
DRP/BCP	△	△	–	✓	✓
Helpdesk Operasional DC	✓	△	–	✓	✓
Tenaga Supporting Operasional DC	✓	△	–	✓	✓

13. Resource Matriks SDM Bidang Data Center

Shift	Tim NOC	Tim Teknis	Tim Security	Supervisor IIX/Supervisor Data Center
06.30–15.30	2	2	2	1
14.30–23.30	2	1	2	1
22.30–07.30	2	1	2	0

14. Struktur Organisasi SDM Data Center APJII



15. Job Description (Ringkas)

- **PIC/Penanggung Jawab Operasional DC APJII**: strategic planning, compliance, supervisi operasional DC & IIX, KPI, pelatihan, reporting ke Manajemen APJII.
- **Supervisor Tim NOC/Teknis**: shift leader, eskalasi insiden.
- **Tim NOC/Teknis**: monitoring, troubleshooting, maintenance.
- **Security**: akses kontrol, patrol.
- **Helpdesk & Tenaga Support**.

16. Manajemen Performa Staff

- KPI bulanan: SLA Waktu Aktif, Response time, Insiden, Kepatuhan SOP.
- Penilaian 360° tiap 6 bulan.
- Reward & recognition untuk staf berprestasi.

17. Program Disiplinari

- Teguran lisan → teguran tertulis → suspensi → terminasi.
- Zero tolerance terhadap pelanggaran keamanan fisik & integritas/kepatuhan.

18. Rotasi Pekerjaan

- Rotasi antar shift setiap 6 bulan.
- Rotasi antar fungsi (NOC ↔ Teknis) untuk cross-skill.

19. Shift Hand-Over

- Mengisi logbook manual/digital.
- Briefing 15 menit sebelum pergantian shift.
- Review insiden, pekerjaan maintenance, outstanding tasks.

20. Perencanaan Contingency & Backup SDM

- Pool staf cadangan (standby).
- Bekerja dari lokasi alternati (remote) jika terjadi bencana.
- Tim BCP terlatih dengan role bergantian.

21. Perencanaan Suksesi

- Identifikasi posisi kritis (PIC/Penanggung Jawab Operasional DC APJII, Supervisor).
- Training kader internal.
- Roadmap karir (Tim Teknis/NOC → Supervisor Tim Teknis/NOC).
- Mentoring oleh senior staff.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN XLV
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP STANDARISASI SDM BIDANG DATA CENTER APJII

1. Pendahuluan

Sumber Daya Manusia (SDM) merupakan faktor kunci dalam keberhasilan operasional data center. Tingkat keandalan infrastruktur data center harus didukung oleh tenaga kerja yang memiliki kompetensi, integritas, serta pemahaman standar internasional. Oleh karena itu, diperlukan **Standar Operasional Prosedur (SOP) SDM** yang mengatur tata kelola, peningkatan kompetensi, serta evaluasi SDM di bidang data center APJII.

2. Latar Belakang

APJII sebagai organisasi pengelola data center yang menjadi tulang punggung ekosistem internet nasional memiliki tanggung jawab dalam menjaga standar layanan, keandalan, dan keamanan. Sejalan dengan tuntutan sertifikasi internasional (misalnya TIA-942, ISO 27001, ISO 22301, ITIL), SDM yang mengelola data center harus distandarisasi, baik dari aspek **kompetensi teknis, prosedural, maupun manajerial**. SOP ini hadir untuk memberikan pedoman baku dalam pengelolaan SDM agar kinerja dan layanan data center tetap sesuai standar.

3. Tujuan SOP

- Menjamin **keseragaman standar kompetensi** SDM data center APJII.
- Menyediakan **kerangka pengelolaan SDM** yang sistematis, terukur, dan sesuai best practice.
- Menentukan **peran, tanggung jawab, dan kewenangan** setiap hierarki SDM.
- Menjadi acuan dalam **proses perekrutan, pelatihan, evaluasi, dan pengembangan SDM**.
- Mendukung **kepatuhan terhadap regulasi nasional dan standar internasional** dalam pengelolaan data center.

4. Obyektif SOP

- Memastikan **kualitas layanan data center** melalui SDM yang kompeten.
- Menjaga **resiliensi operasional** data center melalui ketersediaan tenaga ahli yang memadai.
- Menjamin **transparansi dan akuntabilitas** dalam pengelolaan SDM.

- Meningkatkan **efektivitas governance dan manajemen organisasi** dalam mendukung operasi data center.

5. Dasar & Referensi Standar

SOP ini mengacu pada standar, regulasi, dan pedoman berikut:

- **ISO/IEC 27001:2022** – Information Security Management System
- **ISO 22301:2019** – Business Continuity Management
- **ISO/IEC 20000-1:2018** – IT Service Management
- **ANSI/TIA-942-C:2024** – Data Center Standards
- **ITIL v4** – IT Service Management Best Practices
- **Undang-Undang No. 11 Tahun 2008 (ITE) & Perubahannya**
- **Peraturan Menteri Ketenagakerjaan Republik Indonesia** tentang hubungan kerja, kontrak, dan evaluasi SDM.

6. Definisi & Istilah

- **SDM Data Center**: Tenaga kerja yang berperan dalam pengoperasian, pemeliharaan, pengawasan, dan manajemen data center.
- **Standarisasi SDM**: Proses penetapan standar kompetensi, kualifikasi, dan prosedur kerja bagi tenaga SDM.
- **Kontrak Kerja**: Perjanjian tertulis antara APJII dan tenaga kerja yang memuat hak dan kewajiban kedua belah pihak.
- **Evaluasi SDM**: Proses penilaian kinerja SDM berdasarkan indikator yang telah ditentukan.
- **Governance SDM**: Tata kelola manajemen SDM yang menjamin kepatuhan terhadap kebijakan, regulasi, dan standar layanan.

7. Ruang Lingkup

a. Hierarki SDM

Struktur SDM Data Center & IIX APJII dibagi sebagai berikut:

1. **MANAGER – TOP MANAGEMENT (MANAGER IIX DAN DATA CENTER)**
    - Penanggung Jawab Operasional DC & IIX APJII
    - Bertanggung jawab penuh atas strategi, kepatuhan, dan keberlangsungan layanan.
2. **SUPERVISOR – LEADER (SUPERVISOR IIX, SUPERVISOR DATA CENTER)**
    - Infrastruktur, Operasional, Keamanan & Compliance.
    - Bertugas mengoordinasikan Tim teknis, Tim NOC dan administrasi.
    - Mengatur Jadwal Shift, Jadwal Pemeliharaan dan Jadwal kegiatan Keamanan di DC APJII.
    - Memastikan kegiatan operasional harian berjalan sesuai SOP.
3. **TIM TEKNIS IIX**
    - Bertanggung jawab untuk setiap permasalahan pada Power (Listrik dan UPS), Network (Switch dan OTB), Cooling dan Logical Security (APAR, Fire Supression dan Access Control).
    - Memastikan semua perangkat (termasuk Power) berjalan dengan baik.

4. **TIM TEKNIS DATA CENTER**
    - Bertanggung jawab untuk setiap permasalahan pada Cabling, Server dan Storage.
    - Bertanggung jawab atas pemasangan, penggantian dan dismantle Interkoneksi.
    - Memastikan semua perangkat berjalan dengan baik dalam mendukung kegiatan operasional.
5. **TIM NOC (NOC IIX DAN DATA CENTER)**
    - Melakukan pemantauan, pemeliharaan, dan troubleshooting.
    - Melakukan pendampingan setiap Anggota/Tenant, Vendor dan Tamu yang berkunjung dan melakukan kegiatan di area DC APJII.
6. **ADMINISTRASI DAN SUPPORT**
    - Mendukung seluruh proses Administrasi Operasional yang meliputi proses dokumentasi, pelaporan dan administrasi lainnya.

b. Peningkatan Kualitas SDM

- **Rekrutmen**: Seleksi berbasis kompetensi (kompetensi teknis, manajerial, dan soft skill).
- **Pelatihan & Sertifikasi**: Wajib mengikuti pelatihan standar industri (misalnya CDCP/CDCS/CDCE, ITIL, ISO 27001 Lead Implementer, CCNA/CCNP).
- **Program Pengembangan**: On-the-job training, coaching & mentoring, knowledge sharing, rotasi antar divisi.
- **Continuous Improvement**: Evaluasi kinerja dikaitkan dengan kebutuhan training berkelanjutan.

c. Prosedur Tenaga SDM Kontrak

1. **Perencanaan Kebutuhan**
    - Disusun oleh Manager, disetujui oleh Kepala Bidang Terkait.
2. **Seleksi & Rekrutmen**
    - Melalui HRD APJII dengan proses uji kompetensi.
3. **Penempatan & Orientasi**
    - Kontrak kerja minimal 1 tahun, masa percobaan 3 bulan.
4. **Evaluasi & Perpanjangan**
    - Dilakukan setiap 6 bulan dengan penilaian kinerja.
    - Perpanjangan kontrak berdasarkan hasil evaluasi.
5. **Pemutusan Hubungan Kerja**
    - Mengacu pada ketentuan hukum ketenagakerjaan RI.

d. Governance dan Manajemen Organisasi

- **Kebijakan SDM**: Harus terdokumentasi, dipublikasikan dan dipatuhi oleh seluruh karyawan.
- **Struktur Organisasi**: Jelas, dengan pembagian peran dan tanggung jawab yang transparan.
- **Sistem Dokumentasi**: Semua kegiatan SDM terdokumentasi (training, evaluasi, kontrak, promosi).
- **Audit Internal**: Dilakukan minimal 1x dalam setahun untuk menilai kesesuaian dengan standar.
- **Compliance & Ethics**: Setiap SDM wajib patuh pada kode etik, kerahasiaan data, dan peraturan keamanan informasi.

e. Prosedur Evaluasi SDM

1. **Indikator Evaluasi**
    - Kompetensi teknis (pengetahuan & keterampilan)
    - Disiplin kerja (kehadiran, kepatuhan SOP)
    - Integritas & etika
    - Kinerja individu & kontribusi tim
    - Inovasi & inisiatif perbaikan
2. **Metode Evaluasi**
    - **Penilaian Kinerja** (Performance Appraisal) setiap 6 bulan.
    - **360° Feedback**: Dari atasan, rekan sejawat, bawahan (jika relevan).
    - **Key Performance Indicator (KPI)** yang ditetapkan oleh Manager.
3. **Tindak Lanjut**
    - Hasil evaluasi digunakan untuk:
        - Promosi / mutasi jabatan.
        - Rekomendasi training tambahan.
        - Perpanjangan atau pemutusan kontrak.
        - Penghargaan karyawan berprestasi.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

Lampiran Form SOP Standarisasi SDM Data Center APJII

1. Contoh Form Struktur Hierarki SDM (Organizational Chart Approval Form)

Tujuan: Dokumentasi hierarki SDM, persetujuan struktur organisasi, dan update struktur.

No	Nama Jabatan	Nama Pegawai	Unit/Divisi	Atasan Langsung	Tanggal Efektif	Tanda Tangan Atasan	Catatan
1	Manager IIX dan Data Center		Operasional DC	Kepala Bidang Terkait			
2	Supervisor IIX		Operasional DC	Manager			
3	Supervisor Data Center		Operasional DC	Manager			
4	Tim Teknis IIX		Operasional DC	Supervisor IIX			
5	Tim Teknis Data Center		Operasional DC	Supervisor Data Center			
6	NOC IIX dan Data Center		Operasional DC	Supervisor IIX			
7	Administrasi dan Support		Operasional DC	Manager			

2. Contoh Form Rencana & Realisasi Peningkatan Kualitas SDM (Training & Development Form)

Tujuan: Monitoring rencana pengembangan kompetensi (training, sertifikasi, workshop).

No	Nama Pegawai	Jabatan	Training/Sertifikasi	Penyelenggara	Jadwal	Status (Rencana/Realisasi)	Catatan Evaluasi
1			CDCP (Certified Data Center Professional)	EPI	Jan 2025	Rencana	
2			ISO 27001 Internal Auditor	APJII Academy	Mar 2025	Realisasi	Lulus
3			CCNA/CCNP	Cisco Partner	Jun 2025	Rencana	

3. Contoh Form Rekrutmen & Kontrak SDM (Employment Contract Request Form)

Tujuan: Proses administrasi rekrutmen dan kontrak SDM (tetap/kontrak).

Bagian	Isi
Data Pegawai	Nama: … ; Tempat/Tgl Lahir: … ; Alamat: … ; No. KTP: … ; No. HP: …
Jabatan	……
Divisi/Unit	……
Jenis Kontrak	☐ Pegawai Tetap ☐ Pegawai Kontrak ☐ Outsourcing
Durasi Kontrak	…… (contoh: 1 Tahun, mulai 01/01/2025 – 31/12/2025)

Bagian	Isi
Masa Percobaan	…… (contoh: 3 Bulan)
Gaji & Benefit	Gaji Pokok: …… ; Tunjangan: …… ; Asuransi: ……
Pernyataan & Tanda Tangan	Pegawai: _____ ; HRD: _____ ; Atasan Langsung: _____ ; Tanggal: …

4. Contoh Form Governance & Manajemen Organisasi (HR Governance Compliance Checklist)

Tujuan: Audit internal untuk memastikan tata kelola SDM sesuai SOP.

No	Area Audit	Pertanyaan	Status (Ya/Tidak)	Catatan Temuan	Tindak Lanjut
1	Struktur Organisasi	Apakah struktur organisasi terbaru terdokumentasi?			
2	SOP SDM	Apakah seluruh pegawai sudah membaca & menandatangani kepatuhan SOP?			
3	Training	Apakah training tercatat di database?			
4	Evaluasi	Apakah semua pegawai telah dievaluasi dalam 6 bulan terakhir?			
5	Kontrak Kerja	Apakah kontrak karyawan kontrak terdokumentasi dan berlaku?			

5. Contoh Form Evaluasi Kinerja SDM (Performance Appraisal Form)

Tujuan: Penilaian kinerja karyawan per 6 bulan/tahun.

Data Pegawai	Keterangan
Nama	……
Jabatan	……
Unit/Divisi	……
Periode Evaluasi	……
Atasan Penilai	……

Contoh Indikator Penilaian

Aspek Penilaian	Bobot (%)	Skor (1-5)	Nilai (Bobot x Skor)	Catatan
Kompetensi Teknis	30%			
Disiplin & Kehadiran	20%			
Kepatuhan SOP & Etika	15%			
Inovasi & Inisiatif	15%			
Kinerja Tim & Kolaborasi	10%			
Kepuasan Stakeholder (Internal/External)	10%			

Total Skor: ……..

Kategori Hasil:

- 90–100 = Sangat Baik
- 75–89 = Baik
- 60–74 = Cukup
- <60 = Kurang

Tanda Tangan:

- Pegawai: _____
- Penilai/Atasan: _____
- HRD: _____

6. Contoh Form Catatan Disiplin & Etika (Disciplinary Action Form)

Tujuan: Dokumentasi pelanggaran disiplin dan tindakan perbaikan.

No	Nama Pegawai	Jabatan	Jenis Pelanggaran	Tanggal Kejadian	Tindakan Korektif	Status (Selesai/Proses)	Tanda Tangan HRD
1			Terlambat hadir >3x	10/07/2025	Surat Peringatan 1	Selesai	
2			Lalai SOP Keamanan	20/08/2025	Pembinaan	Proses	

7. Contoh Form Penghargaan & Apresiasi SDM (Employee Recognition Form)

Tujuan: Pencatatan karyawan berprestasi & motivasi kerja.

No	Nama Pegawai	Jabatan	Prestasi	Periode	Jenis Penghargaan	Tanda Tangan Atasan
1			Menyelesaikan migrasi server tanpa downtime	Q3 2025	Employee of the Month	
2			Membuat SOP baru sistem cooling	2025	Bonus & Sertifikat	

8. Contoh Form Rotasi, Mutasi & Promosi (Career Movement Form)

Tujuan: Dokumentasi pergerakan karier SDM.

Data Pegawai	Keterangan
Nama	……
Jabatan Lama	……
Unit Lama	……
Jabatan Baru	……
Unit Baru	……

Data Pegawai	Keterangan
Tanggal Efektif	……
Alasan	……
Persetujuan	Atasan: _____ ; HRD: _____ ; Manajemen: _____

9. Contoh Form Exit Interview SDM (Employee Exit Interview Form)

Tujuan: Evaluasi alasan pegawai berhenti/resign untuk perbaikan manajemen SDM.

Data Pegawai	Keterangan
Nama	……
Jabatan	……
Lama Bekerja	……
Tanggal Resign	……
Alasan Resign	☐ Pindah kerja ☐ Gaji ☐ Lingkungan kerja ☐ Lainnya: ……
Feedback Pegawai	……
Rekomendasi Perbaikan	……
Tanda Tangan HRD	……

LAMPIRAN XLVI
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PEREKRUTAN, TINGKAT PERPUTARAN & PEMBERHENTIAN SDM BIDANG DATA CENTER APJII

1. Pendahuluan

Sumber Daya Manusia (SDM) merupakan aset penting dalam pengelolaan dan pengoperasian data center APJII. Keberhasilan operasional data center sangat ditentukan oleh kualitas, kompetensi, dan stabilitas tenaga kerja yang tersedia. Oleh karena itu, dibutuhkan prosedur baku terkait rekrutmen, pengelolaan tingkat perputaran (turnover), mutasi, dan pemberhentian SDM untuk menjamin kesinambungan layanan sesuai standar internasional manajemen data center.

2. Latar Belakang

Data center APJII berperan sebagai pusat infrastruktur internet nasional yang harus beroperasi dengan tingkat keandalan tinggi (high availability). Untuk mendukung hal tersebut, manajemen SDM wajib diatur melalui SOP yang:

- Menjamin proses rekrutmen dilaksanakan secara transparan, objektif, dan sesuai kebutuhan kompetensi.
- Menetapkan mekanisme mutasi internal agar rotasi SDM tetap mempertahankan kompetensi inti.
- Mengatur indikator rasio perekrutan, mutasi, dan pemberhentian agar selaras dengan target operasional data center.
- Menjamin keberlangsungan operasional dan keamanan data center melalui pengelolaan SDM yang berkelanjutan.

3. Tujuan SOP

1. Menstandarkan proses perekrutan, mutasi, dan pemberhentian SDM di bidang data center APJII.
2. Menjaga kesinambungan tenaga kerja yang kompeten sesuai kebutuhan operasional data center.
3. Mengontrol tingkat perputaran SDM agar tetap berada dalam batas wajar dan tidak mengganggu kinerja organisasi.
4. Menyediakan acuan formal bagi manajemen, HR, dan pimpinan unit dalam pengambilan keputusan terkait SDM.

4. Obyektif SOP

- Memastikan setiap rekrutmen menghasilkan SDM yang sesuai kompetensi teknis (misalnya: network engineer, data center engineer, facility engineer, security officer).
- Menjamin mutasi dilakukan berdasarkan kebutuhan organisasi dan pengembangan karir SDM.
- Mengendalikan tingkat perputaran SDM agar tidak melebihi standar industri data center (≤10% per tahun).
- Menjamin proses pemberhentian SDM dilakukan sesuai ketentuan hukum dan etika organisasi.

5. Dasar & Referensi Standar

- **Peraturan Perundang-undangan**: UU No. 13 Tahun 2003 tentang Ketenagakerjaan (beserta revisi/UU Cipta Kerja).
- **Standar Manajemen Data Center**: TIA-942, ISO/IEC 22237.
- **Standar Keamanan Informasi**: ISO/IEC 27001.
- **Standar Manajemen SDM**: ISO 30405 (Recruitment), ISO 30409 (Workforce Planning).
- **Peraturan Internal APJII**: Kebijakan HR, aturan organisasi, dan perjanjian kerja bersama.

