RFC 2350 SKBF-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal *Update* Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 06 Agustus 2026.

1.2. Daftar Distribusi untuk Pemberitahuan

Pihak – pihak yang menjadi penerima distribusi pemberitahuan CSIRT adalah seluruh divisi dan departemen yang ada di PT Sunindo Kookmin Best Finance.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://www.skbf.co.id/others/rfc2350.pdf

1.4. Keaslian Dokumen

Dokumen ini telah ditandatangani oleh Direktur Utama PT Sunindo Kookmin Best Finance.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 SKBF-CSIRT;
Versi	: 1.0;
Tanggal Publikasi	: 06 Agustus 2026;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Sunindo Kookmin Best Finance-*Computer Security Incident Response Team*
Disingkat : SKBF-CSIRT.

2.2. Alamat

Sahid Sudirman Center, Lantai 50, unit A & E. Jl Jenderal Sudirman Kav. 86 Jakarta Pusat. 10220.

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 22535098 ext 311

2.5. Nomor Fax

–

2.6. Telekomunikasi Lain

–

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

csirt@skbf.co.id

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

-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEah+XVhYJKwYBBAHaRw8BAQdA4RD4hVRy0NEzWa7U2/NnAuMIx5p9PwqBz4Ur
BoyGHG20OEJhbWJhbmcgTXVoYW1tYWQgU3lhZmlpIChubykgPGJhbWJhbmcuc3lh
ZmlpQHNrYmYuY28uaWQ+iLUEExYKAF0WIQSOkhUAFpBZNPWN3vUC/EDZSaI7iQUC
ah+XVhsUgAAAAAAEAA5tYW51MiwyLjUrMS4xMiwyLDECGwMFCQWjmoAFCwkIBwIC
IgIGFQoJCAsCBBYCAwECHgcCF4AACgkQAvxA2UmiO4mvjAEA6C2TgfkF88DxCMPF
KfOLlidFCTzU1H9mzxdapFyiHwcA/iAPw6D2jZlxqdpPvFnTAPHPFf1iL3WkEj5W
Cgi/eLMAuDgEah+XVhIKKwYBBAGXVQEFAQEHQIvbre/LlDoEMQhQSBQdJ4U0s74i
zt0vDuzBdcGj0m8JAwEIB4iaBBgWCgBCFiEEjpIVABaQWTT1jd71AvxA2UmiO4kF
AmofI1YbFIAAAAAABAAObWFudTIsMi41KzEuMTIsMiwxAhsMBQkFo5qAAAoJEAL8
QNlJojuJXEgBAKZHUycWJNJpE1mTlPZQBX9gJUautEsrovK0AhW82TK6AQCyCqJY
uNOz6/tjaVdJ8gcks3u6+F5UhkHvh2c5GQ22CA==
=igfQ
-----END PGP PUBLIC KEY BLOCK-----

2.9. Anggota Tim

Ketua SKBF-CSIRT dijabat oleh Kepala Departemen Teknologi Informasi PT Sunindo Kookmin Best Finance. Untuk anggota tim merujuk kepada Surat Keputusan PT Sunindo Kookmin Best Finance Nomor SK KEB.001-COM-SKBF Tentang Tim Tanggap Insiden Siber (TTIS) / *Computer Security Incident Response Team (CSIRT)*.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak SKBF-CSIRT

Metode yang disarankan untuk menghubungi SKBF-CSIRT adalah melalui *e-mail* pada alamat csirt@skbf.co.id.

3. Mengenai SKBF-CSIRT

3.1. Visi

Visi SKBF-CSIRT adalah terwujudnya ketahanan siber yang andal dan professional di lingkungan PT Sunindo Kookmin Best Finance.

3.2. Misi

Misi dari SKBF-CSIRT, yaitu :

a. Membangun kemampuan dalam ketahanan keamanan siber.
b. Menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan, penanggulangan dan pemulihan terhadap ancaman siber.
c. Menyediakan mekanisme penanggulangan insiden dan/atau pemulihan insiden yang dilakukan oleh tim penanggulangan dan pemulihan insiden siber.

