RFC 2350 Telkom CSIRT

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi Telkom CSIRT berdasarkan RFC 2350, yaitu informasi dasar mengenai Telkom CSIRT, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi Telkom CSIRT.

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 21 Juli 2026.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt.telkom.co.id/rfc2350 (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen telah ditanda tangani secara digital oleh pejabat yang berwenang.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 Telkom CSIRT;
Versi	: 1.1;
Tanggal Publikasi	: 21 Juli 2026;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Telkom Computer Security Incident Response Team
Disingkat : Telkom CSIRT

2.2. Alamat

Gedung Grha Merah Putih lantai 2
Jl. Jenderal Gatot Subroto Kav. 52
Kuningan Barat, Mampang Prapatan
Jakarta Selatan 12710

2.3. Zona Waktu

Jakarta, Indonesia (GMT+07:00)

2.4. Nomor Telepon

+62-21-3020-5885

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

-

2.7. Alamat Surat Elektronik (*E-mail*)

csirt[at]telkom[dot]co[dot]id

2.8. Kunci Publik (*Public Key*) dan Informasi/Data Enkripsi lain

File PGP *key* ini tersedia pada :
https://csirt.telkom.co.id/publickey.asc

2.9. Anggota Tim

Ketua Telkom CSIRT adalah Koordinator Telkom CSIRT dan dibantu oleh Sekretaris Telkom CSIRT serta anggota tim dari bidang Security Operation Center (SOC), Legal, Regulasi, Komunikasi & Public Relation, IT & Infrastruktur, dan bidang Produk & Layanan.

2.10. Informasi/Data lain

-

2.11. Catatan-catatan pada Kontak Telkom CSIRT

Metode yang disarankan untuk menghubungi Telkom CSIRT adalah melalui *e-mail* pada alamat csirt[at]telkom[dot]co[dot]id atau melalui nomor telepon +62 (021) 3020-5885.

3. Mengenai Telkom CSIRT

3.1. Visi

Terwujudnya pengelolaan sistem keamanan informasi dengan baik untuk melindungi aset informasi yang dimiliki oleh Telkom Indonesia.

3.2. Misi

Misi dari Telkom CSIRT yaitu :

a. Mengoordinasikan pencegahan, penanggulangan, dan pemulihan insiden keamanan siber di lingkungan Telkom Indonesia.
b. Membangun kerja sama dengan pihak terkait, baik internal maupun eksternal, dalam rangka peningkatan pengamanan siber.
c. Meningkatkan kapasitas sumber daya manusia terhadap ancaman keamanan siber melalui proses pembelajaran dan peningkatan kualitas yang berkelanjutan.

3.3. Konstituen

Konstituen Telkom CSIRT meliputi internal PT Telkom Indonesia (Persero) Tbk.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan Telkom CSIRT bersumber dari anggaran perusahaan.

3.5. Otoritas

Telkom CSIRT memiliki kewenangan dengan konstituennya dalam penanganan gangguan keamanan siber, mitigasi, dan investigasi insiden keamanan siber di lingkungan perusahaan. Telkom CSIRT dapat berkoordinasi serta bekerja sama dengan pihak lain yang mempunyai kompetensi untuk penanganan insiden siber.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/*Level* Dukungan

Telkom CSIRT melayani penanganan insiden siber dengan jenis antara lain:

a. Web Defacement
b. DDoS
c. Malware
d. Ransomware
e. Phishing

Dukungan yang diberikan oleh Telkom CSIRT kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Telkom CSIRT akan melakukan kerja sama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh Telkom CSIRT akan dirahasiakan sesuai klasifikasi informasi dan ketentuan yang berlaku.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi bersifat biasa dapat menggunakan e-mail csirt[at]telkom[dot]co[dot]id dan telepon +62 (021) 3020-5885. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan email terenkripsi dengan kunci publik Telkom CSIRT (subbab 2.8).

5. Layanan

5.1. Layanan Utama

Layanan utama dari Telkom CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini akan dilaksanakan oleh Telkom CSIRT yang berupa peringatan akan adanya ancaman siber kepada pemilik/penyelenggara sistem elektronik.

5.1.2. Penanganan Insiden Siber

Layanan penanganan insiden siber mencakup siklus penuh penanganan insiden. Penanganan dapat dilaksanakan dengan on-site secara langsung atau pemberian saran penanganan untuk ditindaklanjuti.

5.1.3. Penerimaan Aduan Insiden Siber

Layanan aduan insiden siber dapat disampaikan melalui kanal komunikasi Telkom CSIRT sesuai dengan informasi pada bab 2.

5.2. Layanan Tambahan

Layanan tambahan dari Telkom CSIRT yaitu :

5.2.1. Pemberitahuan hasil pengamatan potensi ancaman

Layanan ini berupa penyampaian informasi hasil pengamatan mengenai potensi ancaman keamanan siber yang dapat berdampak terhadap PT Telkom Indonesia (Persero) Tbk.

5.2.2. Pendeteksian serangan

Layanan ini berupa kegiatan identifikasi dan pendeteksian indikasi serangan siber terhadap sistem dan aset informasi PT Telkom Indonesia (Persero) Tbk.

5.2.3. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini berupa penyelenggaraan sosialisasi security awareness di lingkungan PT Telkom Indonesia (Persero) Tbk.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt[at]telkom[dot]co[dot]id dengan melampirkan sekurang-kurangnya kontak yang dapat dihubungi dan bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan, atau sesuai dengan ketentuan lain yang berlaku.

7. *Disclaimer*

a. Telkom CSIRT melaksanakan kegiatan tanggap insiden dengan menerapkan prinsip kerahasiaan sebagai prinsip kerja, pembagian informasi ke para pihak akan dilakukan dengan menerapkan prinsip *need-to-know*.

b. Telkom CSIRT hanya menyediakan sarana komunikasi melalui kanal yang tercantum pada RFC2350, kami tidak bertanggung jawab atas komunikasi yang mengatasnamakan Telkom CSIRT melalui kanal lain.