RFC 2350 SCI-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 02 Maret 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://www.sucofindo.co.id/sci-csirt/

1.4. Keaslian Dokumen

Dokumen telah ditanda tangani oleh Ketua SCI-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 SCI-CSIRT;
Versi : 1.0;
Tanggal Publikasi : 2 Maret 2026;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

PERUSAHAAN PERSEORAN (PERSERO) PT SUPERINTENDING COMPANY OF INDONESIA atau disingkat PT SUCOFINDO (PERSERO)– Computer Security Incident Response Team
Disingkat : SCI – CSIRT

2.2. Alamat

Graha Sucofindo Lt. 5 (Divisi Teknologi Informasi), KH. Guru Amin No.Kav. 34, RT.4/RW.1, Pancoran, Kec. Pancoran, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta, 12780

2.3. Zona Waktu

Indonesia – Jakarta (GMT+7)

2.4. Nomor Telepon

(021) 798 3666 Ext. 1527

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

N/A.

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

csirt[at]sucofindo[dot]co[dot]id

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

---

File PGP key ini tersedia pada:
https://www.sucofindo.co.id/sci-csirt/

2.9. Anggota Tim

Ketua SCI-CSIRT adalah Kepala Divisi Teknologi Informasi (TI)
Yang termasuk anggota tim adalah :

- Kepala Bagian Operasional dan Pemeliharaan
- Kepala Bagian Perencanaan dan Tata Kelola
- Kepala Bagian Dukungan Operasi dan Solusi Bisnis
- IT Governance
- IT Architect
- IT Development Specialist
- IT System Analyst
- IT System Specialist
- IT Operation Officer
- Kepala Unit Kerja selain Kepala Divisi TI

2.10. Informasi/Data lain

N/A.

2.11. Catatan-catatan pada Kontak SCI-CSIRT

Metode yang disarankan untuk menghubungi SCI-CSIRT adalah melalui *e-mail* pada alamat csirt@sucofindo.co.id atau melalui nomor telepon yang tercantum pada Informasi Data/Kontak. Pada hari Senin-Jumat pada pukul 08.00-17.00 WIB.

3. Mengenai SCI-CSIRT

3.1. Visi

Visi SCI-CSIRT adalah menjadi komponen utama untuk tercapainya Visi Perusahaan dengan meningkatkan ketahanan siber di sektor inspeksi, pengujian, sertifikasi, konsultasi, dan pelatihan.

3.2. Misi

Perwujudan visi sebagaimana dituangkan di atas akan dicapai melalui upaya- upaya yang terkandung dalam misi SCI-CSIRT, yaitu :

a. Mengkoordinasikan dan mengkolaborasikan layanan keamanan siber di lingkungan Perusahaan dan pemangku kepentingan;
b. Membangun kemampuan dan kapasitas sumber daya keamanan di sektor inspeksi, pengujian, sertifikasi, konsultasi, dan pelatihan;
c. Membangun kerjasama dalam rangka penanggulangan dan pemulihan insiden keamanan siber di lingkungan inspeksi, pengujian, sertifikasi, konsultasi, dan pelatihan.

3.3. Konstituen

Konstituen SCI-CSIRT meliputi seluruh pengguna layanan sistem elektronik PT SUCOFINDO (Persero).

3.4. Sponsorship dan/atau Afiliasi

Pendanaan SCI-CSIRT bersumber dari anggaran pendapatan Perusahaan.

3.5. Otoritas

Berdasarkan Kebijakan Pengelolaan Sistem dan Teknologi Informasi dan Kebijakan Pengelolaan Keamanan Informasi, SCI-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi, dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada sektor inspeksi, pengujian, sertifikasi, konsultasi, dan pelatihan.

4. Kebijakan – Kebijakan

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

SCI-CSIRT memiliki otoritas untuk menangani insiden yaitu :

a. Web Defacement;
b. DDOS;
c. Malware;
d. Phising;

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

SCI-CSIRT akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh SCI-CSIRT Indonesia akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa SCI-CSIRT Indonesia dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada e-mail.

5. Layanan

5.1. Layanan Utama

Layanan utama dari SCI-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh SCI-CSIRT berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik terkait layanan ini diberikan oleh konstituen.

5.1.2. Penanggulangan dan Pemulihan Insiden Siber

Layanan ini diberikan berupa kegiatan menghentikan serangan dan memulihkan sistem agar berfungsi normal yang meliputi proses identifikasi, isolasi, perbaikan, dan pemulihan data.

5.2. Layanan Tambahan

Layanan tambahan dari SCI-CSIRT yaitu :

5.2.1. Penanganan Informasi Insiden Siber kepada Pihak Terkait

Layanan ini meliputi penyampaian informasi insiden secara tepat kepada pihak internal maupun eksternal yang berwenang, agar koordinasi penanggulangan dapat berjalan efektif.

5.2.2. Diseminasi Informasi untuk Mencegah dan/atau Mengurangi Dampak dari Insiden

Layanan ini membagikan informasi insiden untuk meningkatkan kesadaran, mengurangi risiko serangan serupa, dan mendukung pencegahan serta mitigasi dampak secara lebih luas.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt[at]sucofindo[dot]co[dot]id dengan melampirkan Formulir Aduan Insiden Siber yang sekurang-kurangnya memuat :

a. Identitas Pelapor;
b. Tipe Laporan;
c. Waktu Terjadinya Insiden;
d. Tipe Insiden;
e. Deskripsi Insiden disertai Bukti (screenshoot, domain name, URL, email dll).
f. Atau sesuai dengan ketentuan lain yang berlaku

7. *Disclaimer*

Tim SCI-CSIRT memiliki beberapa tools untuk menghindari malware antara lain :

a. Melakukan asesmen tingkat risiko dan dampak keamanan informasi terkait potensi insiden dan saat insiden terjadi;
b. Melakukan asesmen tingkat keamanan sistem informasi yang dibuat secara sendiri (in-house), atau disewa/dibeli ke pihak ketiga;

c. Melakukan pengawasan serta intervensi aktif terhadap operasional sistem informasi dalam rangka pemenuhan ketahanan dan keandalan siber yang menunjang tujuan bisnis;
d. Merencanakan, membuat dan mengoperasikan rancang bangun mekanisme pertahanan berlapis siber (cyber defense-in-depth);
e. Melaksanakan program kesadaran keamanan siber bersama stakeholder terkait;
f. Memiliki otoritas penuh untuk melaksanakan koordinasi dan intervensi internal dan eksternal, akses terhadap data dan sistem dalam hal penanganan insiden siber Anti – Malware.