6. Definisi & Istilah

- **Rekrutmen**: Proses penarikan, seleksi, dan penempatan calon SDM sesuai kebutuhan organisasi.
- **Mutasi**: Perpindahan SDM dari satu posisi ke posisi lain, baik secara horizontal (setara) maupun vertikal (promosi/demosi).
- **Turnover Rate (Tingkat Perputaran SDM)**: Persentase jumlah SDM yang keluar dibandingkan dengan jumlah rata-rata karyawan dalam periode tertentu.
- **Pemberhentian**: Berakhirnya hubungan kerja karena pengunduran diri, pemutusan hubungan kerja (PHK), berakhirnya masa kontrak, pension yang sesuai dengan perundang-undangan yang berlaku.
- **Rasio Perekrutan dan Pemberhentian**: Perbandingan antara jumlah SDM yang direkrut dengan jumlah SDM yang diberhentikan dalam periode tertentu.

7. Ruang Lingkup

a. Prosedur Rekrutmen yang Jelas

1. **Analisis Kebutuhan**
    - Manager Divisi mengajukan kebutuhan SDM baru kepada HR berdasarkan manning table dan beban kerja.
2. **Perencanaan Rekrutmen**
    - HR menyusun job description, job specification, dan kualifikasi yang disetujui oleh Kabid terkait.
3. **Sourcing Kandidat**
    - Melalui iklan lowongan, kerjasama universitas, asosiasi profesi, atau headhunter.
4. **Seleksi Administrasi**
    - Verifikasi dokumen (CV, ijazah, sertifikasi teknis).
5. **Tes Kompetensi**
    - Tes teknis (jaringan, sistem, fasilitas data center, dll).

    - Tes psikotes dan wawancara HR.
    - Wawancara user/pimpinan unit data center.
6. **Jangka Waktu Perekrutan**
    - HR berkewajiban melakukan perekrutan paling lama 30 hari sejak diumumkannya kebutuhan SDM.
7. **Penawaran Kerja & Onboarding**
    - Surat penawaran kerja.
    - Orientasi & induction training.

b. Prosedur Mutasi yang Jelas

1. **Identifikasi Kebutuhan Mutasi**
    - Karena rotasi, pengembangan karir, atau kebutuhan organisasi.
2. **Penilaian Kinerja & Kompetensi**
    - Hanya SDM dengan kinerja baik yang memenuhi syarat mutasi.
3. **Persetujuan Manajemen**
    - Mutasi diajukan oleh pimpinan unit dan disetujui oleh HR & Kabid terkait.
4. **Implementasi Mutasi**
    - Penetapan jabatan baru, update struktur organisasi, dan masa adaptasi maksimal 3 bulan.

c. Rasio Perekrutan dan Pemberhentian SDM

- **Target Rasio Perekrutan : Pemberhentian = 1,2 : 1**
  (artinya jumlah perekrutan harus lebih tinggi dari jumlah pemberhentian untuk menjaga ketersediaan tenaga kerja).
- **Turnover Rate Maksimal = 10% per tahun** (mengacu best practice operasional data center).
- **Evaluasi**: HR wajib menyusun laporan bulanan & tahunan terkait rekrutmen, mutasi, dan turnover.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

Lampiran SOP SDM Data Center APJII

Lampiran 1 – Contoh Form Permintaan Rekrutmen SDM

Bagian	Keterangan
Nomor Form	……
Unit Pemohon	……
Tanggal Permintaan	……
Jabatan yang Dibutuhkan	……
Jumlah SDM	……
Alasan Kebutuhan	☐ Penggantian ☐ Penambahan Beban Kerja ☐ Proyek Baru ☐ Lainnya (sebutkan)
Kompetensi Teknis yang Diperlukan	……
Kualifikasi Minimal	☐ D3 ☐ S1 ☐ Sertifikasi Teknis (sebutkan: ……)
Deadline Pemenuhan	……
Persetujuan Atasan Unit	Nama/TTD: ……
Persetujuan HRD	Nama/TTD: ……

Lampiran 2 – Contoh Form Seleksi Rekrutmen SDM

Nama Kandidat	Posisi Dilamar	Tahap Seleksi	Hasil/Ulasan	Status
……	……	Seleksi Administrasi	Lulus/Tidak Lulus	……
		Tes Teknis	Nilai: ……	……
		Psikotes	Nilai: ……	……
		Wawancara User	Catatan: ……	……
		Wawancara HR	Catatan: ……	……

Nama Kandidat	Posisi Dilamar	Tahap Seleksi	Hasil/Ulasan	Status
		Finalisasi	Diterima/Ditolak	……

Lampiran 3 – Contoh Form Onboarding & Induksi SDM Baru

Nama Karyawan	Jabatan	Tanggal Mulai	Unit Kerja	Induction Training	Checklist Dokumen	Keterangan
……	……	……	……	☐ DC Orientation ☐ SOP HR ☐ K3 ☐ Security Awareness	☐ Kontrak ☐ ID Card ☐ NDA ☐ Sertifikat	……

Lampiran 4 – Contoh Form Mutasi SDM

Bagian	Keterangan
Nomor Form	……
Nama Karyawan	……
NIK	……
Jabatan Saat Ini	……
Unit Kerja Saat Ini	……
Jabatan Baru	……
Unit Kerja Baru	……
Alasan Mutasi	☐ Pengembangan Karir ☐ Rotasi Jabatan ☐ Kebutuhan Organisasi

Bagian	Keterangan
	☐ Lainnya: ……
Tanggal Efektif Mutasi	……
Catatan Evaluasi Kinerja (oleh Atasan Lama)	……
Persetujuan Atasan Lama	Nama/TTD: ……
Persetujuan Atasan Baru	Nama/TTD: ……
Persetujuan HRD	Nama/TTD: ……

Lampiran 5 – Contoh Form Laporan Turnover SDM (Bulanan/Tahunan)

Periode	Jumlah Awal SDM	Jumlah Rekrutmen	Jumlah Pemberhentian	Jumlah Mutasi	Jumlah Akhir SDM	Turnover Rate (%)
Jan	……	……	……	……	……	……
Feb	……	……	……	……	……	……
…	……	……	……	……	……	……
Total Tahun	……	……	……	……	……	……

📌**Rumus Turnover Rate**:

Jumlah karyawan yang keluar selama periode waktu tertentu dibagi dengan jumlah rata-rata karyawan pada periode yang sama, lalu dikalikan 100%.

$$\frac{\text{Jumlah karyawan keluar}}{(\text{Jumlah karyawan awal} + \text{Jumlah karyawan akhir})/2} \times 100\%$$

Lampiran 6 – Contoh Form Pemberhentian SDM

Bagian	Keterangan
Nomor Form	……
Nama Karyawan	……
NIK	……
Jabatan	……
Unit Kerja	……
Tanggal Efektif Pemberhentian	……
Jenis Pemberhentian	☐ Pengunduran Diri ☐ PHK ☐ Pensiun ☐ Lainnya: ……
Alasan Pemberhentian	……
Hasil Exit Interview	……
Dokumen Diserahkan	☐ ID Card ☐ Laptop ☐ Akses DC ☐ Lainnya: ……
Kompensasi/Benefit	……
Persetujuan Atasan	Nama/TTD: ……
Persetujuan HRD	Nama/TTD: ……
Persetujuan Direksi	Nama/TTD: ……

Lampiran 7 – Contoh Form Exit Interview SDM

Nama Karyawan	Jabatan	Tanggal Exit Interview	Alasan Resign/PHK	Komentar Karyawan	Rekomendasi HR
……	……	……	☐ Karir ☐ Gaji ☐ Lingkungan Kerja ☐ Lainnya: ……	……	……

LAMPIRAN XLVII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PERATURAN DAN KEPATUHAN SDM BIDANG DATA CENTER APJII

1. Pendahuluan

Sumber Daya Manusia (SDM) merupakan aset strategis dalam pengelolaan Data Center APJII yang berperan menjaga keberlangsungan layanan, keamanan, serta kepatuhan terhadap standar industri. SOP ini disusun sebagai pedoman baku untuk memastikan setiap SDM yang terlibat memahami, mematuhi, dan melaksanakan peraturan serta etika kerja yang berlaku, sekaligus memberikan mekanisme penanganan apabila terjadi pelanggaran.

2. Latar Belakang

Pengelolaan Data Center menuntut tingkat kepatuhan dan profesionalisme yang tinggi karena berkaitan dengan keamanan data, operasional infrastruktur kritis, dan reputasi organisasi. Risiko kesalahan manusia, pelanggaran aturan, atau ketidakpatuhan dapat berdampak serius pada layanan dan kepercayaan anggota/tenant APJII. Oleh sebab itu, perlu adanya sistem peraturan dan kepatuhan SDM yang terdokumentasi, tersosialisasi, serta memiliki mekanisme pengaduan dan penegakan sanksi yang tegas.

3. Tujuan SOP

- Menetapkan pedoman peraturan SDM dalam operasional Data Center APJII.
- Menjamin kepatuhan seluruh SDM terhadap standar etika, regulasi, dan kebijakan organisasi.
- Memberikan ruang pengaduan yang aman dan transparan terkait dugaan pelanggaran.
- Menetapkan mekanisme pemberian sanksi yang adil, proporsional, dan konsisten.

4. Obyektif SOP

- Memastikan seluruh SDM memahami hak dan kewajiban mereka dalam menjaga kepatuhan.
- Mengurangi potensi pelanggaran melalui regulasi dan edukasi yang jelas.

- Menegakkan budaya integritas, profesionalisme, dan akuntabilitas di lingkungan Data Center APJII.
- Melindungi organisasi dari risiko hukum, finansial, dan reputasi akibat pelanggaran SDM.

5. Dasar & Referensi Standar

- **Undang-Undang No. 13 Tahun 2003** tentang Ketenagakerjaan.
- **Peraturan Menteri Kominfo RI** terkait penyelenggaraan Data Center & keamanan informasi.
- **ISO/IEC 27001** – Information Security Management System (ISMS).
- **ISO/IEC 20000** – IT Service Management.
- **ISO 22301** – Business Continuity Management.
- **TIA-942** – Data Center Standards.
- **AD/ART, Peraturan Asosiasi dan Kebijakan Internal APJII** lainnya.

6. Definisi & Istilah

- **SDM Data Center**: Seluruh karyawan, teknisi, staf operasional, manajemen, maupun tenaga kontrak yang bekerja di lingkungan Data Center APJII.
- **Peraturan SDM**: Aturan tertulis mengenai hak, kewajiban, larangan, serta etika kerja yang wajib dipatuhi SDM.
- **Kepatuhan (Compliance)**: Tingkat ketaatan SDM terhadap peraturan, prosedur, standar, dan hukum yang berlaku.
- **Pengaduan**: Laporan resmi dari SDM terkait dugaan pelanggaran atau ketidakpatuhan.
- **Sanksi**: Konsekuensi yang diberikan kepada SDM yang terbukti melakukan pelanggaran.

7. Ruang Lingkup

SOP ini berlaku untuk seluruh SDM Data Center APJII dan mencakup:

1. **Membuat, Menyosialisasikan, dan Menerapkan Peraturan SDM Data Center**
    - Penyusunan Peraturan SDM berdasarkan standar hukum dan kebijakan APJII.
    - Sosialisasi melalui briefing rutin, email resmi, modul e-learning, serta handbook SDM.
    - Penerapan melalui pengawasan harian, audit internal, serta evaluasi berkala.
2. **Menyediakan Ruang Pengaduan atau Pelaporan Dugaan Pelanggaran**
    - Penyediaan kanal pelaporan (email khusus, hotline internal, aplikasi pelaporan).
    - Jaminan kerahasiaan dan perlindungan pelapor (whistleblower protection).
    - Proses investigasi yang transparan, objektif, dan terdokumentasi.
3. **Sanksi terhadap Pelanggaran Peraturan SDM**
    - **Tingkat Pelanggaran**:
        - *Ringan*: keterlambatan, kelalaian administrasi.
        - *Sedang*: ketidakpatuhan SOP operasional, pelanggaran etika kerja.
        - *Berat*: sabotase, pelanggaran keamanan data, penyalahgunaan akses.

- **Jenis Sanksi**:
  - Teguran lisan/tertulis.
  - Skorsing sementara.
  - Penurunan jabatan atau hak tertentu.
  - Pemutusan hubungan kerja (PHK) sesuai ketentuan hukum.
- Sanksi diterapkan berdasarkan hasil investigasi dan keputusan manajemen sesuai prinsip keadilan.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

Lampiran SOP Peraturan & Kepatuhan SDM Data Center APJII

Lampiran 1 – Peraturan Umum SDM Data Center APJII

A. Hak SDM

1. Mendapatkan lingkungan kerja yang aman, tertib, dan kondusif.
2. Mendapatkan pelatihan sesuai kebutuhan operasional Data Center.
3. Mendapatkan kompensasi sesuai peraturan ketenagakerjaan dan kebijakan APJII.
4. Mendapatkan perlindungan hukum atas setiap laporan pelanggaran (whistleblower protection).

B. Kewajiban SDM

1. Mematuhi SOP dan standar kerja yang berlaku di Data Center.
2. Menjaga kerahasiaan data, informasi, dan aset organisasi.
3. Menggunakan akses sistem dan fasilitas hanya untuk kepentingan pekerjaan.
4. Menjaga etika dan profesionalisme dalam setiap interaksi kerja.
5. Melaporkan setiap indikasi pelanggaran atau insiden keamanan.

C. Larangan SDM

1. Membawa perangkat atau media penyimpanan pribadi ke area terbatas tanpa izin.
2. Memberikan akses sistem atau data center kepada pihak tidak berwenang.
3. Menggunakan fasilitas organisasi untuk kepentingan pribadi/ilegal.
4. Melakukan tindakan sabotase, pencurian, atau perusakan aset.
5. Melakukan pelecehan, diskriminasi, atau tindakan yang mencederai integritas organisasi.

Lampiran 2 – Contoh Formulir Pengaduan/Pelaporan Dugaan Pelanggaran

Formulir Pengaduan SDM Data Center APJII

Bagian	Isi
Nomor Laporan	……
Tanggal Laporan	……
Nama Pelapor	…… (dapat anonim)
Jabatan/Unit	……
Media Pelaporan	☐ Email ☐ Hotline ☐ Aplikasi ☐ Lainnya
Jenis Pelanggaran	☐ Ringan ☐ Sedang ☐ Berat
Kronologi Singkat	…… ……

Bagian	Isi
Pihak Terlapor	……
Bukti Pendukung	…… ……
Tindakan yang Diharapkan	…… ……
Tanda Tangan Pelapor	……

Lampiran 3 – Contoh Formulir Berita Acara Pemeriksaan Pelanggaran

Berita Acara Pemeriksaan Dugaan Pelanggaran SDM Data Center APJII

Bagian	Isi
Nomor Berita Acara	……
Tanggal Pemeriksaan	……
Nama Terlapor	……
Jabatan/Unit	……
Jenis Pelanggaran	☐ Ringan ☐ Sedang ☐ Berat
Kronologi Temuan	…… ……
Hasil Pemeriksaan	…… ……
Kesimpulan Tim	…… ……
Rekomendasi Sanksi	☐ Teguran ☐ Skorsing ☐ Penurunan Jabatan ☐ PHK ☐ Lainnya: ……
Nama & Tanda Tangan Pemeriksa	……
Nama & Tanda Tangan Atasan	……

Lampiran 4 – Matriks Jenis Pelanggaran & Sanksi

Kategori Pelanggaran	Contoh Kasus	Jenis Sanksi
Ringan	Datang terlambat, lupa logbook, lalai input laporan	Teguran lisan/tertulis
Sedang	Melanggar prosedur akses ruang server, tidak mengikuti SOP keamanan	Teguran tertulis, skorsing sementara
Berat	Memberikan akses tanpa izin, sabotase sistem, pencurian data/aset	Skorsing, penurunan jabatan, PHK

Lampiran 5 – Contoh Formulir Tanda Terima Sosialisasi Peraturan SDM

Tanda Terima Sosialisasi Peraturan SDM Data Center APJII

Saya yang bertanda tangan di bawah ini menyatakan telah:

- Menerima sosialisasi mengenai peraturan dan kepatuhan SDM Data Center APJII.
- Memahami hak, kewajiban, dan larangan sesuai ketentuan yang berlaku.
- Bersedia mematuhi dan menerima konsekuensi atas pelanggaran peraturan.

Nama Lengkap	Jabatan/Unit	Tanggal	Tanda Tangan
……	……	……	……

Lampiran 6 – Alur Penanganan Dugaan Pelanggaran

1. **Pelaporan** – SDM melaporkan dugaan pelanggaran melalui kanal resmi (email, hotline, aplikasi).
2. **Penerimaan Laporan** – Divisi HR & Compliance mencatat laporan dalam register pelanggaran.
3. **Investigasi Awal** – Tim investigasi melakukan verifikasi bukti awal.
4. **Pemeriksaan** – Terlapor dipanggil untuk memberikan klarifikasi.
5. **Rekomendasi Sanksi** – Tim investigasi menyerahkan hasil pemeriksaan kepada manajemen.
6. **Keputusan Manajemen** – Penetapan sanksi sesuai kategori pelanggaran.
7. **Dokumentasi & Arsip** – Semua dokumen disimpan dalam sistem kepatuhan.

LAMPIRAN XLVIII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP KEPEMIMPINAN ATAU PROMOSI SDM BIDANG DATA CENTER APJII

1. Pendahuluan

Sumber Daya Manusia (SDM) merupakan aset utama dalam pengelolaan data center. Tingginya standar layanan, keberlangsungan operasional, serta kebutuhan akan iklim kerja yang sehat menuntut adanya mekanisme kepemimpinan yang jelas, objektif, dan berkelanjutan. SOP ini disusun untuk memastikan bahwa proses promosi, demosi, dan pengembangan kepemimpinan SDM di lingkungan data center APJII dilakukan secara transparan, terukur, dan selaras dengan standar internasional.

2. Latar Belakang

- Data center APJII berperan vital sebagai pusat layanan infrastruktur internet nasional, sehingga membutuhkan SDM pemimpin yang memiliki kompetensi teknis, manajerial, dan integritas tinggi.
- Proses promosi SDM tidak hanya ditentukan oleh masa kerja atau pengalaman, tetapi juga melalui readiness test yang dilakukan secara berkala.
- Perlu adanya pedoman tertulis yang menjamin konsistensi dalam pengelolaan kepemimpinan, promosi, maupun demosi SDM.

3. Tujuan SOP

- Menetapkan standar proses promosi dan pengembangan kepemimpinan SDM di data center APJII.
- Menjamin bahwa SDM yang dipromosikan memiliki kemampuan kepemimpinan, tanggung jawab, serta berkomitmen menjaga keberlangsungan layanan.
- Menciptakan iklim kerja yang kondusif dengan menempatkan pemimpin yang tepat pada posisi strategis.
- Menjadi acuan evaluasi objektif untuk promosi maupun demosi SDM berdasarkan readiness test.

4. Obyektif SOP

- Meningkatkan kualitas kepemimpinan di lingkungan data center APJII.
- Mengurangi risiko kegagalan operasional akibat kepemimpinan yang tidak kompeten.

- Memberikan jalur karier yang jelas, transparan, dan adil bagi seluruh SDM.
- Memastikan keberlangsungan layanan data center melalui kepemimpinan yang visioner dan bertanggung jawab.

5. Dasar & Referensi Standar

- **ISO/IEC 20000-1:2018** – IT Service Management.
- **ISO/IEC 27001:2022** – Information Security Management Systems.
- **TIA-942-C** – Telecommunications Infrastructure Standard for Data Centers.
- **ISO 22301:2019** – Business Continuity Management.
- **Internal Policy APJII** terkait pengelolaan SDM & pengembangan karier.

6. Definisi & Istilah

- **Readiness Test**: Ujian komprehensif tahunan yang mengukur kompetensi teknis, manajerial, serta soft skills SDM.
- **Promosi**: Kenaikan jabatan/posisi berdasarkan hasil readiness test, evaluasi kinerja, dan kebutuhan organisasi.
- **Demosi**: Penurunan jabatan/posisi karena hasil readiness test yang tidak memenuhi standar atau pelanggaran integritas.
- **Iklim Kerja Kondusif**: Lingkungan kerja yang mendukung produktivitas, kolaborasi, keterbukaan, dan kesejahteraan SDM.
- **Keberlangsungan Layanan**: Kemampuan organisasi menjaga operasional data center tetap berjalan tanpa gangguan.

