RFC 2350 SumselProv-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 20 Januari 2025.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

1.3. Lokasi dimana Dokumen bisa didapatkan

Versi terbaru dari dokumen ini tersedia pada :

https://csirt.sumselprov.go.id/rfc2350.pdf (versi bahasa indonesia)

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP key milik SumselProv-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8

1.5. Indentifikasi Dokumen

Dokumen ini memiliki atribut yaitu :

Judul	:	RFC 2350 SumselProv-CSIRT
Versi	:	1.1
Tanggal Publikasi	:	20 Januari 2025
Kadaluarsa	:	Dokumen ini valid hingga dokumen terbaru dipublikasikan

2. Informasi Data/Kontak

2.1. Nama Tim

Tim Respon Tanggap Insiden Keamanan Komputer/Siber Pemerintah Provinsi Sumatera Selatan (*Computer Security Incident ResponseTeam)* Provinsi Sumatera Selatan yang selanjutnya disebut SumselProv-CSIRT.

2.2. Alamat

Dinas Komunikasi Informatika Provinsi Sumatera Selatan,

Jalan Merdeka No.10 Palembang

2.3. Zona Waktu

Palembang (GMT+07:00)

2.4. Nomor Telepon
(+62) 0711 363480

2.5. Nomor Fax
(+62) 0711 363480

2.6. Telekomunikasi Lain

Tidak ada

2.7. Alamat Surat Elektronik (E-mail)
csirt[at]sumselprov.go.id

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

-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: User ID: csirt <csirt[at]sumselprov.go.id>
Comment: Valid from: 19/12/2024 10:35
Comment: Type: 255-bit EdDSA (secret key available)
Comment: Usage: Signing, Encryption, Certifying User IDs, SSH Authentication
Comment: Fingerprint: 28C1AAA25117679B3FE50994975B4EFBA96D1A11

mDMEZ2OUjBYJKwYBBAHaRw8BAQdADyCiJWm5HfywiBOT9zvPL6HGYtf3
WMOd1q8ji48+1py0HmNzaXJ0IDxjc2lydEBzdW1zZWxwcm92LmdvLmlkPoiTB
BMWCgA7FiEEKMGqolEXZ5s/5QmUl1tO+6ltGhEFAmdjlIwCGyMFCwkIBwICI
gIGFQoJCAsCBBYCAwECHgcCF4AACgkQl1tO+6ltGhE1VgEA1ywk/JBDFw5c/
k+drLg2ipYFojlQzwf6x6qU8jBD+XgA/iCE5Bx59y9TrCLM0pOPQsBSEj0HQL+7
VJVESSbNSAoIuDgEZ2OUjBIKKwYBBAGXVQEFAQEHQGXEDC3goAtV6eg0
EImIldeSXYIOYkYweFHAsLFSStVcAwEIB4h4BBgWCgAgFiEEKMGqolEXZ5s/
5QmUl1tO+6ltGhEFAmdjlIwCGwwACgkQl1tO+6ltGhFLyAD+NaCzPYXRGt2hF
1iT7z5xd8Lu5ZSPTtJRJWVbjdSxal4BAKT7LTn08ANB/bvPcHPdKiLAh42hdJO7
BDHL+TInKrwE=EKw5
-----END PGP PUBLIC KEY BLOCK-----

File *pgp key* ini tersedia pada :
https://csirt.sumselprov.go.id/publickey.asc

2.9. Anggota Tim

Koordinator SumselProv-CSIRT adalah Sekretaris Daerah Provinsi Sumatera Selatan, Ketua SumselProv-CSIRT adalah Kepala Dinas Komunikasi Informatika Provinsi Sumatera Selatan, Sekretaris SumselProv-CSIRT adalah Kepala Bidang TIK dan Persandian, Anggota Tim terdiri dari Dinas Komunikasi dan Informatika Provinsi Sumatera Selatan yang menangani insiden siber / teknologi informasi dan Perangkat Daerah Provinsi Sumatera Selatan sebagai agen siber.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak SumselProv-CSIRT

Metode yang disarankan untuk menghubungi SumselProv-CSIRT adalah melalui e-mail pada alamat csirt[at]sumselprov.go.id atau melalui nomor telepon (0711) 363480 selama jam kerja.

3. Mengenai SumselProv-CSIRT

3.1. Visi

Visi SumselProv-CSIRT adalah terwujudnya ketahanan siber di lingkungan Pemerintah Provinsi Sumatera Selatan yang handal dan profesional.

3.2. Misi

Tujuan dari SumselProv-CSIRT, yaitu :

a. Membangun pusat pencatatan, pelaporan dan penanggulangan insiden keamanan informasi di lingkungan Pemerintah Provinsi Sumatera Selatan;

b. Membangun kapasitas Sumber Daya Keamanan Siber di Pemerintah Provinsi Sumatera Selatan.

3.3. Konstituen

Konstituen SumselProv-CSIRT meliputi Perangkat Daerah di lingkungan Pemerintah Provinsi Sumatera Selatan yang menggunakan layanan Data Center Provinsi Sumatera Selatan.

3.4. Sponsorship dan/atau Afiliasi

SumselProv-CSIRT merupakan bagian dari Pemerintah Provinsi Sumatera Selatan sehingga seluruh pembiayaan bersumber dari APBD Provinsi Sumatera Selatan.

3.5. Otoritas

SumselProv-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber di lingkungan Pemerintah Provinsi Sumatera Selatan.

SumselProv-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya dan dapat berkoordinasi dengan BSSN / Pihak lainnya untuk insiden yang tidak dapat ditangani.

4. Kebijakan – Kebijakan

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

SumselProv-CSIRT memiliki otoritas untuk menangani insiden yaitu :

a. Web Defacement;

b. DDOS;

c. Malware;

d. Phising.

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

4.2. Kerja sama, Interaksi dan Penggungkapan Informasi / Data

SumselProv-CSIRT akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber.

Seluruh informasi yang diterima oleh SumselProv-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, SumselProv-CSIRT dapat menggunakan alamat email tanpa enkripsi data (email konvensional) dan telepon. Namun, untuk komunikasi yang membuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada email.

5. Layanan

5.1. Layanan Reaktif

Layanan reaktif dari SumselProv-CSIRT merupakan layanan utama dan bersifat prioritas yaitu :

5.1.1 Layanan pemberian peringatan terkait dengan laporan insiden siber

Layanan ini dilaksanakan berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik terkait layanan.

5.1.2 Layanan penanggulangan dan pemulihan Insiden

Layanan ini diberikan berupa koordinasi, analisis, rekomendasi teknis, dan bantuan *on-site* dalam rangka penanggulangan dan pemulihan insiden siber.

5.1.3 Layanan penanganan kerawanan

Layanan ini diberikan berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (*hardening*), layanan ini hanya berlaku apabila syarat-syarat berikut terpenuhi :

a. Pelapor atas kerawanan adalah pemilik sistem elektronik. Jika pelapor adalah bukan pemilik sistem, maka laporan kerawanannya tidak dapat ditangani;
b. Layanan penanganan kerawanan yang dimaksud dapat juga merupakan tindak lanjut atas kegiatan Vulnerability Assessment.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt[at]sumselprov.go.id dengan melampirkan sekurang kurangnya :

a. Foto/Scan kartu identitas;

b. Bukti insiden berupa foto atau screenshoot atau log file yang ditemukan.

7. Disclaimer

Tidak ada