RFC 2350 BPS-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 01 Oktober 2021.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan pembaruan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt.bps.go.id/assets/rfc2350/rfc2350-id.pdf (versi Bahasa Indonesia)
https://csirt.bps.go.id/assets/rfc2350/rfc2350-en.pdf (versi Bahasa Inggris)

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP *Key* milik BPS-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 BPS-CSIRT;
Versi	: 1.0;
Tanggal Publikasi	: 01 Oktober 2021;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Badan Pusat Statistik - Computer Security Incident Response Team
Disingkat : BPS - CSIRT.

2.2. Alamat

Badan Pusat Statistik
Jl. Dr. Sutomo 6-8 Jakarta

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 3519746

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

(021) 3841195, (021) 3842508, (021) 3810291 Ext 3320

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

csirt[at]bps.go.id

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

File PGP *key* ini tersedia pada :
https://csirt.bps.go.id/assets/bps-csirt.asc

2.9. Anggota Tim

Ketua BPS-CSIRT adalah Direktur Sistem Informasi Statistik. Yang termasuk anggota tim adalah Pejabat Fungsional pada Direktorat Sistem Informasi Statistik.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak BPS-CSIRT

Metode yang disarankan untuk menghubungi BPS-CSIRT adalah melalui *e-mail* pada alamat csirt[at]bps[dot]go[dot]id atau melalui nomor telepon (021) 3519746 pada hari kerja jam 08.00 - 16.00.

3. Mengenai Gov-CSIRT

3.1. Visi

Terwujudnya keamanan siber dalam mendukung layanan TI berkualitas untuk BPS, dalam mewujudkan Indonesia Maju

3.2. Misi

Misi dari BPS-CSIRT, yaitu :

1. Melaksanakan kegiatan pengamanan siber terhadap layanan TI.
2. Meningkatkan kapasitas sumber daya pada aspek pencegahan, penanggulangan dan pemulihan insiden keamanan siber.
3. Membangun kesadaran terhadap ancaman keamanan siber pada pengguna layanan TI

3.3. Konstituen

Konstituen BPS-CSIRT yaitu pengguna layanan TI di lingkungan Badan Pusat Statistik

3.4. Sponsorship dan/atau Afiliasi

BPS-CSIRT merupakan bagian dari Direktorat Sistem Informasi Statistik sehingga seluruh pembiayaannya bersumber dari APBN.

3.5. Otoritas

BPS-CSIRT memiliki kewenangan dengan konstituennya dalam penanganan gangguan keamanan siber. BPS-CSIRT dapat berkoordinasi serta bekerjasama dengan pihak lain yang mempunyai kompetensi untuk insiden yang tidak dapat ditangani.

4. Kebijakan – Kebijakan

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

BPS-CSIRT melayani penanganan insiden siber dengan jenis berikut :

a. Web Defacement;
b. DDoS;
c. Malware;
d. Phising;
e. Spamming.

Dukungan yang diberikan oleh BPS-CSIRT kepada konstituen dapat bervariasi bergantung pada jenis dan dampak insiden. Layanan penanganan insiden berdasarkan pada laporan konstituen.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

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

5. Layanan

5.1. Layanan Utama

Layanan utama dari BPS-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

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

5.1.2. Penanganan Insiden Siber

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

5.2. Layanan Tambahan

Layanan tambahan dari BPS-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (*hardening*).

5.2.2. Penanganan Artefak Digital

Layanan ini berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Pemberitahuan hasil pengamatan terkait dengan potensi ancaman baru yang mungkin terjadi.

5.2.4. Pendeteksian Serangan

Melakukan pendeteksian terhadap berbagai serangan yang terjadi dan di pantau melalui sistem deteksi dan monitoring keamanan

5.2.5. Analisis Risiko Keamanan Siber

Layanan ini berupa identifikasi kerentanan dan penilaian risiko kerentanan yang di temukan. Selanjutnya di berikan rekomendasi yang dapat dilakukan untuk mengurangi risiko tersebut.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Pemberian konsultasi terkait kesiapan penanggulangan dan pemulihan insiden keamanan siber.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Sosialisasi dan pembinaan kepada seluruh pegawai di lingkungan BPS yang bertujuan untuk meningkatkan kesadaran dan kepedulian para pegawai tentang keamanan siber.

6. Pelaporan Insiden

Laporan dapat dikirim melalui email csirt[at]bps[dot]go[dot]id atau melalui website csirt.bps.go.id dengan melampirkan : *logfile, timestamp, screenshot*, nama pelapor, nomor telepon.

7. *Disclaimer*

- Sampai saat ini BPS - CSIRT hanya merespon dan menangani insiden keamanan siber yang terjadi pada perangkat kerja yang bersifat dinas;
- Terkait penanganan insiden jenis *malware* tergantung pada ketersediaan *tools* yang dimiliki.