7. Ruang Lingkup

1. **Readiness Test Tahunan**
    - Dilakukan minimal 1 kali setiap tahun.
    - Materi meliputi:
        - *Teknis*: Data center operation, keamanan informasi, disaster recovery, standar TIA-942, dsb.
        - *Manajerial*: Leadership, decision-making, problem solving, time management.
        - *Soft Skills*: Komunikasi, etika kerja, kolaborasi tim.
2. **Hasil Readiness Test Sebagai Parameter Promosi/Demosi**
    - Nilai ≥ 80: Berhak dipertimbangkan untuk promosi.
    - Nilai 60–79: Tetap pada posisi saat ini, wajib mengikuti coaching/mentoring.
    - Nilai < 60: Dipertimbangkan untuk demosi/rotasi sesuai kebutuhan organisasi.
3. **Menciptakan SDM Pemimpin yang Bertanggung Jawab terhadap Iklim Kerja Kondusif**
    - Pemimpin wajib menjaga komunikasi terbuka, keadilan dalam pembagian tugas, serta membangun suasana kerja kolaboratif.

- Pemimpin bertanggung jawab melakukan *employee engagement* dan penyelesaian konflik.

4. **Menciptakan SDM Pemimpin yang Menjaga Keberlangsungan Layanan**
   - Pemimpin wajib memahami dan menerapkan standar layanan data center (waktu aktif, keamanan, kontinuitas bisnis).
   - Pemimpin harus mampu membuat keputusan cepat dalam kondisi darurat untuk menjamin SLA (Service Level Agreement).
   - Pemimpin bertanggung jawab atas implementasi rencana BCP/DRP (Business Continuity Plan / Disaster Recovery Plan).

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

Lampiran SOP Kepemimpinan/Promosi SDM Data Center APJII

Lampiran 1 – Format Readiness Test Tahunan

Contoh Form Ujian Readiness Test SDM Data Center APJII

Keterangan:

- Penilaian menggunakan skala 0–100.
- Skor akhir dihitung dengan bobot.

No	Aspek Uji	Bobot (%)	Nilai Maks	Nilai Hasil	Skor Akhir
A. Kompetensi Teknis (40%)					
1	Penguasaan standar TIA-942 (Infra & Facility)	10	100		
2	Operasional PAC, UPS, Fire System, WLDS	10	100		
3	Cyber & Physical Security (ISO 27001)	10	100		
4	Business Continuity & DRP (ISO 22301)	10	100		
B. Kompetensi Manajerial (30%)					
5	Leadership & Decision Making	10	100		
6	Problem Solving & Crisis Handling	10	100		
7	Planning & Resource Management	10	100		
C. Soft Skills (20%)					
8	Komunikasi & Kolaborasi Tim	10	100		
9	Etika Kerja & Disiplin	10	100		
D. Pengembangan Diri (10%)					
10	Inovasi, Improvement, & Knowledge Sharing	10	100		
TOTAL	100%	1000		**____ / 100**	

Lampiran 2 – Form Penilaian Promosi/Demosi

Contoh Form Evaluasi Promosi/Demosi SDM Data Center APJII

Identitas Pegawai

- Nama: _____
- NIP: _____
- Jabatan Saat Ini: _____
- Unit Kerja: _____

Hasil Readiness Test Tahunan

- Nilai Akhir: _____ / 100
- Status: ☐ Lulus ☐ Tidak Lulus

Penilaian Aspek Tambahan

Aspek	Deskripsi	Skor (1–5)	Catatan Evaluator
Integritas & Etika	Konsistensi, kejujuran, disiplin		
Kepemimpinan	Mampu memimpin tim & mengambil keputusan		
Tanggung Jawab	Menjaga SLA, BCP/DRP, keamanan data center		
Kontribusi Organisasi	Inisiatif, inovasi, loyalitas		

Rekomendasi

- ☐ Dipromosikan ke Jabatan: _____
- ☐ Dipertahankan di Jabatan Saat Ini
- ☐ Demosi ke Jabatan: _____

Evaluator:

- Nama: _____
- Jabatan: _____
- Tanggal: _____

Tanda tangan: _____

Lampiran 3 – Matriks Skor & Kriteria Promosi/Demosi

Nilai Readiness Test	Keterangan	Tindak Lanjut
≥ 80	Kompeten Tinggi	Layak dipromosikan, masuk talent pool kepemimpinan
60 – 79	Kompeten Cukup	Tidak ada promosi, wajib coaching & re-test tahun depan
< 60	Kompetensi Kurang	Demosi/rotasi jabatan, wajib program pembinaan intensif

Lampiran 4 – Contoh Form Penilaian Iklim Kerja Kondusif (360° Feedback)

Survei Kepemimpinan (diisi oleh anggota tim & rekan kerja)

No	Pertanyaan	Skala 1–5 (Sangat Tidak Setuju – Sangat Setuju)
1	Pemimpin membangun komunikasi terbuka dengan tim.	
2	Pemimpin adil dalam pembagian tugas & tanggung jawab.	
3	Pemimpin mendorong kolaborasi & kerja sama tim.	
4	Pemimpin mampu menyelesaikan konflik secara profesional.	
5	Pemimpin memberi teladan disiplin & etika kerja.	

Catatan Tambahan Responden:

Lampiran 5 – Form Penilaian Keberlangsungan Layanan

Contoh Form Evaluasi Kepemimpinan terhadap SLA & BCP/DRP

Aspek	Indikator	Skor (1–5)	Catatan
SLA (Service Level Agreement)	Pemimpin memastikan waktu aktif DC & IIX sesuai target		
Manajemen Insiden	Respon cepat terhadap gangguan layanan		
BCP/DRP	Mampu menjalankan prosedur pemulihan bencana		

Aspek	Indikator	Skor (1–5)	Catatan
Keamanan	Menjamin physical & cyber security berjalan baik		
Audit Kepatuhan	Memastikan kepatuhan standar ISO & TIA		

Lampiran 6 – Contoh Form Rekap Tahunan Pengembangan SDM

Tahun	Nama Pegawai	Jabatan	Nilai Readiness Test	Status Promosi/Demosi	Catatan Coaching/Mentoring
2025					
2026					

Dengan adanya **Lampiran 1 – 6**, SOP ini bisa langsung digunakan dalam operasional DC APJII untuk:
✓ Menilai kompetensi SDM setiap tahun
✓ Menentukan promosi/demosi secara objektif
✓ Menilai iklim kerja & kepemimpinan
✓ Menjamin keberlangsungan layanan data center

LAMPIRAN XLIX
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP BUDAYA ORGANISASI SDM BIDANG DATA CENTER APJII

1. Pendahuluan

Sumber Daya Manusia (SDM) merupakan aset utama dalam pengelolaan dan operasional Data Center APJII. Budaya organisasi yang sehat, terarah, dan sesuai dengan visi-misi organisasi menjadi pondasi keberhasilan dalam menjaga standar layanan data center yang handal, aman, dan berkelanjutan. SOP ini disusun untuk memastikan seluruh SDM memahami, menerapkan, dan menjaga nilai budaya kerja dalam keseharian mereka di lingkungan Data Center APJII.

2. Latar Belakang

Perkembangan teknologi informasi dan komunikasi menuntut layanan data center dengan standar internasional yang tinggi. Kinerja dan profesionalisme SDM menjadi faktor kunci dalam mencapai keberhasilan tersebut.

Namun, keberhasilan tidak hanya ditentukan oleh kompetensi teknis, melainkan juga oleh nilai budaya organisasi yang mencakup cara berinteraksi, bekerja sama, dan menegakkan norma yang berlaku. Oleh karena itu, diperlukan SOP Budaya Organisasi SDM yang menjadi acuan dalam menilai, mengelola, dan meningkatkan perilaku serta interaksi antar SDM Data Center APJII.

3. Tujuan SOP

- Membentuk dan menjaga budaya organisasi yang positif, produktif, dan berorientasi pada pelayanan unggul.
- Menjadi panduan dalam menilai dan mengelola norma serta perilaku SDM.
- Mengatur cara bekerja dan berinteraksi SDM sesuai standar organisasi dan etika profesional.
- Menyediakan mekanisme pengukuran melalui survei karyawan secara berkala.
- Menjadi dasar perbaikan berkelanjutan dalam pengelolaan SDM Data Center APJII.

4. Obyektif SOP

- Meningkatkan kepuasan kerja karyawan.
- Membangun hubungan yang sehat antara atasan dan bawahan.

- Memperkuat hubungan kerja sama antar-SDM.
- Menjamin kejelasan peran, tanggung jawab, dan jobdesk masing-masing SDM.
- Mendukung terciptanya lingkungan kerja yang harmonis, inovatif, dan profesional.

5. Dasar & Referensi Standar

SOP ini disusun berdasarkan:

- **Undang-Undang Nomor 13 Tahun 2003** tentang Ketenagakerjaan.
- **Peraturan Menteri Ketenagakerjaan RI** terkait norma kerja, keselamatan, dan hubungan industrial.
- **ISO 9001:2015** – Quality Management System.
- **ISO 22301:2019** – Business Continuity Management System (BCMS).
- **TIA-942-C** – Data Center Standard (best practice dalam pengelolaan data center).
- **Best Practices Human Capital Management** dalam industri ICT dan data center.

6. Definisi & Istilah

- **Budaya Organisasi**: Nilai, norma, dan kebiasaan yang menjadi pedoman dalam bekerja dan berinteraksi di lingkungan Data Center APJII.
- **SDM (Sumber Daya Manusia)**: Seluruh karyawan, staf, dan manajemen yang terlibat dalam operasional Data Center APJII.
- **Jobdesk**: Rincian tugas dan tanggung jawab yang melekat pada setiap posisi pekerjaan.
- **Survei Karyawan**: Instrumen pengukuran yang digunakan untuk menilai kepuasan kerja, hubungan interpersonal, dan kejelasan peran SDM.
- **Norma Kerja**: Aturan dan etika yang wajib dipatuhi dalam aktivitas kerja.

7. Ruang Lingkup

SOP Budaya Organisasi SDM ini meliputi:

7.1 Budaya Organisasi

- Menetapkan nilai inti (integritas, profesionalisme, kolaborasi, inovasi, dan pelayanan).
- Menjaga lingkungan kerja yang inklusif, transparan, dan saling menghargai.
- Mendorong keterbukaan komunikasi dan akuntabilitas.

7.2 Menilai dan Mengelola Norma serta Perilaku SDM

- Penilaian rutin melalui mekanisme **Key Behavioral Indicators (KBI)**.
- Menerapkan sistem reward & recognition untuk perilaku positif.
- Memberikan pembinaan atau tindakan korektif bagi pelanggaran norma.

7.3 Mengatur serta Menilai Cara Bekerja dan Berinteraksi SDM

- Penerapan standar komunikasi internal (rapat, laporan, koordinasi lintas divisi).
- Menilai efektivitas kolaborasi tim melalui **performance review**.
- Mengatur kode etik profesional terkait kerahasiaan, keamanan, dan etika kerja.

7.4 Survei Karyawan

Dilakukan secara berkala minimal **2 kali dalam setahun**, dengan aspek pengukuran:

1. **Kepuasan Kerja**: Lingkungan kerja, kompensasi, kesempatan pengembangan diri.
2. **Hubungan dengan Atasan**: Kualitas kepemimpinan, keterbukaan komunikasi, dukungan karier.
3. **Hubungan antar SDM**: Kolaborasi, solidaritas, resolusi konflik.
4. **Kejelasan Peran/Jobdesk**: Pemahaman tugas, tanggung jawab, dan target kerja.
5. **Indeks Budaya Organisasi (IBO)**: Indikator umum untuk mengukur kesehatan budaya kerja.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

Lampiran SOP Budaya Organisasi SDM Data Center APJII

Lampiran 1: Contoh Form Survei Karyawan

Tujuan: Mengukur kepuasan kerja, hubungan kerja, dan kejelasan peran SDM.

No	Aspek Penilaian	Pertanyaan	Skala (1–5)	Catatan/Opini
1	Kepuasan Kerja	Saya merasa puas dengan lingkungan kerja di Data Center APJII	1 2 3 4 5	……
2	Kepuasan Kerja	Kompensasi dan fasilitas yang saya terima sudah sesuai	1 2 3 4 5	……
3	Pengembangan Diri	Saya memiliki kesempatan berkembang (pelatihan, promosi)	1 2 3 4 5	……
4	Hubungan dengan Atasan	Atasan saya memberikan arahan yang jelas dan dukungan	1 2 3 4 5	……
5	Hubungan dengan Atasan	Atasan saya terbuka untuk komunikasi dan diskusi	1 2 3 4 5	……
6	Hubungan Antar SDM	Rekan kerja saya saling membantu dan mendukung	1 2 3 4 5	……
7	Hubungan Antar SDM	Konflik antar rekan kerja dapat diselesaikan dengan baik	1 2 3 4 5	……
8	Kejelasan Peran/Jobdesk	Saya memahami tugas dan tanggung jawab saya dengan jelas	1 2 3 4 5	……
9	Kejelasan Peran/Jobdesk	Target kerja saya sesuai dengan kemampuan dan sumber daya	1 2 3 4 5	……
10	Indeks Budaya Organisasi	Saya merasa bangga menjadi bagian dari Data Center APJII	1 2 3 4 5	……

Keterangan Skala:
1 = Sangat Tidak Setuju, 2 = Tidak Setuju, 3 = Netral, 4 = Setuju, 5 = Sangat Setuju

Lampiran 2: Contoh Form Penilaian Perilaku SDM

Tujuan: Mengukur kesesuaian perilaku SDM terhadap norma dan budaya organisasi.

No	Perilaku yang Dinilai	Indikator	Skor (1–5)	Catatan Evaluator
1	Integritas	Menjaga kejujuran, etika kerja, dan kerahasiaan data	1 2 3 4 5	……
2	Profesionalisme	Menjalankan pekerjaan sesuai SOP dan standar teknis	1 2 3 4 5	……
3	Kolaborasi	Bersedia bekerja sama dan mendukung tim	1 2 3 4 5	……
4	Disiplin	Tepat waktu, patuh aturan kerja dan jadwal	1 2 3 4 5	……
5	Komunikasi	Menyampaikan ide dan informasi secara jelas & sopan	1 2 3 4 5	……
6	Inovasi	Memberikan ide baru atau solusi terhadap masalah	1 2 3 4 5	……
7	Tanggung Jawab	Menyelesaikan tugas sesuai target & standar	1 2 3 4 5	……
8	Kepedulian	Menunjukkan perhatian terhadap rekan kerja & fasilitas	1 2 3 4 5	……

Keterangan Skor:
1 = Sangat Buruk, 2 = Buruk, 3 = Cukup, 4 = Baik, 5 = Sangat Baik

Lampiran 3: Contoh Form Evaluasi Budaya Organisasi

Tujuan: Menilai kesehatan budaya organisasi secara keseluruhan.

No	Dimensi Budaya Organisasi	Pertanyaan Utama	Skor (1–5)	Catatan/Opini
1	Nilai Inti (Core Values)	Apakah nilai integritas, profesionalisme, kolaborasi, inovasi, dan pelayanan sudah diterapkan?	1 2 3 4 5	……
2	Kepemimpinan	Apakah kepemimpinan di unit Anda mencerminkan nilai organisasi?	1 2 3 4 5	……
3	Kolaborasi Tim	Apakah koordinasi antar tim berjalan efektif dan harmonis?	1 2 3 4 5	……
4	Lingkungan Kerja	Apakah lingkungan kerja mendukung produktivitas & kenyamanan?	1 2 3 4 5	……

No	Dimensi Budaya Organisasi	Pertanyaan Utama	Skor (1–5)	Catatan/Opini
5	Inovasi & Perbaikan	Apakah organisasi mendorong inovasi dan perbaikan berkelanjutan?	1 2 3 4 5	……
6	Kepuasan Karyawan	Apakah budaya organisasi meningkatkan kepuasan kerja?	1 2 3 4 5	……
7	Reputasi Organisasi	Apakah SDM bangga menjadi bagian dari Data Center APJII?	1 2 3 4 5	……

Keterangan Skor:
1 = Sangat Tidak Baik, 2 = Tidak Baik, 3 = Cukup, 4 = Baik, 5 = Sangat Baik

Catatan Implementasi

- Form di atas harus diisi secara **rahasia** untuk menjaga kejujuran responden.
- Survei karyawan dilakukan **2x dalam setahun** (semesteran).
- Hasil penilaian perilaku SDM dilakukan oleh **atasan langsung** setiap **3 bulan (triwulanan)**.
- Evaluasi budaya organisasi dilakukan oleh **HRD & Manajemen** setiap **1 tahun**.
- Semua hasil form dikompilasi untuk menjadi dasar **peningkatan budaya kerja dan SDM** di Data Center APJII.

LAMPIRAN L
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP KESEHATAN & KESELAMATAN KERJA SDM BIDANG DATA CENTER APJII

1. Pendahuluan

Kesehatan dan Keselamatan Kerja (K3) merupakan aspek penting dalam operasional Data Center, mengingat lingkungan kerja di data center memiliki risiko teknis yang cukup tinggi, seperti paparan listrik bertegangan tinggi, sistem pendingin, serta keterbatasan ruang kerja. Penerapan SOP K3 bagi SDM Data Center APJII bertujuan menciptakan lingkungan kerja yang aman, sehat, serta meningkatkan produktivitas dan keberlanjutan operasional.

2. Latar Belakang

Data Center APJII berfungsi sebagai pusat infrastruktur strategis yang mendukung layanan internet Indonesia. SDM yang bekerja di dalamnya terpapar potensi bahaya teknis maupun fisik yang dapat berdampak terhadap kesehatan, keselamatan, dan produktivitas kerja. Oleh karena itu, diperlukan standar operasional prosedur (SOP) untuk:

- Menjamin lingkungan kerja yang aman dan sehat.
- Meminimalisir potensi kecelakaan kerja.
- Memastikan kepatuhan terhadap standar nasional dan internasional terkait K3.
- Meningkatkan kesadaran dan pemahaman SDM terkait pentingnya K3.

3. Tujuan SOP

- Menetapkan pedoman penerapan K3 di lingkungan Data Center APJII.
- Melindungi SDM dari risiko kecelakaan kerja dan penyakit akibat kerja.
- Menjamin kepatuhan terhadap regulasi pemerintah dan standar internasional.
- Meningkatkan produktivitas SDM melalui penerapan K3 yang konsisten.

4. Obyektif SOP

- Menurunkan tingkat kecelakaan kerja hingga 0 (*zero accident*).
- Memastikan seluruh SDM memahami prosedur K3.
- Memastikan tingkat kehadiran SDM minimal **95% per bulan** sebagai indikator produktivitas.
- Melaksanakan evaluasi kepatuhan K3 secara berkala minimal **setiap 6 bulan sekali**.

- Menyediakan prosedur tanggap darurat jika terjadi kecelakaan kerja.

5. Dasar & Referensi Standar

- **UU No. 1 Tahun 1970** tentang Keselamatan Kerja dan **UU Ketenagakerjaan No.13 Tahun 2003**.
- **PP No. 50 Tahun 2012** tentang Penerapan SMK3.
- **Permenaker No. 5 Tahun 2018** tentang Keselamatan dan Kesehatan Kerja Lingkungan Kerja.
- **ISO 45001:2018** Occupational Health and Safety Management System.
- **ISO/IEC 27001:2022** (terkait keamanan informasi yang juga mencakup aspek K3 fisik).
- **TIA-942-C** (Data Center Standard – Facility & Safety).
- Kebijakan internal APJII terkait pengelolaan Data Center.

