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 1.0 yang diterbitkan pada tanggal 21 Agustus 2023.

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-Telkom-CSIRT.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen ini telah ditandatangani dengan PGP *Key* milik Telkom CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen ini memiliki atribut:

Judul	: RFC 2350 Telkom CSIRT;
Versi	: 1.0;
Tanggal Publikasi	: 21 Agustus 2023;
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 Graha Merah Putih lantai 2
Jl. Jenderal Gatot Subroto Kav. 52
Kuningan Barat, Mampang Prapatan
Jakarta Selatan 12710

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 3020-5885

2.5. Nomor Fax

N/A

2.6. Telekomunikasi Lain

N/A

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* Telkom CSIRT tersedia pada:
https://csirt.telkom.co.id/publickey.asc

Signature dari file ini tersedia pada:
https://csirt.telkom.co.id/RFC2350-Telkom-CSIRT.pdf.sig

2.9. Anggota Tim

Ketua Telkom CSIRT adalah *Operational Vice President Cyber Security* Direktorat *Network & IT Solution* yang menjabat sebagai Koordinator CSIRT, dengan anggota tim meliputi bidang *Security Operation Center* (SOC), Legal, Regulasi, Komunikasi & *Public Relation*, IT & Infrastruktur, dan bidang Layanan & Produk.

2.10. Informasi/Data lain

N/A

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 nomor telepon (021) 3020-5885.

3. Mengenai Telkom CSIRT

3.1. Visi

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

3.2. Misi

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 adalah internal Telkom Indonesia.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan Telkom CSIRT bersumber dari anggaran perusahaan.

3.5. Otoritas

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

4. Kebijakan – Kebijakan

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

Telkom CSIRT melayani penanganan insiden siber dengan jenis sebagai berikut, namun tidak terbatas pada:

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

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

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.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi bersifat biasa dapat menggunakan e-mail tanpa enkripsi data khusus (e-mail konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada e-mail atau lampiran email.

5. Layanan

5.1. Layanan Utama

Layanan utama dari Telkom CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh Telkom CSIRT 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.

5.2. Layanan Tambahan

Layanan tambahan dari Telkom CSIRT yaitu :

5.2.1. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini dilaksanakan oleh Telkom CSIRT berupa penyelenggaraan sosialisasi *security awareness* di lingkungan Telkom Indonesia.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt[at]telkom[dot]co[dot]id dengan melampirkan sekurang-kurangnya: *file log*, *timestamp*, *screenshot*, nama pelapor, dan nomor telepon pelapor.

7. *Disclaimer*

7.1. 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*.

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