# 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 2.0 yang diterbitkan pada tanggal 16 Desember 2024.

### 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

### 1.4. Keaslian Dokumen

Dokumen ini 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 | : 2.0; |
| Tanggal Publikasi | : 16 Desember 2024; |
| Kedaluwarsa | : Dokumen ini valid hingga dokumen terbaru dipublikasikan; |

## 2. Informasi Data/Kontak

### 2.1. Nama Tim

Badan Pusat Statistik - Computer Security Incident Response Team (CSIRT), atau disingkat: BPS-CSIRT.

### 2.2. Alamat

Badan Pusat Statistik Republik Indonesia
Jl. Dr. Soetomo No 6-8
Sawah Besar, Jakarta 10710

### 2.3. Zona Waktu

Jakarta (GMT+07:00)

### 2.4. Nomor Telepon

(021) 3863735

### 2.5. Nomor Fax

-

### 2.6. Telekomunikasi Lain

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

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

csirt@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, dengan anggota tim adalah Pejabat Fungsional pada Direktorat Sistem Informasi Statistik sesuai dengan Keputusan Kepala BPS Nomor 582 tahun 2024 tentang Tim Tanggap Insiden Siber Badan Pusat Statistik.

### 2.10. Informasi/Data lain

-

### 2.11. Catatan-catatan pada Kontak BPS-CSIRT

Metode yang disarankan untuk menghubungi BPS-CSIRT adalah melalui *e-mail* pada alamat csirt@bps.go.id atau melalui nomor telepon (021) 3863735 pada hari kerja jam 08.00 - 16.00.

## 3. Mengenai BPS-CSIRT

### 3.1. Visi

Visi BPS-CSIRT adalah terwujudnya manajemen keamanan informasi dalam mendukung layanan TI BPS yang aman dan andal.

### 3.2. Misi

Misi dari BPS-CSIRT, yaitu :

1. Menerapkan manajemen keamanan informasi pada layanan TI dan aset informasi BPS.
2. Meningkatkan kapasitas sumber daya keamanan informasi pada aspek pencegahan, penanggulangan dan pemulihan insiden keamanan informasi.
3. Membangun kesadaran pengguna layanan TI terhadap keamanan informasi.

### 3.3. Konstituen

Konstituen BPS-CSIRT meliputi semua pengguna layanan teknologi informasi 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. Denial of Services (DoS)/Distributed Denial of Services (DDoS)
c. Virus/Malware
d. Phishing
e. Spamming
f. Lainnya

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 mengenai hasil temuan kerawanan pada sistem elektronik tertentu dalam rangka penguatan keamanan (*hardening*).

#### 5.2.2. Penanganan Artefak Digital

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

#### 5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini berupa pemberitahuan mengenai hasil dari kegiatan pengamatan potensi ancaman pada suatu aset teknologi informasi.

#### 5.2.4. Pendeteksian Serangan

Layanan ini berupa hasil pemantauan terhadap aktivitas siber yang bersifat anomali dalam rangka mendeteksi adanya serangan siber pada suatu aset teknologi informasi.

#### 5.2.5. Analisis Risiko Keamanan Siber

Layanan ini berupa identifikasi kerentanan dan penilaian risiko kerentanan yang di temukan, untuk selanjutnya diberikan rekomendasi yang dapat dilakukan untuk mengurangi risiko tersebut.

#### 5.2.6. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini berupa sosialisasi dan pembinaan kepada seluruh pegawai di lingkungan BPS yang bertujuan untuk meningkatkan kesadaran dan kepedulian para pegawai tentang keamanan siber.

## 6. Pelaporan Insiden

Temuan insiden keamanan siber dapat dilaporkan melalui *ticketing system* HALOSIS pada alamat https://halosis.bps.go.id atau melaui email csirt@bps.go.id dengan melampirkan dokumen laporan insiden yang setidaknya memuat log file, timestamp, temuan kerentanan, identifikasi/analisis insiden, nama pelapor, dan nomor telepon seluler pelapor.

## 7. *Disclaimer*

- BPS-CSIRT hanya melayani laporan analisis kerentanan dan insiden keamanan yang terjadi pada aset teknologi informasi yang bersifat kedinasan.
- Cakupan penanganan insiden tergantung pada ketersediaan *tools* yang dimiliki oleh CSIRT-BPS.