6. Definisi & Istilah

- **K3 (Kesehatan dan Keselamatan Kerja):** Upaya untuk menjamin keselamatan dan kesehatan tenaga kerja dengan pencegahan kecelakaan kerja dan penyakit akibat kerja.
- **SDM Data Center:** Seluruh personel yang bekerja tetap maupun kontrak di lingkungan Data Center APJII.
- ***Zero Accident*:** Kondisi dimana tidak terjadi kecelakaan kerja yang menimbulkan cedera.
- **P3K:** Pertolongan Pertama Pada Kecelakaan.
- **APD:** Alat pelindung diri, seperti sarung tangan anti-listrik, sepatu safety, helm, ear protection, dsb.
- ***Near Miss*:** Insiden yang berpotensi menyebabkan kecelakaan namun tidak menimbulkan kerugian.

7. Ruang Lingkup

7.1 Kesehatan dan Keselamatan Kerja (K3)

- Penggunaan APD (Alat Pelindung Diri) wajib saat bekerja di area berisiko tinggi.
- Pemeriksaan kesehatan SDM secara berkala minimal 1x/tahun.
- Penyediaan fasilitas P3K dan titik assembly point untuk evakuasi darurat.

7.2 Pemahaman K3 bagi SDM Data Center

- Seluruh SDM wajib mengikuti induksi K3 sebelum bekerja.
- Penyuluhan mengenai potensi bahaya (listrik, panas, pendinginan, bahan kimia, ruang terbatas).
- Penyampaian hak & kewajiban SDM terkait K3.

7.3 Pelatihan K3

- Pelatihan dasar K3 dilakukan minimal **1x per tahun**.
- Pelatihan pemadaman kebakaran & evakuasi darurat dilakukan minimal **2x per tahun**.
- Simulasi tanggap darurat (fire drill, electrical hazard response, chemical spill response).

7.4 Evaluasi Kepatuhan K3 Secara Berkala

- Audit internal K3 dilakukan **setiap 6 bulan**.
- Laporan hasil audit disampaikan kepada manajemen APJII.
- Tindak lanjut (corrective action) wajib dilakukan dalam **30 hari** setelah temuan.

7.5 Tingkat Kecelakaan Kerja

- Monitoring dilakukan dengan mencatat jumlah kecelakaan, insiden, dan *near miss*.
- Target tingkat kecelakaan kerja: **0 (zero) *fatal incidents*** per tahun.

7.6 Pencegahan Terjadinya Kecelakaan Kerja

- Identifikasi bahaya (hazard identification) dan penilaian risiko (risk assessment).
- Penyediaan rambu keselamatan, jalur evakuasi, dan tata letak kerja ergonomis.
- Pengecekan instalasi listrik, genset, UPS, dan pendingin secara berkala.

7.7 Prosedur Penanganan Kecelakaan Kerja

1. Segera hentikan aktivitas di area kejadian.
2. Laporkan insiden ke atasan langsung & tim K3.
3. Lakukan P3K bila diperlukan.
4. Evakuasi korban ke fasilitas kesehatan terdekat.
5. Dokumentasikan insiden (form laporan kecelakaan kerja).
6. Analisis penyebab dan lakukan tindakan pencegahan.

7.8 Tingkat Kehadiran SDM

- Absensi dicatat melalui sistem presensi resmi APJII.
- Tingkat kehadiran menjadi indikator produktivitas dengan target minimal **95% per bulan**.
- Ketidakhadiran karena sakit harus disertai surat dokter.

7.9 Sebagai Indikator Produktivitas SDM

- Kesehatan & keselamatan kerja berbanding lurus dengan produktivitas.
- Tingkat kehadiran, minimnya kecelakaan kerja, serta kepatuhan terhadap SOP K3 dijadikan KPI (Key Performance Indicator) untuk SDM Data Center.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

Lampiran SOP K3 SDM Data Center APJII

Lampiran 1 – Contoh Form Evaluasi Kepatuhan K3

Judul Form: Form Evaluasi Kepatuhan K3
Periode Evaluasi: ☐ Bulanan ☐ Triwulan ☐ Semester

No	Aspek Evaluasi	Ya	Tidak	Catatan/Temuan
1	SDM menggunakan APD sesuai ketentuan (helm, sarung tangan, sepatu safety, dsb.)	☐	☐	
2	Jalur evakuasi bebas hambatan	☐	☐	
3	Alat pemadam api (APAR/Fire Suppression) tersedia dan berfungsi	☐	☐	
4	SDM mengikuti briefing K3 sebelum kerja	☐	☐	
5	P3K tersedia dan terisi lengkap	☐	☐	
6	Laporan *near miss* dibuat jika ada kejadian	☐	☐	
7	SDM mengikuti pelatihan/simulasi K3 sesuai jadwal	☐	☐	
8	Area kerja bebas dari kabel atau peralatan yang berpotensi menimbulkan bahaya	☐	☐	

Evaluator: ……
Tanggal: ……
Tanda Tangan: ……

Lampiran 2 – Contoh Form Laporan Kecelakaan Kerja
Judul Form: Form Laporan Kecelakaan Kerja

Bagian	Keterangan
Nama Korban	
Jabatan	
Tanggal & Waktu Kejadian	

Bagian	Keterangan
Lokasi Kejadian	
Jenis Kecelakaan (listrik, mekanik, terjatuh, lainnya)	
Kronologi Kejadian	
Saksi Mata	
Tindakan P3K yang Diberikan	
Rumah Sakit/Fasilitas Kesehatan Rujukan	
Tingkat Cedera (Ringan/Sedang/Berat/Fatal)	
Analisa Penyebab	
Rekomendasi Pencegahan	

Dilaporkan oleh: ……
Diterima oleh (Tim K3): ……
Tanggal: ……

Lampiran 3 – Contoh Form Checklist APD (Alat Pelindung Diri)
Judul Form: Form Checklist Penggunaan APD

No	Nama SDM	Tanggal	Helm	Sarung Tangan	Sepatu Safety	Ear Protection	Rompi	Status (Lengkap/Tidak)	Catatan
1			☐	☐	☐	☐	☐		
2			☐	☐	☐	☐	☐		

Petugas K3: ……
Tanggal: ……

Lampiran 4 – Contoh Form Absensi Kehadiran SDM
Judul Form: Form Absensi Kehadiran SDM Data Center

No	Nama SDM	Jabatan	Tanggal	Hadir	Izin	Sakit	Cuti	Catatan
1				☐	☐	☐	☐	
2				☐	☐	☐	☐	

Keterangan:
- Target kehadiran minimal **95% per bulan**.
- Surat dokter wajib untuk ketidakhadiran karena sakit.

Lampiran 5 – Contoh Form Laporan *Near Miss*
Judul Form: Form Laporan *Near Miss* (Kejadian Nyaris Celaka)

Bagian	Keterangan
Pelapor	
Jabatan	
Tanggal & Waktu	
Lokasi	
Jenis Potensi Bahaya	
Kronologi Singkat	
Dampak yang Mungkin Terjadi	
Tindakan Pencegahan yang Diambil	
Rekomendasi	

Pelapor: ……
Disetujui (Tim K3): ……

Lampiran 6 – Contoh Form Checklist Audit Internal K3
Judul Form: Form Audit Internal K3

No	Aspek Audit	Sesuai	Tidak Sesuai	Catatan
1	APD digunakan sesuai ketentuan	☐	☐	
2	Alat P3K tersedia & lengkap	☐	☐	
3	Jalur evakuasi jelas & aman	☐	☐	
4	Alarm kebakaran berfungsi	☐	☐	
5	Sistem pendingin aman & tidak bocor	☐	☐	
6	Instalasi listrik sesuai standar	☐	☐	
7	Dokumentasi kecelakaan & *near miss* lengkap	☐	☐	

Auditor: ……
Tanggal Audit: ……

Lampiran 7 – Contoh Form Checklist Briefing K3 Harian
Judul Form: Form Briefing K3 Harian

No	Tanggal	Nama SDM	Topik K3 Dibahas	Tanda Tangan SDM	Catatan
1					

Petugas K3/PIC Shift: ……

LAMPIRAN LI
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PRODUKTIVITAS KERJA SDM BIDANG DATA CENTER APJII

1. Pendahuluan

Sumber Daya Manusia (SDM) merupakan aset utama dalam operasional data center APJII (Asosiasi Penyelenggara Jasa Internet Indonesia). Produktivitas kerja SDM sangat menentukan kualitas layanan, keberlangsungan operasional, dan daya saing data center. Untuk itu, diperlukan Standar Operasional Prosedur (SOP) yang mengatur pengelolaan, pemantauan, dan evaluasi produktivitas SDM secara sistematis, objektif, dan berkelanjutan.

2. Latar Belakang

Dalam lingkungan data center, keandalan layanan dan kepuasan pelanggan sangat dipengaruhi oleh kinerja SDM. Produktivitas kerja yang tinggi berhubungan langsung dengan efisiensi operasional, kualitas layanan, dan optimalisasi biaya. Namun, tanpa adanya ukuran dan indikator yang jelas, produktivitas sulit untuk dinilai secara objektif.
Oleh karena itu, SOP ini dibuat sebagai pedoman pengukuran dan peningkatan produktivitas kerja SDM Data Center APJII, dengan memperhatikan aspek revenue per karyawan, KPI individu maupun tim, serta indikator penggunaan lembur.

3. Tujuan SOP

SOP ini bertujuan untuk:

1. Menetapkan standar pengukuran produktivitas SDM di data center APJII.
2. Menjamin konsistensi dalam evaluasi produktivitas kerja.
3. Mengoptimalkan peran SDM agar selaras dengan target organisasi.
4. Meningkatkan efisiensi penggunaan sumber daya melalui pengendalian lembur.
5. Memberikan dasar objektif untuk penilaian kinerja, remunerasi, dan pengembangan SDM.

4. Obyektif SOP

- Menjadi acuan resmi bagi manajemen dalam melakukan pengukuran dan pemantauan produktivitas SDM.
- Memberikan mekanisme evaluasi berbasis KPI yang terukur dan dapat dibandingkan.
- Menyediakan indikator untuk menentukan kebutuhan pengembangan kompetensi SDM.
- Mengaitkan produktivitas kerja dengan sistem remunerasi, insentif, dan kebijakan lembur.

5. Dasar & Referensi Standar

SOP ini disusun dengan mengacu pada standar berikut:

1. **ISO 9001:2015** – Quality Management System.
2. **ISO/IEC 20000-1:2018** – IT Service Management.
3. **ISO/IEC 27001:2022** – Information Security Management System.
4. **ISO 22301:2019** – Business Continuity Management System.
5. **TIA-942-C** – Telecommunications Infrastructure Standard for Data Centers.
6. **Peraturan Ketenagakerjaan RI** terkait jam kerja, lembur, dan remunerasi.
7. **Kebijakan Internal APJII** terkait pengelolaan SDM dan operasional data center.

6. Definisi & Istilah

- **Produktivitas SDM**: Perbandingan antara output (hasil kerja, revenue, layanan) dengan input (waktu, tenaga, biaya) yang digunakan.
- **KPI (Key Performance Indicator)**: Indikator kinerja utama yang digunakan untuk mengukur efektivitas individu maupun tim dalam mencapai target.
- **Lembur (Overtime)**: Jam kerja tambahan di luar jam kerja normal sesuai ketentuan hukum.
- **Insiden Darurat**: kejadian yang tidak terduga dan tidak normal yang dapat menimbulkan ancaman langsung terhadap jiwa, kesehatan, properti, atau lingkungan, sehingga memerlukan tindakan penanggulangan segera untuk meminimalkan dampak buruk. Meliputi bencana alam, kebakaran, kecelakaan, tumpahan bahan kimia, hingga ancaman keamanan.

7. Ruang Lingkup: Produktivitas

a. Key Performance Indicator (KPI) / Produktivitas SDM

1. KPI ditentukan berdasarkan fungsi kerja SDM di data center, meliputi:
    - **Operasional**: Tingkat ketersediaan layanan, response time terhadap insiden.
    - **Teknis**: Keberhasilan pemeliharaan sistem tanpa downtime, kepatuhan SOP.
    - **Administrasi**: Ketepatan laporan, kelengkapan dokumentasi.
    - **Keamanan**: Kepatuhan terhadap standar keamanan fisik dan informasi.
2. Skoring KPI menggunakan metode kuantitatif (angka capaian) dan kualitatif (evaluasi supervisor).
3. KPI di-review per bulan, dengan evaluasi penuh per kuartal.
4. Pencapaian KPI menjadi dasar untuk penilaian kinerja tahunan.
5. KPI harus sesuai dengan sasaran mutu (ISO-90001 dan ISO-27001) dan menuju tujuan misi dan visi Perusahaan.
6. KPI mencakup penilaian:
    - Absensi karyawan
    - Target pekerjaan yang dilakukan
    - Inisiatif yang dilakukan untuk efisiensi pekerjaan
    - Tingkat kepatuhan
    - Attitude dan Kerjasama Tim (Team work)

b. Penggunaan Lembur

1. Lembur hanya dilakukan untuk:
    - Aktivitas maintenance terjadwal yang tidak bisa dilakukan pada jam kerja normal.
    - Insiden darurat (emergency response).
2. Setiap jadwal lembur akan diatur oleh masing-masing Supervisor hanya untuk tim operasional, dan Supervisor bertanggung jawab atas pelaksanaan tim yang akan melakukan lembur.
3. Surat Perintah Lembur (SPL) dibuat oleh Supervisor, disetujui oleh Manager dan diketahui oleh Kepala Bidang terkait.

c. Lembur sebagai Indikator Produktivitas SDM

1. Efisiensi dan efektifitas dalam menyelesaikan pekerjaan.
2. Analisa Insiden darurat.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

Lampiran SOP Produktivitas Kerja SDM Bidang Data Center APJII

Lampiran 1. Contoh Formulir Perintah Lembur (FPL)

Formulir Perintah Lembur (FPL)	**Nomor Dokumen: ……**	**Tanggal: ……**

Data Karyawan

- Nama Karyawan : .....
- Jabatan : .....
- Departemen/Tim : .....

Rincian Lembur

Tanggal Lembur	Jam Mulai	Jam Selesai	Jumlah Jam	Deskripsi Pekerjaan	Alasan Lembur	Persetujuan Atasan

Tanda Tangan

- Supervisor : _____
- Manager : _____
- Kabid : _____

Lampiran 2. Contoh Form Penilaian KPI Individu

Form Penilaian KPI Individu | Periode: Bulanan/Kuartal/Tahunan | Nomor Dokumen: ……

Identitas Karyawan

- Nama : .....
- Jabatan : .....
- Unit Kerja : .....

Matriks KPI

No	KPI Utama	Bobot (%)	Target	Realisasi	Nilai (Target x Bobot)	Catatan Evaluator
1	Operasional (Availability, Response Time)	30%	99.9% Waktu Ketersediaan	…	…	…
2	Teknis (Pemeliharaan, SOP Compliance)	25%	100% pemenuhan jadwal	…	…	…

No	KPI Utama	Bobot (%)	Target	Realisasi	Nilai (Target x Bobot)	Catatan Evaluator
3	Administrasi (Laporan, Dokumentasi)	15%	100% tepat waktu	…	…	…
4	Keamanan (Physical & ISMS Compliance)	20%	100% kepatuhan	…	…	…
5	Inovasi / Improvement	10%	≥ 1 improvement	…	…	…

Total Skor KPI: …… (Skala 0–100)
Kesimpulan Penilaian:
☐ Sangat Baik ☐ Baik ☐ Cukup ☐ Kurang
Tanda Tangan

- Evaluator : _____
- Karyawan : _____

LAMPIRAN LII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP KOMPETENSI, KETERAMPILAN & KAPABILITAS SDM BIDANG DATA CENTER APJII

1. Pendahuluan

Pengelolaan data center membutuhkan sumber daya manusia (SDM) dengan kompetensi, keterampilan, dan kapabilitas yang tinggi agar operasional berjalan sesuai standar internasional. SOP ini menjadi acuan bagi APJII dalam memastikan SDM memiliki kemampuan teknis, manajerial, dan profesional sesuai dengan standar data center modern.

2. Latar Belakang

Dalam perkembangan infrastruktur digital Indonesia, peran data center APJII sangat penting untuk menjamin ketersediaan, keandalan, keamanan, dan kontinuitas layanan internet nasional. Oleh karena itu, SDM yang mengelola data center wajib memiliki kompetensi teknis dan non-teknis yang terukur, terstandar, serta diakui secara internasional melalui pelatihan dan sertifikasi.

3. Tujuan SOP

- Menetapkan standar kompetensi, keterampilan, dan kapabilitas SDM data center APJII.
- Menjamin kualitas operasional, keamanan, dan keberlangsungan layanan data center.
- Memberikan panduan pelatihan, evaluasi, dan sertifikasi SDM secara berkesinambungan.
- Mendukung tercapainya sertifikasi dan standar internasional (misalnya TIA-942, ISO 27001, ISO 22301, ISO 20000).

4. Obyektif SOP

- Menyediakan mekanisme identifikasi kebutuhan kompetensi SDM.
- Menetapkan program pengembangan melalui pelatihan dan sertifikasi.
- Melaksanakan evaluasi kompetensi secara periodik.
- Mengurangi risiko operasional akibat human error dengan peningkatan keterampilan.
- Mendorong budaya kerja profesional, aman, dan sesuai operasional data center.

5. Dasar & Referensi Standar

1. **TIA-942-C** – Telecommunications Infrastructure Standard for Data Centers.

2. **ISO/IEC 27001** – Information Security Management System (ISMS).
3. **ISO/IEC 22301** – Business Continuity Management System (BCMS).
4. **ISO/IEC 20000-1** – IT Service Management (ITSM).
5. **ASHRAE TC 9.9** – Thermal Guidelines for Data Centers.
6. **BNSP (Badan Nasional Sertifikasi Profesi)** – Skema kompetensi bidang TIK & Data Center.
7. **EPI Data Center Training & Certification** – CDCP, CDCS, CDFOS, CDFOM , CTDC, CTIA, CDFOM.

6. Definisi & Istilah

- **Kompetensi**: Kemampuan yang mencakup pengetahuan, keterampilan, dan sikap kerja yang ditunjukkan oleh SDM.
- **Keterampilan (Skill)**: Kemampuan teknis yang dapat diaplikasikan dalam tugas operasional data center.
- **Kapabilitas**: Kapasitas individu/organisasi untuk melakukan fungsi tertentu dengan konsisten.
- **Pelatihan**: Proses peningkatan pengetahuan dan keterampilan SDM melalui metode belajar formal maupun non-formal.
- **Sertifikasi**: Pengakuan resmi atas kompetensi SDM oleh lembaga berwenang.
- **Evaluasi Kompetensi**: Proses pengukuran kemampuan SDM melalui tes, observasi, atau penilaian kinerja.

7. Ruang Lingkup

7.1 Kompetensi, Keterampilan, dan Kapabilitas

SDM Data Center APJII wajib memiliki kompetensi dalam:

- **Teknis**: Infrastruktur data center (power, cooling, rack, cabling, fire suppression, monitoring).
- **Operasional**: Manajemen insiden, change management, patching, troubleshooting, reporting.
- **Keamanan**: Cybersecurity, akses fisik, keamanan jaringan, prosedur ISO 27001.
- **Kontinuitas Layanan**: DRP (Disaster Recovery Plan), BCP (Business Continuity Plan), simulasi recovery.
- **Manajerial**: Teamwork, komunikasi efektif, kepatuhan regulasi, pengelolaan vendor.

7.2 Pelatihan SDM

- **Induksi**: Orientasi SDM baru terkait SOP, standar keselamatan, dan pengenalan fasilitas.
- **Teknis Rutin**: Training sistem power, cooling, monitoring tools, network, dan cybersecurity.
- **Soft Skill**: Leadership, komunikasi, problem solving.
- **Advanced Training**: Persiapan sertifikasi internasional (CDCP, CDCS, ISO Lead Implementer, dll).

7.3 Evaluasi Kompetensi Berkala

- **Frekuensi**: Dilakukan setiap 6 bulan dan tahunan.

- **Metode**: Tes tertulis, simulasi operasional, on-the-job evaluation, penilaian kinerja.
- **Kriteria Lulus**: Minimum 80% penguasaan materi dan keterampilan praktis.
- **Tindak Lanjut**: SDM yang belum memenuhi kriteria wajib mengikuti re-training.