3.3. Konstituen

Konstituen SKBF-CSIRT meliputi seluruh unit kerja pengguna teknologi informasi di lingkungan PT Sunindo Kookmin Best Finance.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan SKBF-CSIRT bersumber dari anggaran perusahaan PT Sunindo Kookmin Best Finance.

3.5. Otoritas

SKBF-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden keamanan siber, investigasi dan analisis dampak insiden, serta pelaksanaan kegiatan pemulihan pasca-insiden di lingkungan PT Sunindo Kookmin Best Finance. Selain itu, SKBF-CSIRT bertanggung jawab untuk melakukan koordinasi dan pelaporan kepada Badan Siber dan Sandi Negara (BSSN) selaku *Government Computer Security Incident Response Team* (Gov-CSIRT) dalam rangka penanganan insiden keamanan siber.

4. Kebijakan – Kebijakan

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

Dukungan yang diberikan oleh SKBF-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden seperti dibawah ini namun tidak terbatas pada:

a. *Denial Of Services (DOS) / Distributed Denial Of Services (DDOS)*
b. *Malware*
c. *Phishing*
d. *Compromised Information*
e. *Unauthorized Activity*
f. *Compromised Asset*

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

SKBF-CSIRT akan melakukan kerja sama dan berbagi informasi dengan tim CSIRT/TTIS atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diberikan dan diterima oleh SKBF-CSIRT harus dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, SKBF-CSIRT dapat menggunakan alamat email tanpa enkripsi data (email konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi pada email, data atau jalur komunikasi lainnya.

5. Layanan

5.1. Layanan Utama

Layanan utama dari SKBF-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh SKBF-CSIRT berupa memastikan kebenaran insiden dan pelaporan, menilai dampak dan prioritas insiden.

5.1.2. Penanganan Insiden Siber

Layanan ini dilaksanakan oleh SKBF-CRIST berupa analisis, rekomendasi teknis dan koordinasi kepada Badan Siber dan Sandi Negara (BSSN) selaku Government Computer Security Incident Response Team (Gov-CSIRT), serta pihak yang berkepentingan dalam rangka penganggulangan dan pemulihan insiden siber.

5.2. Layanan Tambahan

Layanan tambahan dari SKBF-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

SKBF-CSIRT melaksanakan analisis, koordinasi dan /atau rekomendasi teknis yang dilakukan secara berkala dalam rangka perbaikan keamanan sistem informasi.

5.2.2. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini dilaksanakan oleh SKBF-CSIRT berupa monitoring dan komunikasi secara berkala atas asset-aset milik perusahaan terhadap adanya potensi ancaman siber.

5.2.3. Pendeteksian Serangan

Menganalisa data untuk mendeteksi adanya serangan terhadap sistem elektronik atau aktivitas yang mencurigakan terhadap sistem elektronik atau pelanggaran terhadap keamanan siber.

5.2.4. Analisis Risiko Keamanan Siber

Mengidentifikasi dan menilai risiko keamanan siber serta merekomendasikan langkah –langkah tindak lanjut untuk menghadapi risiko tersebut.

5.2.5. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Memberikan pelatihan, pemahaman, dan cara yang perlu dilaksanakan dalam rangka membantu penanganan insiden siber.

5.2.6. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Melaksanakan kegiatan meningkatkan kesadaran dan kepedulian pengguna sistem informasi terhadap keamanan sistem/siber dengan cara sosialisasi/pelatihan kepada Konstituen terkait.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@skbf.co.id dengan melampirkan sekurang-kurangnya :

a. Foto/*scan* kartu identitas
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
c. Atau sesuai dengan ketentuan lain yang berlaku

7. *Disclaimer*

- Seluruh penanganan insiden siber bergantung pada ketersediaan tools dan sumber daya terkait yang dimiliki oleh SKBF-CSIRT.
- Waktu penyelesaian insiden siber bervariasi sesuai dengan kondisi situasional terhadap insiden yang dihadapi.