7.4 Sertifikasi

- **Internal**: Sertifikasi kompetensi dari APJII berdasarkan standar operasional internal.
- **Eksternal**: Sertifikasi dari lembaga resmi (EPI, ISO, BNSP, Cisco, VMware, Microsoft).
- **Program Wajib**:
    - Minimal **CDCP/CDFOS** untuk level operator.
    - **CDCS/CDFOM** untuk level supervisor/manager.
    - **ISO/IEC 27001 Lead Implementer** untuk keamanan informasi.
    - **ISO/IEC 22301** untuk manajemen kontinuitas bisnis.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

Contoh Matriks Kompetensi SDM Data Center APJII

Jabatan/Posisi	Kompetensi Inti	Pelatihan Wajib	Sertifikasi yang Harus Dimiliki
• **Tim Teknis IIX** • **Tim Teknis Data Center** • **Tim NOC IIX dan Data Center**	○ Dasar infrastruktur data center (power, cooling, rack, cabling) ○ Monitoring & reporting ○ SOP operasional harian ○ Penanganan insiden dasar	○ Induksi Data Center ○ Safety & Fire Safety Training ○ Basic Networking & Server ○ Monitoring Tools Training ○ ISO 27001 Awareness	○ **CDCP** (Certified Data Center Professional, EPI) ○ Fire Safety Certification
	○ Troubleshooting jaringan & sistem ○ Konfigurasi perangkat (server, storage, switch, firewall) ○ Pengelolaan power & cooling system ○ Implementasi patch & change management	○ Advanced Networking (Cisco/Juniper) ○ Virtualization (VMware/Hyper-V) ○ Data Center Facility Training (power, cooling, fire suppression) ○ Cybersecurity Basics	○ **CDCP** (Certified Data Center Professional, EPI) ○ Cisco CCNA/CCNP ○ VMware VCP / Microsoft Certified
• **Supervisor IIX** • **Supervisor Data Center**	○ Manajemen tim operasional ○ Change & incident management ○ SLA & reporting ○ Audit internal & compliance ○ Business Continuity Planning (BCP)	○ Leadership & Communication ○ IT Service Management (ISO 20000 Awareness) ○ ISO 22301 Awareness (BCMS) ○ Incident & Problem Management	○ **CDCS / CDFOM** (Certified Data Center Facilities Operations Manager, EPI) ○ ISO/IEC 20000 Foundation ○ ISO 22301 Foundation
• **Manager IIX dan Data Center**	○ Perencanaan strategis operasional data center ○ Risk Management ○ Budgeting & vendor management ○ Kepatuhan regulasi (Kominfo dan ISO)	○ Advanced Data Center Management ○ Risk & Compliance Training ○ ISO 27001 ISMS Lead Implementer ○ Crisis & Disaster Recovery Simulation	○ **CDFOM, EPI** ○ ISO/IEC 27001 Lead Implementer ○ ISO/IEC 22301 Lead Implementer ○ ITIL Foundation / ISO 20000 Lead Implementer

Jabatan/Posisi	Kompetensi Inti	Pelatihan Wajib	Sertifikasi yang Harus Dimiliki
	○ Business Continuity & Disaster Recovery		
	○ Strategic planning & governance ○ Kapabilitas manajerial tinggi ○ Audit & compliance ○ Roadmap pengembangan data center ○ Hubungan dengan regulator & stakeholder	○ Executive Leadership ○ Risk Governance ○ Data Center Strategy Training ○ Cybersecurity Management	○ **CTDC/CTIA** (Certified TIA-942 Design Consultant/Auditor) ○ ISO/IEC 27001 Lead Auditor ○ ISO/IEC 22301 Lead Auditor ○ ITIL Expert

📌 **Catatan Penting Implementasi di APJII**:

1. **Tim Teknis/NOC** minimal wajib memiliki **CDCP**.
2. **Supervisor** (Leader) diarahkan ke **CDCS/CDFOS/CDFOM**.
3. **Manager Divisi** ditargetkan **CDFOM + ISO 27001/22301 Lead Implementer &** difokuskan pada sertifikasi desain & audit (CTDC/CTIA) untuk mendukung compliance dan standar internasional.
4. Evaluasi kompetensi dilakukan **setiap 6 bulan** dengan review sertifikasi, pelatihan tambahan, serta simulasi operasional (misalnya disaster recovery drill).

Contoh Form Evaluasi Kompetensi SDM Data Center APJII

📌 Petunjuk Penggunaan:

- Checklist ini digunakan oleh HR/atasan langsung untuk menilai kompetensi SDM sesuai jabatan.
- Skor penilaian:
  - **1 = Tidak Memenuhi**
  - **2 = Perlu Perbaikan**
  - **3 = Cukup**
  - **4 = Baik**
  - **5 = Sangat Baik**
- Evaluasi dilakukan minimal **6 bulan sekali**.
- Hasil dievaluasi dan ditindaklanjuti dengan pelatihan/retraining bila skor < 3.

A. Tim Teknis IIX, Tim Teknis Data Center dan Tim NOC IIX dan Data Center

Kompetensi	Indikator	Skor (1-5)	Catatan
Pengetahuan dasar infrastruktur DC	Paham power, cooling, rack, cabling		
Monitoring & reporting	Mampu menggunakan tools monitoring		
Penanganan insiden dasar	Dapat mengikuti SOP insiden ringan		
Keamanan fisik & akses	Menjalankan prosedur akses dengan benar		
Troubleshooting	Menangani masalah jaringan/sistem/fasilitas		
Konfigurasi perangkat	Dapat mengkonfigurasi server, switch, firewall		
Change Management	Mengikuti prosedur perubahan system		
Dokumentasi teknis	Membuat laporan teknis lengkap		
Sertifikasi (CDCP/CDCS/ CCNA/VMware/BNSP)	Sertifikat aktif dan berlaku		

B. Supervisor IIX dan Supervisor Daa Center

Kompetensi	Indikator	Skor (1-5)	Catatan
Manajemen tim	Mengatur shift & tugas dengan efektif		
Incident & problem management	Menangani insiden tingkat menengah		
SLA & reporting	Menyusun laporan sesuai standar SLA		
Audit internal & compliance	Melakukan review operasional sesuai SOP		
Sertifikasi wajib (CDFOS/CDFOM, ISO Awareness)	Sertifikat aktif dan berlaku		

C. Manager IIX dan Data Center

Kompetensi	Indikator	Skor (1-5)	Catatan
Perencanaan strategis	Menyusun roadmap operasional DC		
Risk management	Menerapkan mitigasi risiko operasional		
Vendor management	Mengelola kontrak & performa vendor		
Business Continuity	Menyusun & melaksanakan BCP/DRP		
Strategic leadership	Mengarahkan strategi DC jangka panjang		
Governance & compliance	Memastikan DC sesuai standar (TIA, ISO)		
Audit & regulasi	Mampu menghadapi audit eksternal		
Stakeholder management	Berkoordinasi dengan regulator & mitra		
Sertifikasi wajib (CDFOM/CTDC/CTIA, ISO 27001/22301 Lead Implementer)	Sertifikat aktif dan berlaku		

LAMPIRAN LIII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP KETERSEDIAAN TENAGA KERJA SDM BIDANG DATA CENTER APJII

1. Pendahuluan

Ketersediaan tenaga kerja yang memadai dan terstruktur merupakan faktor kritis dalam menjamin keberlangsungan operasional data center APJII. Sistem operasional data center yang berjalan 24x7x365 membutuhkan SDM dengan kualifikasi dan jumlah yang tepat untuk menghindari potensi gangguan layanan akibat kekosongan personel. SOP ini disusun untuk menjadi acuan resmi dalam pengelolaan, perencanaan, dan pengaturan tenaga kerja, khususnya terkait jadwal kerja, shifting, serta pengaturan cuti/libur.

2. Latar Belakang

Data center APJII merupakan infrastruktur vital yang mendukung ekosistem internet nasional. Kegagalan dalam menjaga ketersediaan layanan dapat berdampak signifikan terhadap operasional anggota APJII dan masyarakat luas. Salah satu faktor utama yang mempengaruhi keberlangsungan layanan adalah **ketersediaan SDM yang kompeten dan selalu siaga**.

Untuk itu diperlukan mekanisme formal berupa SOP guna memastikan tenaga kerja tersedia sesuai kebutuhan operasional, dengan pengaturan shifting dan libur yang adil, proporsional, serta sejalan dengan standar operasional data center internasional.

3. Tujuan SOP

1. Menjamin ketersediaan tenaga kerja SDM yang cukup dan kompeten dalam mendukung operasional data center APJII.
2. Menghindari risiko terjadinya kekosongan SDM yang dapat mengganggu keberlangsungan layanan data center.
3. Mengatur pola shifting dan libur SDM agar seimbang antara kebutuhan operasional dan kesejahteraan personel.
4. Menyediakan pedoman bagi manajemen dalam merencanakan jadwal kerja, penggantian personel, dan rotasi tim.

4. Obyektif SOP

- Menyusun sistem kerja SDM berbasis shift 24x7 yang konsisten dan terdokumentasi.

- Menetapkan rasio ideal jumlah tenaga kerja dalam satu shift.
- Menjamin ada personel cadangan (standby/backup) untuk mengantisipasi ketidakhadiran mendadak.
- Memberikan transparansi dalam pengaturan jadwal libur, cuti, serta lembur.
- Menjamin tingkat layanan (service level) data center tetap terjaga meskipun terdapat absensi personel.

5. Dasar & Referensi Standar

1. **TIA-942-C** – Telecommunications Infrastructure Standard for Data Centers.
2. **ISO/IEC 27001:2022** – Information Security Management System (ISMS).
3. **ISO 22301:2019** – Business Continuity Management System (BCMS).
4. **ISO 20000-1:2018** – IT Service Management.
5. Peraturan Ketenagakerjaan Republik Indonesia (UU No. 13 Tahun 2003 dan perubahannya, UU Cipta Kerja No. 11 Tahun 2020).
6. Kebijakan internal APJII tentang Manajemen SDM dan Operasional Data Center.

6. Definisi & Istilah

- **Shift**: Pembagian waktu kerja personel dalam periode tertentu (pagi, sore, malam).
- **On-duty**: Status ketika personel bertugas sesuai jadwal shift.
- **Standby/On-call**: Status personel cadangan yang siap dipanggil saat terjadi kekurangan tenaga kerja.
- **Libur**: Hari istirahat terjadwal sesuai dengan ketentuan perusahaan.
- **Rasio Shift**: Perbandingan jumlah personel yang bertugas dalam satu shift terhadap kebutuhan operasional.
- **Critical Operation Role**: Posisi/pekerjaan yang wajib selalu terisi di data center (misalnya: Tim NOC/Teknis, Security, PIC/Penanggung Jawab Operasional DC APJII).

7. Ruang Lingkup:

Ketersediaan Tenaga Kerja

SOP ini berlaku untuk seluruh tenaga kerja SDM yang terlibat dalam operasional data center APJII, mencakup fungsi operasional, teknis, dan pendukung.

a. Memastikan layanan tetap berjalan dan menghindari risiko kekosongan SDM

1. **Kebutuhan minimum personel per shift** ditetapkan berdasarkan analisis beban kerja dan *best-practice* operasional:
    - Operator Tim NOC/Teknis: minimal 2 orang/shift.
    - Tim Teknis/NOC (Power & Cooling): minimal 1 orang/shift.
    - Security: minimal 2 orang/shift.
    - Supervisor Tim Teknis/NOC on-call: 1 orang tersedia setiap saat (tidak harus onsite, dapat remote/on-call).
2. **Backup Personel**
    - Setiap shift wajib memiliki 1 orang standby yang dapat dipanggil dalam waktu maksimal 2 jam bila terjadi absensi mendadak.
    - Standby schedule diatur bergilir.

3. **Rencana Kontinjensi SDM**
    - Jika terdapat kekosongan mendadak (sakit, izin darurat), maka supervisor Tim NOC/Teknis wajib segera mengaktifkan personel standby.
    - Jika kekosongan lebih dari 24 jam, manajemen HR wajib melakukan redistribusi personel antar-shift.

b. Pengaturan Rasio Jadwal Shifting dan Libur

1. **Pola Shift 24x7x365**
    - 3 shift kerja:
        - Shift 1: 06.30 – 15.30
        - Shift 2: 14.30 – 23.30
        - Shift 3: 22.30 – 07.30
2. **Rasio Personel dalam Shift**
    - Minimal 1 Supervisor (on-call).
    - Minimal 5 personel onsite (2 NOC, 1 Teknis, 2 Security).
    - Perbandingan ideal: 5 personel onsite: 1 personel standby.
3. **Jadwal Libur dan Cuti**
    - Libur wajib diberikan 1 hari setelah 6 hari kerja (6-1 pattern).
    - Pergeseran jadwal libur dilakukan secara bergilir agar adil bagi seluruh personel.
    - Cuti tahunan mengikuti ketentuan ketenagakerjaan nasional (minimal 12 hari/tahun).
4. **Pengaturan Lembur**
    - Lembur hanya diperbolehkan jika terdapat kebutuhan darurat.
    - Setiap lembur harus disetujui oleh Supervisor (Leader) / PIC / Penanggung Jawab Operasional DC & IIX APJII.
5. **Monitoring & Evaluasi Jadwal**
    - Jadwal shift bulanan wajib disusun oleh Supervisor (Leader) Data Center atau Supervisor (Leader) IIX dan disetujui oleh PIC / Penanggung Jawab Operasional DC & IIX APJII.
    - Evaluasi kepatuhan jadwal dilakukan setiap triwulan.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

Lampiran SOP Ketersediaan Tenaga Kerja SDM Data Center APJII

1. Contoh Jadwal Shift Harian

Format:

- Shift 1: 06.30 – 15.30
- Shift 2: 14.30 – 23.30
- Shift 3: 22.30 – 07.30

Posisi	Shift 1 (06.30–15.30)	Shift 2 (14.30–23.30)	Shift 3 (22.30–07.30)	Standby (On-Call)
Tim NOC	Fahrur, Dea	Dhipo	Irsyad	Ary
Tim Teknis	Tomi	Reza	Romi	Sahli
Security	??	??	??	??
Supervisor	Supervisor (On-Call)	Supervisor (On-Call)	Supervisor (On-Call)	Supervisor (On-Call)

2. Contoh Jadwal Shift Mingguan

(1 minggu = 7 hari kerja; libur dirotasi agar adil)

Hari	Shift 1 (06.30–15.30)	Shift 2 (14.30–23.30)	Shift 3 (22.30–07.30)	Standby
Senin	Fahrur, Dea, Tomi	Dhipo, Reza	Irsyad, Romi	Ary, Sahli
Selasa	Fahrur, Dea, Tomi	Reza, Sahli	Irsyad, Ary	Romi
Rabu	Dea, Tomi, Sahli	Ary, Reza	Irsyad, Romi	Fahrur
Kamis	Dea, Tomi, Ary	Fahrur, Sahli	Ary, Fahrur	Reza

Hari	Shift 1 (06.30–15.30)	Shift 2 (14.30–23.30)	Shift 3 (22.30–07.30)	Standby
Jumat	Ary, Romi	Dea, Reza	Sahli, Ary	Tomi
Sabtu	Reza, Ary	Romi, Sahli	Reza, Fahrur	Dea
Minggu	Rotasi Tim (Cuti bergilir sesuai jadwal)	Rotasi Tim	Rotasi Tim	Supervisor On-Call

3. Contoh Jadwal Shift Bulanan

Format rotasi bulanan (contoh 1 bulan, tim dirotasi agar semua personel kebagian shift malam/pagi/sore secara seimbang).

Minggu Ke-	Shift 1 (06.30–15.30)	Shift 2 (14.30–23.030)	Shift 3 (22.30–07.30)	Catatan Libur
Minggu 1	Tim A	Tim B	Tim C	Tim D libur
Minggu 2	Tim B	Tim C	Tim D	Tim A libur
Minggu 3	Tim C	Tim D	Tim A	Tim B libur
Minggu 4	Tim D	Tim A	Tim B	Tim C libur

Keterangan Tim:

- **Tim A:** …
- **Tim B:** …
- **Tim C:** …
- **Tim D:** …

4. Contoh Jadwal Shift Cuti & Libur Tahunan

- Setiap SDM berhak atas **12 hari cuti tahunan**.
- Cuti diatur agar tidak bersamaan lebih dari 1 orang per shift **(kecuali keadaan khusus/izin darurat)**.

Bulan	Personel Cuti	Pengganti (Shift Ditukar)
Januari	…	…
Februari	…	…
Maret	…	…
April	…	…
Mei	…	…
Juni	…	…
Juli	…	…
Agustus	…	…
September	…	…
Oktober	…	…
November	…	….
Desember	…	…

5. Contoh Jadwal Standby / On-Call

Untuk memastikan tidak ada kekosongan personel mendadak:

Hari	Personel Standby	Kontak Darurat
Senin	…	0812-xxx-xxx
Selasa	…	0813-xxx-xxx

Hari	Personel Standby	Kontak Darurat
Rabu	…	0814-xxx-xxx
Kamis	…	0812-xxx-xxx
Jumat	…	0813-xxx-xxx
Sabtu	…	0814-xxx-xxx
Minggu	…	0812-xxx-xxx

LAMPIRAN LIV
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

JOB DESCRIPTION MANAGER IIX DAN DATA CENTER APJII

1. Pendahuluan

Penanggung Jawab Operasional Data Center (DC) APJII dan Operasional IIX merupakan personel kunci yang memiliki tanggung jawab utama dalam memastikan seluruh kegiatan operasional, pemeliharaan, keamanan, serta kontinuitas layanan di lingkungan Data Center APJII dan infrastruktur Internet Exchange Indonesia (IIX) berjalan dengan **andalan, aman, efisien, dan sesuai standar layanan (Service Level Agreement/SLA)**.

Peran ini menjadi krusial karena Data Center APJII berfungsi sebagai **pusat konektivitas utama antar anggota ISP di Indonesia**, tempat beroperasinya infrastruktur IIX sebagai **tulang punggung pertukaran lalu lintas internet nasional**. Oleh karena itu, personel PIC wajib memahami aspek **teknis, operasional, manajerial, dan keamanan informasi** secara menyeluruh.

2. Tujuan

Tujuan dari penetapan Job Description ini adalah untuk:

1. Menjelaskan secara rinci **peran, tanggung jawab, dan wewenang** PIC Operasional DC APJII dan Operasional IIX.
2. Menjamin terlaksananya kegiatan operasional Data Center dan IIX secara **terpadu, efisien, dan sesuai prosedur operasional standar (SOP)**.
3. Memastikan **kepatuhan terhadap kebijakan dan standar** yang berlaku, termasuk:
    - **TIA-942** (Data Center Facility Standard)
    - **ISO/IEC 27001** (Information Security Management)
    - **ISO/IEC 20000** (IT Service Management)
    - **ISO 22301** (Business Continuity Management)
4. Menetapkan tanggung jawab dalam hal **pengawasan, koordinasi, dan pengendalian** seluruh aktivitas teknis-operasional Data Center dan IIX.
5. Mendukung tujuan strategis APJII dalam menyediakan **layanan infrastruktur internet nasional yang berkualitas dan andal**.

3. Ruang Lingkup

Ruang lingkup pekerjaan PIC/Penanggung Jawab Operasional mencakup **dua domain utama**, yaitu:

A. Operasional Data Center APJII

Meliputi seluruh aktivitas pengelolaan fasilitas fisik, sistem infrastruktur pendukung, dan pemeliharaan layanan Data Center, antara lain:

1. **Fasilitas & Infrastruktur**
    - Sistem kelistrikan utama & cadangan (UPS, panel distribusi)
    - Sistem pendingin (PAC/CRAC)
    - Sistem keamanan fisik (CCTV, akses kontrol, fire suppression)
    - Sistem monitoring
    - Sistem jaringan lokal dan interkoneksi
    - Manajemen ruang rak (rack space management) dan power distribution.
2. **Operasional Harian**
    - Melaksanakan jadwal operasional, inspeksi harian, dan preventive maintenance.
    - Memonitor kondisi lingkungan (temperature, kelembapan, kebersihan, daya, dll.).
    - Berkoordinasi dengan Manager/Staff Divisi APJII lainnya.
    - Melakukan pencatatan dan pelaporan log operasional.
    - Mengatur jadwal kunjungan teknis dan kegiatan anggota/tenant.
    - Melaksanakan Standard Operating Procedure (SOP) sesuai ISO dan TIA-942.
3. **Pemeliharaan & Perbaikan**
    - Mengkoordinasikan kegiatan pemeliharaan rutin.
    - Melakukan evaluasi performa sistem pendukung DC (power, cooling, fire system, network).
    - Menangani gangguan (incident handling) dan melakukan root cause analysis.
4. **Keamanan & Keselamatan**
    - Menjamin keamanan aset, fasilitas, dan personel yang bekerja di area DC.
    - Melaksanakan prosedur tanggap darurat (Emergency Response Plan) bila terjadi insiden.
    - Melakukan koordinasi dengan pihak keamanan, vendor, dan tenant dalam situasi krisis.
5. **Pelaporan & Dokumentasi**
    - Membuat laporan operasional harian, mingguan, dan bulanan.
    - Melakukan review SOP dan update jika terdapat perubahan infrastruktur.
    - Menyusun laporan audit internal maupun eksternal.

B. Operasional IIX (Indonesia Internet Exchange) di DC APJII

Meliputi kegiatan yang berhubungan dengan pengelolaan infrastruktur jaringan pertukaran lalu lintas internet nasional (peering exchange), yaitu:

1. **Manajemen Infrastruktur Jaringan**
    - Monitoring performa switch core, router, dan link backbone IIX.
    - Menjaga ketersediaan port dan kapasitas konektivitas antar anggota ISP.
    - Memastikan redundansi jaringan dan routing berjalan optimal.

2. **Operasional dan Monitoring**
    - Melakukan pemantauan (24x7) terhadap traffic, latency, dan packet loss.
    - Menangani gangguan jaringan (fault management) serta melakukan troubleshooting awal.
    - Melaksanakan prosedur escalation ke tim NOC atau vendor terkait bila terjadi insiden besar.
3. **Manajemen Anggota dan Interkoneksi**
    - Mengatur penjadwalan dan pendampingan pemasangan koneksi anggota baru.
    - Memastikan dokumentasi topologi dan port assignment selalu diperbarui.
    - Memberikan dukungan teknis kepada anggota ISP terkait peering setup atau routing issue.
4. **Koordinasi dan Kolaborasi**
    - Berkoordinasi dengan tim NOC pusat, tim Network Engineering, serta pihak ketiga (vendor & telco provider).
    - Berkoordinasi dengan Manager/Staff Divisi APJII lainnya.
    - Melaksanakan kegiatan maintenance terjadwal (planned maintenance) dan change management.
5. **Pelaporan & Analisis**
    - Menyusun laporan traffic summary harian/mingguan/bulanan IIX.
    - Melakukan analisis kapasitas (capacity planning) dan rekomendasi upgrade.
    - Menyusun laporan kinerja jaringan dan availability SLA.

4. Tanggung Jawab Utama (Key Responsibilities)

No	Area	Uraian Tanggung Jawab
1	**Operasional DC**	Mengawasi operasional Data Center agar berjalan 24x7 dengan SLA 99,982% (Rated-3).
2	**Maintenance & Inspection**	Memastikan kegiatan preventive dan corrective maintenance berjalan tepat waktu dan terdokumentasi.
3	**Monitoring Infrastruktur**	Mengontrol sistem power, cooling, keamanan, dan jaringan melalui BMS atau DCIM.
4	**Manajemen IIX**	Mengelola operasi jaringan IIX, memastikan performa, stabilitas, dan peering berjalan baik.
5	**Incident Response**	Menangani insiden operasional dengan cepat, akurat, dan sesuai prosedur tanggap darurat.
6	**Reporting & Documentation**	Menyusun laporan rutin (harian, mingguan, bulanan) dan dokumentasi teknis-operasional.
7	**Compliance**	Memastikan semua kegiatan sesuai standar ISO 27001, TIA-942, dan kebijakan internal APJII.
8	**Vendor & Tenant Coordination**	Mengatur jadwal kerja vendor, mendampingi kegiatan anggota, serta memastikan keamanan dan prosedur akses.
9	**BCP & DRP**	Mengimplementasikan Business Continuity Plan dan Disaster Recovery Plan untuk menjaga kelangsungan layanan.
10	**Continuous Improvement**	Memberikan rekomendasi perbaikan efisiensi operasional dan peningkatan keandalan sistem.

5. Kualifikasi dan Kompetensi

Kualifikasi Umum:

- Pendidikan minimal S1 Teknik Elektro / Teknik Informatika / Sistem Informasi.
- Pengalaman minimal 3–5 tahun di bidang operasional Data Center, NOC, atau ISP.
- Memahami standar **TIA-942**, **ISO 27001**, **ISO 22301**, dan **ISO 20000**.
- Menguasai sistem listrik, pendingin, jaringan, serta keamanan fisik Data Center.

Kompetensi Teknis:

- Network Monitoring Tools
- DCIM operation.
- Troubleshooting listrik, UPS, genset, PAC, fire system.
- Linux/Unix system administration (untuk operasional IIX).
- Dokumentasi dan pelaporan teknis.

Kompetensi Manajerial & Soft Skill:

- Kepemimpinan dan tanggung jawab tinggi.
- Kemampuan analitis dan pengambilan keputusan cepat.
- Komunikatif dan kolaboratif dengan berbagai pihak (internal & eksternal).
- Disiplin, jujur, dan berorientasi pada hasil.

6. Wewenang

PIC/Penanggung Jawab Operasional DC & IIX berwenang untuk:

1. Mengambil keputusan operasional darurat sesuai prosedur (Emergency Action Authority).
2. Menyetujui atau menolak aktivitas vendor/tenant yang berpotensi mengganggu layanan.
3. Mengajukan permintaan perbaikan atau pengadaan komponen infrastruktur.
4. Melaporkan dan mengeskalasi insiden ke jajaran Pengurus APJII.
5. Mengeluarkan laporan resmi operasional dan rekomendasi teknis.

7. Pelaporan dan Hubungan Kerja

- **Atasan Langsung:** Ketua Bidang Terkait
- **Koordinasi Fungsional:**
    - Supervisor
    - Tim Teknis/NOC
    - Administrasi dan Support
- **Pihak Eksternal:**
    - Anggota/Tenant ISP
    - Vendor pihak ketiga
    - Pengelola Gedung

8. Key Performance Indicators (KPI)

Kinerja PIC Operasional DC APJII dan IIX diukur melalui sejumlah **Key Performance Indicators (KPI)** yang menggambarkan efektivitas, efisiensi, dan keandalan operasional layanan. KPI ini mencakup aspek teknis, administratif, serta kepatuhan terhadap standar.

No	Kategori	Indikator Kinerja Utama	Target
A. Operasional Data Center			
1	**Availability**	Waktu ketersediaanlayanan Data Center	≥ 99,982% (sesuai Rated-3 TIA-942)
2	**Incident Handling**	Rata-rata waktu penanganan insiden (MTTR)	< 30 menit untuk kategori medium; < 10 menit untuk critical
3	**Preventive Maintenance**	Persentase pelaksanaan preventive maintenance tepat waktu	≥ 98% dari jadwal
4	**Power & Cooling Monitoring**	Tidak ada downtime akibat kegagalan power/cooling	0 kejadian/tahun
B. Operasional IIX			
5	**Network Availability**	Ketersediaan konektivitas IIX (switch/router core)	≥ 99.99%
6	**Traffic Stability**	Tidak ada degradasi signifikan traffic >10% dari baseline	Maks. 1 kali/tahun
7	**Incident Resolution**	Waktu respon dan penyelesaian gangguan jaringan	Respon < 10 menit, resolusi < 60 menit
C. Administratif & Kepatuhan			
8	**Pelaporan Operasional**	Ketepatan waktu pengiriman laporan operasional (harian/mingguan/bulanan)	100% sesuai jadwal
9	**Audit Kepatuhan**	Tidak ada temuan mayor dari audit internal/eksternal	0 temuan mayor
10	**SOP Compliance**	Tingkat kepatuhan terhadap prosedur operasi standar	≥ 95%

PIC wajib melakukan **self-assessment** terhadap KPI setiap akhir bulan dan melaporkan ke **Ketua Umum APJII**.

9. Prosedur Pelaksanaan Tugas Harian

Prosedur pelaksanaan tugas harian PIC Operasional meliputi aktivitas rutin, monitoring, pelaporan, dan komunikasi koordinatif dengan berbagai pihak. Berikut rinciannya:

A. Daily Routine (Setiap Shift)

1. **Morning Briefing / Handover**
    - Menerima dan mengevaluasi laporan dari Supervisor (incident, maintenance, atau alarm aktif).
    - Memeriksa logbook operasional dan status sistem utama (power, cooling, fire, security, network).
2. **Pemeriksaan Fisik (Visual Inspection)**
    - Memeriksa ruang server, UPS room, battery room, genset area, PAC/CRAC, dan panel distribusi.
    - Mencatat dan menganalisa anomali suhu, suara, getaran, atau kebocoran (WLDS check).
3. **Monitoring Dashboard**
    - Memeriksa status Jaringan melalui Portal Pusat Layanan APJII berupa aplikasi dan Tools yang digunakan.
    - Memastikan tidak ada alarm aktif pada sistem utama.
4. **Log & Reporting**
    - Mengisi log sheet operasional (power, temperature, humidity, load, dan traffic).
    - Mencatat hasil pemeriksaan di sistem ticketing atau Excel-based log book.
5. **Koordinasi Kegiatan**
    - Mengatur kegiatan vendor atau tenant yang akan bekerja (melalui Work Permit).
    - Mengawasi pekerjaan on-site agar sesuai SOP dan safety requirement.

B. Weekly Routine

- Review performa beban listrik dan distribusi daya.
- Pemeriksaan kelengkapan APAR, panel indikator, dan sistem monitoring.
- Update dokumentasi topologi jaringan IIX.
- Menyusun laporan mingguan (Weekly Operational Summary).

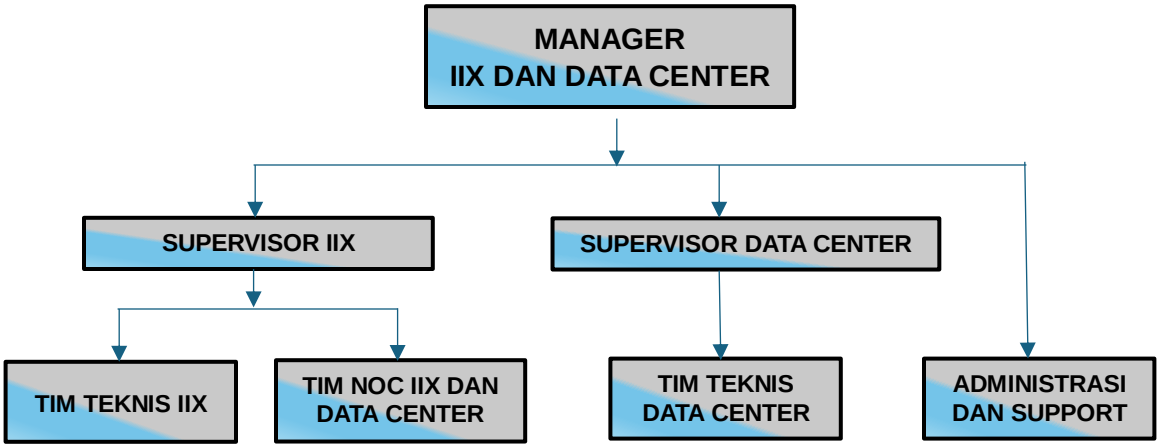
C. Monthly Routine

- Melakukan koordinasi preventive maintenance dengan vendor (UPS, PAC/CRAC, VESDA, WLDS, DCIM).
- Analisis tren energi, cooling, dan traffic IIX.
- Update data rack utilization, power usage, dan environmental performance.
- Laporan bulanan kepada Manajemen APJII.

10. Struktur Tim Pendukung Operasional

Struktur organisasi operasional DC APJII dan IIX disusun untuk mendukung kegiatan 24x7 dengan pembagian fungsi yang jelas.

A. Struktur Organisasi Operasional (Functional Structure)



B. Shift & Coverage

- **Shift 1:** 07.00 – 15.00
- **Shift 2:** 15.00 – 23.00
- **Shift 3:** 23.00 – 07.00
- **PIC Operasional:** on-call 24x7 (primary escalation point)

PIC wajib hadir pada jam kerja normal (Senin–Jumat) dan standby untuk **escalation atau emergency call** kapanpun dibutuhkan.

11. Format Pelaporan & Eskalasi Insiden

A. Format Laporan Operasional

PIC wajib menyusun laporan rutin sebagai berikut:

Jenis Laporan	Frekuensi	Isi Utama	Tujuan
Laporan Harian Operasional	Harian	Status sistem, alarm aktif, aktivitas tenant/vendor, issue minor	Dokumentasi monitoring
Laporan Mingguan	Mingguan	Rekap insiden, preventive maintenance, kondisi power & cooling	Analisis tren mingguan
Laporan Bulanan	Bulanan	Statistik Ketersediaan Waktu, utilisasi daya, traffic IIX, rekomendasi perbaikan	Evaluasi manajemen
Laporan Insiden	Setiap kejadian	Kronologi, waktu kejadian, dampak, tindakan korektif	Audit dan RCA
Laporan Audit Kepatuhan	Triwulan	Temuan, gap compliance, rekomendasi	Peningkatan kualitas operasional

B. Mekanisme Eskalasi Insiden

Level Eskalasi:

1. **Level 1:** Dapat ditangani oleh Helpdesk/Tim Teknis/NOC (alarm minor, sensor error, dll.)
2. **Level 2:** Tim Teknis/NOC (gangguan subsystem, UPS, CRAC, link IIX intermittent)
3. **Level 3:** PIC/Penanggung Jawab Operasional DC & IIX atau ICO (gangguan mayor, potensi downtime)
4. **Level 4:** Ketua Umum APJII (major outage, force majeure)

SOP Eskalasi Cepat (Emergency Escalation):

- Notifikasi ke stakeholder dalam waktu **≤ 10 menit** sejak insiden terdeteksi.
- Pelaporan awal (Initial Report) ≤ 30 menit.
- Root Cause Analysis (RCA) maksimal 2x24 jam setelah insiden tertangani.

12. Skema Shift Operasional & Rotasi Tugas

Untuk memastikan ketersediaan layanan 24 jam sehari dan 7 hari seminggu, PIC Operasional bersama tim menjalankan **sistem shift bergilir (rotating schedule)** dengan ketentuan sebagai berikut:

Shift	Jam Operasional	Personel	Tanggung Jawab Utama
1	06.00 – 15.00	1 NOC + 2 teknisi	Pemeriksaan rutin harian, koordinasi vendor, laporan harian
2	14.00 – 23.00	1 PIC + 1 teknisi	Monitoring traffic IIX, kontrol akses malam, laporan shift
3	22.00 – 07.00	1 teknisi + standby PIC on-call	Pemantauan sistem malam hari, alarm monitoring, laporan insiden

Rotasi:

- Rotasi dilakukan **setiap 2 minggu** untuk menjaga keadilan dan kompetensi lintas shift.
- PIC wajib melakukan **briefing antar shift (handover meeting)** minimal 10 menit sebelum pergantian shift.

13. Penutup

Job Description ini menjadi acuan resmi dalam menjalankan tanggung jawab dan fungsi operasional di **Data Center APJII dan IIX Facility**. Setiap PIC wajib memahami dan mematuhi seluruh isi dokumen ini sebagai bentuk profesionalisme dan tanggung jawab terhadap kelangsungan layanan internet nasional Indonesia.

Dokumen ini harus ditinjau dan diperbarui **setiap tahun** atau apabila terdapat perubahan struktur organisasi, infrastruktur, atau standar operasional.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN LV
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

JOB DESCRIPTION SUPERVISOR IIX APJII

1. Pendahuluan

Supervisor IIX bertanggung jawab dalam memastikan keberlangsungan layanan pertukaran trafik internet nasional (Internet Exchange Point) yang dikelola oleh APJII. Posisi ini memegang peran strategis dalam menjamin operasional infrastruktur interkoneksi antar Pengguna IIX agar dapat berjalan optimal, stabil, aman, serta memenuhi standar teknis dan operasional yang berlaku.

Sebagai koordinator teknis, Supervisor IIX mengawasi aktivitas instalasi, pengelolaan, dan pemeliharaan perangkat jaringan, memastikan kinerja dan kapasitas IIX tetap sesuai dengan kebutuhan pertumbuhan trafik nasional.

2. Tujuan

Job description ini bertujuan untuk:

1. Menjadi acuan formal bagi pelaksanaan tugas Supervisor IIX dalam mendukung kelancaran operasi Indonesia Internet eXchange.
2. Menjamin seluruh proses operasional IIX berjalan secara efisien, aman, dan sesuai standar industri.
3. Memberikan kejelasan peran, tanggung jawab, dan ruang lingkup kerja dalam manajemen jaringan, interkoneksi, dan koordinasi operasional.
4. Mendorong peningkatan kualitas layanan, kepatuhan, serta kontinuitas operasional di lingkungan Data Center APJII.

3. Dasar dan Referensi Standar

Supervisor IIX mengacu pada standar, pedoman, dan praktik terbaik berikut:

Standar Teknis & Infrastruktur

- TIA-942 Data Center Standard (Rated Facility).
- ISO/IEC 27001 – Information Security Management System (ISMS).
- ISO 20000 – IT Service Management.
- ITIL Framework v4 – Operation, Incident, Problem, Change Management.

4. Definisi Istilah

- **IIX (Indonesia Internet Exchange)**: Platform pertukaran trafik internet nasional yang menghubungkan ISP, operator, CDN, cloud provider, dan peserta jaringan lainnya.
- **Peering**: Pertukaran langsung trafik internet antar dua entitas jaringan untuk meningkatkan kecepatan dan efisiensi rute.
- **Interkoneksi**: Mekanisme fisik dan logis untuk menghubungkan jaringan peserta ke infrastruktur IIX.
- **BGP (Border Gateway Protocol)**: Protokol routing utama yang digunakan dalam interkoneksi peering.
- **Uplink/Downlink**: Arah trafik keluar atau masuk dari jaringan ke IIX.
- **Port Capacity Management**: Pengelolaan kapasitas port untuk memastikan ketersediaan dan skalabilitas interkoneksi.
- **NOC (Network Operation Center)**: Unit operasional yang memantau dan menangani insiden jaringan.

5. Ruang Lingkup Tugas dan Tanggung Jawab

A. Manajemen Peering dan Interkoneksi

1. Memastikan setiap permohonan peering dan interkoneksi sudah lengkap secara administrasi.
2. Memastikan setiap pekerjaan peering dan interkoneksi dikerjakan sesuai SOP.
3. Menjaga kebijakan peering agar sesuai dengan SOP IIX dan standar global.
4. Melakukan evaluasi kapasitas peering dan kebutuhan upgrading port.

B. Instalasi & Pemeliharaan Hardware Jaringan

1. Melakukan supervisi instalasi perangkat (switch, router, cross-connect, patch panel dan perangkat lainnnya).
2. Memastikan patching fiber dilakukan sesuai standar labeling dan manajemen kabel.
3. Melakukan preventive maintenance perangkat IIX secara berkala.
4. Memantau utilisasi hardware dan melakukan rencana kapasitas (capacity planning).

C. Pemantauan dan Kinerja Jaringan

1. Memantau performa IIX menggunakan Monitoring tools dan system lainnya.
2. Menganalisis trafik, latency, throughput, dan kualitas interkoneksi.
3. Menyusun laporan tren trafik bulanan, kuartalan, dan tahunan.
4. Menangani isu degradasi performa dan melakukan optimasi routing.

D. Troubleshooting dan Incident Management

1. Menangani gangguan jaringan, kegagalan link, atau anomali trafik secara cepat.
2. Supervisi pekerjaan root cause analysis (RCA) dan memberikan rekomendasi perbaikan.
3. Mengelola eskalasi insiden kepada vendor atau Anggota.
4. Memastikan SLA ketersediaan waktu aktif IIX terpenuhi sesuai standar APJII.

E. Koordinasi Vendor dan Mitra

1. Mengelola hubungan teknis dengan vendor perangkat, provider backbone, dan Anggota.
2. Melakukan evaluasi performa vendor dan review kontrak teknis.
3. Mengkoordinasikan kegiatan instalasi perangkat baru, replacement, dan maintenance.

F. Manajemen Proyek

1. Supervisi proyek peningkatan kapasitas IIX (capacity upgrade), migrasi system dan penambahan Node IIX baru.
2. Supervisi progres timeline dan pelaporan perkembangan proyek.
3. Supervisi resource allocation untuk proyek
4. Melakukan pengujian penerimaan (commissioning) perangkat dan layanan baru.

G. Dokumentasi, Pelaporan Dan Keamanan Data

1. Menjaga dokumentasi jaringan, diagram topologi, dan baseline konfigurasi.
2. Membuat laporan operasional, insiden, pemakaian port, dan pemantauan performa.
3. Memastikan seluruh dokumentasi diperbarui sesuai change management process.
4. Menjaga kerahasiaan Data

H. Kepatuhan terhadap Standar & Kebijakan

1. Memastikan seluruh prosedur operasional merujuk kepada standar TIA-942, ISO 27001, ISO 20001 dan ITIL.
2. Menjaga keamanan informasi, akses jaringan, dan perlindungan data.
3. Mendampingi audit internal dan eksternal, serta menindaklanjuti temuan audit.
4. Memastikan penerapan SOP Data Center APJII dan standar keselamatan kerja.

6. Penutup

Job description ini menjadi landasan peran Supervisor IIX APJII dalam mendukung keberlangsungan operasional Internet Exchange nasional yang aman, efisien, dan handal. Posisi ini memiliki dampak strategis terhadap kualitas internet Indonesia dan menjadi penghubung utama antar pelaku ekosistem jaringan nasional.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN LVI
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

JOB DESCRIPTION SUPERVISOR DATA CENTER APJII

1. Pendahuluan

Supervisor Data Center merupakan posisi strategis yang bertanggung jawab untuk memastikan operasional harian Data Center APJII berjalan dengan aman, efisien, dan sesuai dengan standar industri. Peran ini mencakup supervisi langsung terhadap tim operasional, pengendalian kualitas layanan, penerapan prosedur operasional standar, serta memastikan bahwa seluruh infrastruktur, fasilitas, dan layanan Data Center berada dalam kondisi optimal.

2. Tujuan

Dokumen ini disusun untuk:

1. Menjabarkan tugas dan tanggung jawab Supervisor Data Center secara jelas dan terstruktur.
2. Menjadi acuan baku bagi pelaksanaan operasi Data Center APJII.
3. Menjamin konsistensi layanan, keamanan, dan kepatuhan terhadap standar operasional dan regulasi yang berlaku.
4. Mendukung pengembangan kompetensi tim dan efisiensi manajemen fasilitas Data Center.

3. Dasar dan Referensi Standar

Tugas Supervisor Data Center merujuk pada standar dan panduan berikut:

- **TIA-942 (Telecommunications Infrastructure Standard for Data Centers):** Khususnya aspek Rated Facilities, operasi, pemeliharaan, dan keamanan.
- **ISO/IEC 27001:** Sistem Manajemen Keamanan Informasi (Information Security Management System).
- **ISO 20000:** Sistem Manajemen Layanan TI (IT Service Management).
- **ISO 22301:** Business Continuity Management System.

4. Definisi Istilah

- **Data Center:** Fasilitas terpusat yang digunakan untuk menyimpan, mengolah, dan mendistribusikan data serta layanan jaringan.
- **SOP (Standard Operating Procedure):** Prosedur baku yang memandu pelaksanaan operasional Data Center.
- **Kepatuhan (Compliance):** Pemenuhan terhadap standar, regulasi, dan kebijakan internal maupun eksternal.
- **SLA (Service Level Agreement):** Kesepakatan tingkat layanan antara Data Center dan penggunanya.
- **Critical Infrastructure:** Komponen vital Data Center seperti UPS, PAC/CRAC, fire suppression, access control, dan jaringan.

5. Ruang Lingkup Tugas & Tanggung Jawab

A. Supervisi Operasional Harian Data Center APJII

1. Memastikan operasional 24/7 berjalan sesuai SOP dan standar teknis.
2. Memantau kondisi infrastruktur kritikal: listrik, pendinginan, keamanan fisik, jaringan, dan sistem monitoring.
3. Melakukan analisis insiden harian dan memastikan tindak lanjut tepat waktu.
4. Mengawasi aktivitas layanan colocation, rack provisioning, dan monitoring kapasitas.
5. Menjamin kebersihan area operasional, kontrol lingkungan, dan keselamatan kerja.

B. Manajemen Tim Data Center

1. Mengatur jadwal shift, pembagian tugas, dan evaluasi kinerja staf Data Center.
2. Memberikan arahan teknis dan mentoring kepada teknisi.
3. Melakukan pelatihan berkala terkait standar operasional, keselamatan, dan keamanan informasi.
4. Memastikan tim siap merespons insiden, emergency, dan prosedur eskalasi.

C. Pengembangan & Implementasi SOP

1. Menyusun, memperbarui, dan meningkatkan Layanan Operasional, Maintenance, Incident Handling, Visitor Management, dan Change Management.
2. Melakukan koordinasi antar Divisi Terkait untuk memastikan SOP selaras dengan kebijakan APJII.
3. Membantu kebutuhan audit internal pemenuhan SOP terkait Data dan Laporan yang dibutuhkan.
4. Mengelola dokumen operasional: logbook, checklist harian, laporan insiden, dan laporan bulanan.

D. Pengawasan & Pemeliharaan Sistem

1. Mengawasi pelaksanaan **Preventive Maintenance** dan **Predictive Maintenance** untuk seluruh sistem kritikal:
    - Sistem kelistrikan (UPS, battery, panel listrik).
    - Sistem mekanikal (PAC/CRAC, Fire Suppression).
    - Sistem keamanan (CCTV, access control).
2. Memastikan vendor eksternal dan teknisi menjalankan pekerjaan sesuai jadwal dan standar.
3. Memvalidasi laporan hasil maintenance dan memastikan tidak ada temuan yang terlewat.
4. Memantau kapasitas daya, cooling, cable tray, ducting dan ruang rak untuk memastikan ketersediaan yang optimal.

E. Manajemen Inventaris dan Aset

1. Mengelola aset Data Center baik infrastruktur, perangkat TIK, spare part, dan consumable.
2. Memastikan keakuratan data inventaris melalui sistem pencatatan yang valid.
3. Melakukan pengawasan terhadap keluar-masuknya perangkat pelanggan (rack-mounted, cable patch, server dan perangkat lainnya).
4. Memastikan standar labeling, dokumentasi, dan tata letak peralatan sesuai prosedur.
5. Melakukan pengawasan dan pengelolaan terhadap perangkat BackUp dan ketersediaan stok untuk:
    1. Kabel dan SFP untuk kebutuhan Interkoneksi
    2. Perangkat Router, Switch dan perangkat lainnya

F. Kepatuhan terhadap Standar & Keamanan Data Center

1. Memastikan seluruh kegiatan operasional mematuhi standar TIA-942, ISO 27001, ISO 20001 dan regulasi yang relevan.
2. Mengawasi penerapan keamanan fisik termasuk akses tamu, inspeksi perangkat, serta penanganan insiden keamanan.
3. Menjamin lingkungan Data Center terlindungi dari risiko kebakaran, banjir, suhu ekstrem, dan ancaman lainnya.
4. Melakukan koordinasi untuk audit internal dan eksternal terkait operasional Data Center.

G. Pengembangan Sumber Daya Manusia

1. Melakukan Pengembangan Sumber Daya Manusia secara berkala dengan mengikuti Pelatihan dan Sertifikasi yang relefan dengan pekerjaannya
2. Melakukan pengawasan terhadap kinerja Tim Data Center sebagai acuan Penilaian dan Pengembangan Sumber Daya Manusia.

6. Penutup

Supervisor Data Center memiliki peran penting dalam memastikan stabilitas layanan, efisiensi operasional, keamanan, dan keandalan fasilitas Data Center APJII. Dengan menjalankan tugas dan tanggung jawab sesuai dokumen ini, diharapkan kualitas operasional Data Center dapat selalu terjaga dan memenuhi ekspektasi anggota APJII dan stakeholder lainnya.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN LVII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

JOB DESCRIPTION TIM TEKNIS IIX, TIM TEKNIS DATA CENTER, TIM NOC IIX DAN DATA CENTER APJII

1. Pendahuluan

Tim Teknis & NOC (Network Operations Center) IIX merupakan unit operasional strategis yang bertanggung jawab memastikan ketersediaan, keandalan, keamanan, dan kinerja optimal dari seluruh infrastruktur jaringan Indonesia Internet Exchange (IIX) yang berada di Data Center APJII.

Tim ini merupakan garda terdepan dalam pengelolaan operasional jaringan 24x7, penanganan insiden, pemeliharaan proaktif, serta dukungan teknis tingkat lanjut kepada anggota/tenant, operator jaringan, dan internal APJII.

NOC IIX menjadi pusat kendali yang memastikan layanan peering berjalan stabil, pertukaran trafik berjalan performa optimal, serta infrastruktur tumbuh mengikuti perkembangan kebutuhan internet nasional.

2. Tujuan

Job Description ini disusun untuk:

1. Mendefinisikan peran, fungsi, tanggung jawab, dan batasan kerja Tim Teknis/NOC IIX.
2. Menjadi pedoman operasional dan standar kerja dalam menjalankan kegiatan pemantauan, pemeliharaan, troubleshooting, dan perencanaan jaringan IIX.
3. Menjamin konsistensi kualitas layanan, keandalan operasional, dan kepatuhan terhadap standar nasional maupun internasional dalam pengelolaan Internet Exchange.
4. Menjadi dasar evaluasi kinerja dan pengembangan kompetensi untuk seluruh personel Tim Teknis/NOC IIX.

3. Dasar & Referensi Standar

Standar Internasional

- ISO/IEC 27001 – Information Security Management Systems (ISMS)
- ISO/IEC 20000 – IT Service Management
- ISO 22301 – Business Continuity Management
- ITIL v4 – Service Operation & Service Management

4. Definisi Istilah

- **IIX (Indonesia Internet Exchange):** Platform pertukaran trafik internet nasional antar ISP, penyelenggara jasa internet, dan organisasi anggota APJII.
- **NOC (Network Operations Center):** Pusat kendali operasional jaringan yang melakukan monitoring 24x7 dan penanganan insiden jaringan.
- **Incident:** Gangguan atau penurunan kualitas layanan yang berdampak pada operasional jaringan.
- **Problem:** Akar masalah dari insiden yang terjadi terus menerus dan memerlukan investigasi lanjutan.
- **Change Request (CR):** Permintaan perubahan terencana pada sistem jaringan.
- **Planned Maintenance:** Kegiatan pemeliharaan rutin yang sudah terjadwal.
- **Unplanned Outage:** Gangguan layanan yang terjadi tidak terduga.
- **Peering:** Kerjasama pertukaran trafik antar anggota IIX.
- **Member/Tenant:** Anggota APJII yang terhubung ke IIX.

5. Ruang Lingkup Tugas & Tanggung Jawab

5.1 Pemantauan Jaringan (Network Monitoring) – 24x7

- Melakukan pemantauan proaktif terhadap:
  - Router, switch, dan perangkat jaringan IIX
  - Link peering anggota
  - Bandwidth utilization, latency, packet loss, dan throughput
  - Sistem otomatisasi dan perangkat pendukung NMS (Network Monitoring System)
- Menggunakan tools seperti NMS, SNMP, syslog, NetFlow/sFlow, dan dashboard internal.
- Melakukan early detection untuk potensi gangguan dan perlambatan trafik.
- Membuat laporan pemantauan harian, mingguan, dan bulanan.

5.2 Manajemen Insiden (Incident Management)

- Menerima, mencatat, mengkategorikan, dan menindaklanjuti setiap insiden yang terjadi.
- Analisa awal (initial diagnostics) terhadap sumber gangguan.
- Eskalasi berjenjang ke Supervisor, Manager, Pengelola Gedung dan vendor.
- Melakukan koordinasi dan komunikasi insiden kepada Anggota/Tenant, internal APJII, dan stakeholder lain.

- Mendampingi penanganan insiden hingga resolusi dan layanan pulih sepenuhnya.
- Melaporkan perihal incident yang terjadi (Incident Report).

5.3 Manajemen Permasalahan (Problem Management)

- Menyelidiki akar penyebab (Root Cause Analysis / RCA) untuk insiden berulang atau kritikal.
- Berkolaborasi dengan Vendor dan/atau Pengelola Gedung untuk perbaikan permanen.
- Mengelola Problem Record dan memastikan tindakan korektif dilakukan.
- Melaporkan perihal penyebab insiden yang telah terjadi (RCA).

5.4 Manajemen Perubahan (Change Management)

- Memproses permintaan perubahan jaringan (CR).
- Menilai risiko perubahan dan memberikan rekomendasi teknis.
- Koordinasi jadwal pemeliharaan terencana dengan Anggota/Tenant & internal.
- Melakukan implementasi perubahan jaringan sesuai SOP & standar keamanan.
- Melaporkan Change Implementation.

5.5 Pemeliharaan Sistem Jaringan (Network Maintenance)

- Preventive maintenance pada perangkat IIX secara berkala:
    - Pengecekan hardware
    - Upgrade firmware & OS
    - Pembersihan fisik perangkat
    - Validasi konfigurasi & routing
    - Melakukan BackUp konfigurasi
- Melakukan patching perangkat IIX sesuai siklus agar keamanan dan kestabilan selalu terjaga.

5.6 Instalasi & Konfigurasi (Deployment & Provisioning)

- Melakukan instalasi perangkat jaringan baru (switch, router, optical device, DWDM serta perangkat Infrastruktur pendukung IIX).
- Provisioning VLAN, routing, policy, dan peering untuk Anggota baru.
- Penerapan best practices routing menggunakan BGP pada IIX.
- Dokumentasi lengkap atas setiap instalasi & konfigurasi.

5.7 Dukungan Teknis Lanjutan (Advanced Technical Support)

- Menangani permasalahan teknis kompleks yang tidak dapat diselesaikan oleh Anggota.
- Analisa mendalam terkait:
    - Routing loops, route leaks, prefix issues
    - Peering misconfiguration
    - Interface flapping, link quality degradation

- Memberikan rekomendasi teknis dan optimasi kepada Anggota.

5.8 Manajemen Infrastruktur Jaringan

- Memastikan seluruh infrastruktur IIX berjalan optimal:
    - Core Router dan redudansi Router
    - Distribution Switch
    - Peering LAN
    - CPE (*Customer Premises Equipment*) member
    - Power & cooling untuk perangkat IIX
- Monitoring kapasitas dan melakukan kapasitas planning berkala.
- Menjaga inventory perangkat, lisensi, dan spare-part availability.
- Menyediakan backup perangkat infrastruktur IIX baik bersifat pasif maupun aktif.

5.9 Perencanaan & Perancangan Pengembangan IIX (Engineering & Architecture)

- Berpartisipasi dalam desain arsitektur dan ekspansi jaringan IIX.
- Memberikan masukan terkait kebutuhan upgrade:
    - Bandwidth link
    - Switching fabric
    - Optical transport
- Berkontribusi dalam roadmap pengembangan IIX jangka panjang untuk memenuhi kebutuhan internet nasional.

5.10 Dokumentasi Teknis & Pelaporan

- Mengelola dan memperbarui:
    - Network diagrams
    - IP addressing
    - Mac Address
    - Routing policies
    - Peering procedure
    - Laporan operasional
- Menyusun laporan outage, maintenance, dan kinerja jaringan.

5.11 Kepatuhan, Keamanan, & Audit

- Memastikan operasional sesuai standar keamanan jaringan dan kebijakan internal.
- Mengimplementasikan hardening pada perangkat jaringan.
- Mendukung audit internal & eksternal terkait operasional IIX.
- Menjaga kerahasiaan data anggota & informasi teknis.

5.12 Kolaborasi & Komunikasi

- Berkoordinasi dengan:

    - Tim teknis Anggota APJII
    - Vendor perangkat
    - Internal APJII (operational, security, Divisi terkait)
- Memberikan edukasi teknis kepada Anggota terkait best practices peering.

6. Penutup

Dokumen Job Description ini, dapat menjadi rujukan resmi bagi seluruh personel Tim Teknis & NOC IIX APJII dalam menjalankan operasional sehari-hari, memastikan kualitas layanan yang optimal, serta mendukung strategi pembangunan infrastruktur internet nasional melalui IIX APJII.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN LVIII
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

JOB DESCRIPTION TEAM SECURITY DATA CENTER & IIX APJII

1. Pendahuluan

Data Center APJII dan Indonesia Internet Exchange (IIX) merupakan fasilitas kritikal nasional yang mendukung layanan internet Indonesia dan berbagai anggota APJII. Keamanan fisik pada fasilitas ini merupakan faktor utama untuk menjaga ketersediaan layanan, integritas infrastruktur, dan kerahasiaan aset yang dikelola. Untuk itu, Tim Security/Satuan Pengaman berperan sebagai garda terdepan dalam memastikan seluruh area data center dan IIX tetap aman, tertib, dan beroperasi sesuai prosedur keamanan yang berlaku.

2. Tujuan

Job Description ini disusun untuk:

1. Menjadi pedoman bagi Tim Security dalam menjalankan fungsi pengamanan fisik di Data Center dan IIX APJII.
2. Menjamin semua aktivitas pengamanan mengikuti standar operasional dan praktik terbaik industri data center.
3. Mengatur tanggung jawab pengawasan, pemeriksaan, pengendalian akses, pemantauan, hingga penanganan insiden keamanan.
4. Menciptakan koordinasi yang baik antara Tim Security APJII, Tim Operasional Data Center, serta Tim Security Gedung Cyber-1 sebagai pemilik bangunan.

3. Dasar dan Referensi Standar

Pelaksanaan tugas Tim Security mengacu pada standar dan kebijakan sebagai berikut:

1. **Standar Keamanan Data Center Internasional**
    - TIA-942 (Telecommunications Infrastructure Standard for Data Centers) – bagian Physical Security
    - ISO/IEC 27001 – Information Security Management System (kontrol keamanan fisik – Annex A.11)
    - ISO 22301 – Business Continuity Management (pengelolaan situasi darurat)

2. **Regulasi Nasional**
    - Peraturan Kepolisian RI terkait Satuan Pengamanan (Satpam)
    - Kebijakan pengamanan gedung dan fasilitas vital nasional (bila relevan)

4. Definisi Istilah

- **Data Center APJII**: Fasilitas yang digunakan untuk penyimpanan server, perangkat jaringan, sistem IIX, dan infrastruktur pendukung.
- **IIX (Indonesia Internet Exchange)**: Titik pertukaran trafik internet nasional yang dikelola APJII.
- **MMR (Meet-Me Room)**: …
- **Security**: Personel satuan pengamanan yang bertugas menjaga keamanan fisik fasilitas.
- **Akses Fisik**: Proses masuk/keluar ke area terbatas menggunakan kunci, kartu akses, atau biometrik.
- **Vendor**: Pihak ketiga yang melakukan pekerjaan instalasi, pemeliharaan, atau perbaikan perangkat di area data center.
- **CCTV**: Sistem kamera pengawas yang digunakan untuk pemantauan keamanan.
- **Insiden Keamanan**: Aktivitas atau kejadian yang berpotensi mengganggu keamanan dan ketertiban fasilitas.

5. Ruang Lingkup Tugas & Tanggung Jawab

A. Menjaga Keamanan dan Ketertiban

1. Memastikan kondisi lingkungan di dalam Data Center, area IIX, MMR, serta area sekitar selalu dalam keadaan aman, tertib, dan sesuai prosedur.
2. Menegakkan tata tertib, peraturan, dan prosedur keamanan fisik yang berlaku di APJII.
3. Mencegah potensi gangguan keamanan, ancaman, vandalisme, atau aktivitas yang mencurigakan.

B. Pengawasan dan Pengendalian Akses

1. Mengendalikan akses masuk/keluar orang, dan barang ke dalam fasilitas Data Center APJII.
2. Melakukan pemeriksaan terhadap staf, tamu, pengunjung, dan vendor sesuai protokol keamanan dan prosedurnya.
3. Memastikan hanya personel yang memiliki otorisasi yang dapat mengakses area sensitif:
    - Ruang Server/Datahall, MMR, IIX.
    - Ruang NOC & Staging.
    - Ruang UPS, Battery, PAC, Panel Listrik dan Infrastruktur pendukung lainnya.
4. Mengoperasikan sistem akses (kartu akses, logbook, biometrik) serta memastikan pencatatan dilakukan dengan benar dan lengkap.

C. Patroli Berkala

1. Melaksanakan patroli rutin di seluruh area fasilitas, termasuk:
    - Perimeter luar Data Center
    - Ruang Server/Datahall, MMR, IIX.
    - Ruang UPS, Battery, PAC, Panel Listrik dan Infrastruktur pendukung lainnya.
    - Koridor dan common area
2. Deteksi dini terhadap ancaman: pintu tidak terkunci, kerusakan, kebocoran, suara abnormal, atau individu mencurigakan.
3. Melaporkan dengan segera bila terpantau potensi terjadinya insiden.
4. Melaporkan hasil patroli dalam bentuk log atau laporan harian.

D. Penanganan dan Pelaporan Insiden

1. Melakukan penanganan awal terhadap insiden seperti:
    - Upaya akses tidak sah
    - Kerusakan properti
    - Keadaan darurat (kebakaran, banjir, gempa, gangguan listrik)
2. Melakukan prosedur evakuasi sesuai SOP darurat bila diperlukan.
3. Menyusun laporan insiden lengkap untuk disampaikan kepada manajemen dan otoritas terkait.
4. Berpartisipasi dalam drill keamanan dan pelatihan BCP yang dilakukan APJII.

E. Penerapan Kebijakan Keamanan Fisik

1. Menegakkan seluruh kebijakan keamanan fisik yang ditetapkan oleh APJII.
2. Memastikan setiap staf, tamu, dan vendor memahami aturan keselamatan dan keamanan sebelum memasuki area terbatas.
3. Memberikan briefing keamanan kepada pihak eksternal jika diperlukan.

6. Tanggung Jawab Spesifik di Lingkungan Data Center & IIX

A. Perlindungan Infrastruktur Kritis

1. Mengamankan rak server, perangkat jaringan, patch panel, cross-connect, dan perangkat IIX.
2. Menjaga integritas area MMR yang merupakan titik interkoneksi kritikal antar operator/ISP.
3. Melarang membawa peralatan yang tidak diperlukan di dalam Data Center (Tas, Rokok/Rokok Elektrik, Korek Api, Makanan dan Minuman, dan peralatan lainnya).
4. Melaporkan setiap potensi ancaman atau aktivitas yang berisiko terhadap infrastruktur kritis.

B. Manajemen Kunci dan Kartu Akses

1. Mengelola dan mengawasi penggunaan kunci fisik, kartu akses, dan biometrik.
2. Mencatat setiap pemberian, pengambilan, atau pengembalian kunci/kartu.
3. Melakukan pengecekan terhadap barang-barang yang dibawa pada saat masuk, dan body checking pada saat keluar/masuk area Data Center.
4. Melakukan pengawasan akses secara berkala untuk memastikan tidak ada penyalahgunaan.

C. Koordinasi dengan Tim NOC/Tim Teknis Data Center

1. Menyediakan pengawasan keamanan untuk vendor atau teknisi eksternal.
2. Menjadi penghubung antara Tim Security Gedung Cyber-1 dan Tim Operasional APJII terkait isu keamanan gedung.

D. Pencatatan Tamu & Vendor

1. Memastikan seluruh tamu dan vendor terdaftar lengkap dalam logbook atau sistem visitor management.
2. Memberikan visitor badge atau kartu akses sementara sesuai regulasi.
3. Menjelaskan aturan keamanan sebelum tamu atau vendor memasuki area terbatas.
4. Membuat Laporan Harian kegiatan aktivitas pengunjung Data Center.

7. Penutup

Job Description ini diharapkan menjadi acuan yang jelas bagi seluruh Tim Security APJII dalam menjaga keamanan fisik Data Center dan IIX. Pengamanan yang efektif adalah fondasi utama dalam menjaga kelangsungan layanan digital nasional dan operasional APJII. Evaluasi dan pembaruan JD dapat dilakukan secara berkala sesuai perkembangan kebutuhan operasional dan standar keamanan terbaru.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF

LAMPIRAN LIX
PERATURAN ASOSIASI PENYENGGARA JASA INTERNET INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PERUBAHAN ATAS PERATURAN ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA NOMOR 5 TAHUN 2024
TENTANG
PENGGUNAAN FASILITAS APJII

SOP PENYELENGGARAAN LAYANAN INTERNET EXCHANGE APJII

1. Pendahuluan

Dokumen ini menjelaskan Standar Operasional Prosedur (SOP) penyelenggaraan layanan Internet Exchange (IXP), khususnya IIX (Internet Exchange Indonesia). SOP ini berfungsi sebagai panduan resmi yang mengatur semua aspek layanan, mulai dari administrasi, operasi jaringan, penanganan insiden, hingga tata kelola (governance).

2. Tujuan

Tujuan SOP ini adalah:

2.5 Memberikan panduan yang jelas dan terstruktur terkait administrasi layanan dan operasi jaringan IIX.
2.6 Memastikan konsistensi dalam penanganan gangguan (insiden) dan respons keamanan.
2.7 Menjamin keandalan (reliability), skalabilitas (scalability), dan keamanan platform IIX.
2.8 Mendukung praktik terbaik (best practices) yang diadopsi dari IXP Internasional (AMS-IX, DE-CIX, LINX, Euro-IX, dan SGIX).

3. Definisi & Referensi Standar

Kategori	Deskripsi
IIX/IXP	Internet Exchange Point, platform yang memfasilitasi pertukaran traffic internet antar anggota (peer).
Referensi IXP	**AMS-IX, DE-CIX, LINX, Euro-IX, SGIX (Singapore Internet Exchange)**.
Standar & Protokol	BGP (Border Gateway Protocol), IRR (Internet Routing Registry), RPKI (Resource Public Key Infrastructure), L2 ACLs (Layer 2 Access Control Lists), RFC 9234 (ASPA Validation).

4. Definisi Istilah

Istilah	Definisi
Anggota/Member	Perusahaan atau entitas yang terhubung dan melakukan *peering* di IIX.
Route Server	Perangkat BGP yang memfasilitasi *multilateral peering* untuk efisiensi *peering*.
Flapping	Port jaringan yang berulang kali (lebih dari 3x dalam 5 detik) berubah status dari Up ke Down.
Prefix Leak	Kesalahan *propagasi* rute BGP di luar cakupan yang seharusnya atau yang disepakati.
Hijacking	Routing BGP secara tidak sah untuk mengalihkan *traffic*.
Spoofing	Memalsukan alamat IP sumber untuk tujuan penyerangan atau penyembunyian.
NMS	Network Management System, sistem pengendalian dan monitoring jaringan terpusat.
RCA	Root Caused Analysis, analisis penyebab utama suatu insiden.
RTBH	Remote Triggered Blackhole, teknik mitigasi DDoS menggunakan BGP *community*.
Soft block	Isolir/Disable Port
PKS	Perjanjian Kerja Sama
MoU	Nota kesepahaman/Memorandum of Understanding
Peering Agrreement	MLPA (Multilateral Peering Agreement), MLPA BLPA (Bilateral Peering Agreement)

5. Ruang Lingkup

SOP ini berlaku untuk semua personel dan pihak terkait yang bertanggung jawab atas penyelenggaraan, pengoperasian, pemeliharaan, dan tata kelola layanan IIX, termasuk:

5. Administrasi Layanan dan Anggota.
6. Operasi dan Monitoring Jaringan.
7. Penanganan Gangguan dan Keamanan Jaringan.
8. Manajemen Infrastruktur Fisik.

6. Prosedur Operasional Inti (Core SOP)

6.1 Administrasi Layanan

Prosedur	Detail Pelaksanaan
Permohonan, Perubahan, dan Pemutusan Layanan	Semua permintaan interkoneksi, *upgrade/downgrade* port, maupun penghentian layanan harus diajukan secara **resmi** melalui **formulir** (email/sistem online) dan disetujui Pengelola IIX.
Prosedur Isolasi/Staging Peering Baru	Anggota baru akan ditempatkan pada **jaringan isolasi** untuk **uji coba** sebelum masuk ke jaringan produksi/IXP.
Prosedur Alokasi IP IIX	Alamat IP dialokasikan berdasarkan **kebijakan *numbering plan* IXP**. Setiap anggota hanya diperbolehkan menggunakan IP yang diberikan.
Prosedur Alokasi Port IIX	Penentuan port dilakukan berdasarkan **ketersediaan kapasitas**, kebutuhan anggota, dan **perencanaan kapasitas jangka panjang**.
Prosedur Upgrade Port IIX	Port dapat di-*upgrade* dari 10G secara bertahap (2x10G, 40G/100G, Nx100G) jika utilisasi harian mencapai **70%** selama 7 hari berturut-turut.
Prosedur Penggunaan Aggregate Port	Untuk Port **10G** maksimal hanya sampai 2 x 10G. Jika lebih dari 20G, diarahkan ke 40G/100G. Port 100G tidak memiliki batasan agregasi saat ini.
Ketentuan untuk Pengguna Khusus	Pengguna dengan *outbound traffic* (kontribusi konten) dominan **1:5 (20%)** dapat terhubung ke IIX secara **gratis** (tidak dikenakan biaya *cross connect* 100G) dengan syarat memiliki PKS dengan APJII.

6.2 Penanganan Gangguan

Gangguan diklasifikasikan berdasarkan *severity* (dampak) dengan tindakan dan mitigasi yang berbeda:

Severity Level	Tindakan NOC (Network Operations Center)	Jenis Gangguan	Mitigasi yang Diterapkan
Low	Diberikan **Notifikasi** hingga Anggota melakukan perbaikan. Port akan diisolasi otomatis **minimal** 3x 24 jam dan akan dirilis	Broadcast Flood	Sistem akan mendeteksi dan membatasi *broadcast traffic* abnormal.
		Network/Port Flapping	Sistem akan mendeteksi dan membatasi Network/Port Flapping abnormal.

	setelah anggota memberikan RCA. Jika berulang, diisolasi **minimal 30 hari**.		
Medium	Dilakukan **Soft Block** dan akan dibuka kembali setelah Anggota melakukan perbaikan. Port akan diisolasi otomatis **minimal** 3x 24 jam dan akan dirilis setelah anggota memberikan RCA. Jika berulang, diisolasi **minimal 30 hari**.	Route/Prefix Leak	*Route server* melakukan **filtering IRR/RPKI** untuk mencegah *prefix leak*.
		Looping (L2/L3)	*Monitoring* akan mendeteksi anomali *looping* L2/L3.
High	Dilakukan **Shutdown Port** sampai dilakukan Rapat Klarifikasi.	Hijacking	**Validasi RPKI & IRR** digunakan untuk mencegah *prefix hijacking*.
		Spoofing	**Port security (L2 ACLs)** diterapkan untuk mengurangi *spoofing*.

6.3 Prosedur Pencegahan Gangguan

Prosedur	Detail Pencegahan dan Mitigasi
Isolasi Member Bermasalah	Anggota yang menyebabkan gangguan serius dapat **diisolasi sementara** hingga **shutdown port** sampai masalah terselesaikan.
Mitigasi Resource Availability	Jika traffic backbone antar switch sudah mencapai **80%**, maka wajib menambah kapasitas traffic antar backbone. Jika total port yang tersedia kurang dari **10%**, maka wajib menambah kapasitas infrastruktur.
Port Congestion (Anggota)	Diberikan **Surat Peringatan (SP)** secara bertahap kepada anggota yang menyebabkan *port congestion*: **SP1** (1 bulan), **SP2** (2 bulan), dan **SP3** (jika 3 bulan berturut-turut tidak ada aksi). Jika dalam jangka waktu 6 (enam) bulan tidak dilakukan upgrade, maka terhadap Port tersebut akan dilakukan soft block berdasarkan pemberitahuan terlebih dahulu dari NOC-APJII.

6.4 Monitoring & Pelaporan

Prosedur	Detail Pelaksanaan
Pengendalian Jaringan Terpusat	**NMS** memantau semua perangkat, port, dan trafik secara *real-time*. (Contoh *tools*: Observium).
Pencatatan & Pelaporan Rutin	Laporan mencakup: Jumlah anggota, port terpakai & tersedia, *traffic* per anggota, jumlah gangguan bulanan, laporan aset & inventori, laporan

	perubahan layanan, pencatatan insiden (hardware failure, Broadcast Flood, Network/Port Flapping, Route/Prefix Leak, Looping (L2/L3), Hijacking, Spoofing) dan syslog
Penanganan Port Congestion (Proaktif)	Surat Pemberitahuan dikirimkan dari NOC-APJII kepada Anggota yang pemakaian Port-nya telah melebihi **80%**.
	Anggota diberikan kesempatan *upgrade interface* selambat-lambatnya dalam jangka waktu **6 bulan**.
	Jika dalam 6 bulan tidak di-*upgrade*, dilakukan **soft block** berdasarkan pemberitahuan, diikuti oleh **pencabutan kabel** dari Port (untuk dimanfaatkan anggota lain).

7. Kebijakan Peering

Prosedur	Detail Pelaksanaan & Mitigasi Keamanan
Prosedur Bilateral Peering	Anggota dapat melakukan *bilateral peering* langsung antar-router dengan persetujuan kedua pihak (tanpa komunikasi melalui APJII).
Prosedur Multilateral Peering	Anggota dapat bergabung melalui **Route Server** untuk efisiensi *peering*.
Mitigasi Network Loops (Port Security)	Implementasi **Layer 2 Access Control Lists (L2 ACLs)** membatasi MAC address yang diizinkan pada port (hanya MAC address router Anggota).
Penanganan MAC Address Changes	Perubahan MAC address dapat dilakukan melalui **web portal** (direkomendasikan beberapa jam sebelumnya) atau kontak NOC IIX dalam keadaan darurat.
Port Flap Dampening	Jika port transisi Up/Down/Up lebih dari **tiga kali dalam lima detik**, port akan dinonaktifkan (*disabled*) dan diaktifkan kembali secara otomatis setelah sepuluh detik.

8. Infrastruktur & Perawatan

Prosedur	Detail Pelaksanaan
Perawatan Berkala	Perawatan berkala dilakukan setiap bulan, meliputi pembersihan, **update *firmware (jika diperlukan)***, dan pengecekan koneksi optik.
Manajemen Fasilitas Fisik	DC harus memiliki sistem **pendingin, UPS, dan generator cadangan** yang memadai.
Prosedur Pergantian Perangkat Rusak	Jika ada *switch/transceiver* rusak, harus diganti maksimal **4 jam** sejak insiden.
Hardware Lifecycle Policy	Perangkat diganti setiap **5 tahun** untuk menjamin keandalan operasional.
Spares & N+1 Plan	Tersedia *spare* **switch, transceiver, PSU, dan *linecard*** dengan spesifikasi yang sama (redundansi N+1).

Cross-Connect Policy	Semua koneksi ke IIX *fabric* harus melalui **patch panel resmi** sesuai standar.

9. Desain & BGP Policy

Prosedur	Detail Pelaksanaan
Topologi Jaringan IIX	Menggunakan **core-switch redundant** dengan distribusi ke *edge-switch*.
IXP Network Scalability	Kapasitas direncanakan untuk pertumbuhan **3-5 tahun**. Pengadaan *hardware* baru jika ketersediaan port tersisa kurang dari **10%**.
Redudansi & Failover	Semua jalur kritis memiliki **backup otomatis** (*failover*).
Peering Policy (Route Server)	*Default*: semua prefix **ditolak** kecuali yang **valid IRR/RPKI**.
BGP Community	Disediakan *community* standar untuk *control* (**blackhole, prepend, selective announce**).
Route/Prefix Filtering	Prefiks diverifikasi **max-length, IRR, dan RPKI**.
AS-SET	Setiap member wajib memiliki konfigurasi AS-SET.
Validasi IRR DB & Route Object	Semua prefix harus memiliki *route object* dan *as-set* yang valid.
Validasi ROA & RPKI	Prefix yang diumumkan harus **ROA valid**.
Prefix Limit	Setiap *member* wajib menetapkan batasan **max prefix** untuk mencegah *overload*. Wajib diisi saat mengisi form registrasi membership IIX.
PeeringDB	Anggota memiliki akun PeeringDB yang up to date.

10. Security & Abuse Handling

Prosedur	Detail Pelaksanaan
RTBH (Remote Triggered Blackhole)	Disediakan BGP *community* khusus untuk melakukan **blackhole prefix** yang diserang (DOS/DDoS *attack*).
Abuse Handling	Semua laporan *abuse* (*spam, malware, botnet*) diterima dan ditindaklanjuti oleh kontak **abuse-c**.
Traffic Policing	*Broadcast & unknown unicast flood* akan diberikan **rate-limit** untuk menjaga stabilitas jaringan.

11. Transparansi & Publikasi

- **Realtime Looking Glass:** Tersedia portal publik untuk pengecekan **routing & BGP session** secara *real-time*.
- **Publik Traffic Graph:** Statistik *traffic* IXP tersedia di **website resmi** untuk transparansi.

12. Governance (Tata Kelola)

Prosedur	Detail Pelaksanaan
Change Management Procedure	Semua perubahan jaringan (*maintenance, upgrade*) harus melalui proses **Change Request (CR)** terstruktur.
Incident Management Framework	Insiden dikategorikan berdasarkan *severity*, dilaporkan dengan detail, dan disertai **RCA (Root Cause Analysis)**.
Disaster Recovery Plan (DRP)	Prosedur pemulihan layanan (termasuk *failover* infrastruktur) jika terjadi **bencana besar**.
Business Continuity Plan (BCP)	Menjamin ketersediaan layanan (*waktu aktif*) meskipun ada gangguan signifikan pada infrastruktur utama.
Membership Agreement & SLA	Kontrak resmi berisi hak & kewajiban anggota, termasuk **SLA (Service Level Agreement)** terkait platform ketersediaan layanan.

13. Penutup

Dokumen Standar Operasional Prosedur (SOP) ini merupakan panduan wajib bagi seluruh personel NOC/Operasi IIX dan seluruh Anggota/Tenant yang terhubung dengan platform IIX.

Kepatuhan terhadap semua prosedur, kebijakan routing, dan ketentuan keamanan yang tercantum dalam dokumen ini adalah **mandatory** untuk menjaga stabilitas, keamanan, dan keandalan layanan *Internet Exchange*.

SOP ini akan **ditinjau dan diperbarui secara berkala** (minimal setiap tahun) atau sewaktu-waktu jika terjadi perubahan signifikan pada teknologi, regulasi, atau kebutuhan operasional. Dengan demikian, semua pihak diwajibkan untuk selalu mengacu pada versi dokumen yang paling terakhir.

Disahkan di Jakarta
pada tanggal 25 Maret 2026

KETUA UMUM
ASOSIASI PENYELENGGARA JASA
INTERNET INDONESIA,

ttd.

MUHAMMAD ARIF