

RFC 2350

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 14 Juli 2021.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Versi terbaru dari dokumen ini tersedia pada :

https://csirt.pom.go.id/public/assets/rfc2350/rfc2350_id.pdf (versi Bahasa Indonesia)

https://csirt.pom.go.id/public/assets/rfc2350/rfc2350_en.pdf (versi Bahasa Inggris)

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP Key milik Pusat Data dan Informasi Obat dan Makanan (Pusdatin) - Badan Pengawas Obat dan Makanan (Badan POM). Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Kedua dokumen (versi bahasa inggris dan bahasa Indonesia) memiliki atribut yang sama, yaitu :

Judul : RFC 2350 BPOM-CSIRT;

Versi : 1.0;

Tanggal Publikasi : 14 Juli 2021;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Badan Pengawas Obat dan Makanan (BPOM) - *Computer Security Incident Response Team* (CSIRT)

Disingkat : BPOM -CSIRT

2.2. Alamat

Badan POM

Jalan Percetakan Negara No. 23, Johar Baru, Kecamatan Johar Baru, Jakarta Pusat, 10560, Indonesia

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 42889117

2.5. Nomor Fax

(021) 42889117

2.6. Telekomunikasi Lain

Tidak Ada

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

csirt@pom.go.id

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

Bits : 4096

ID : BPOM-CSIRT <csirt@pom.go.id>

Key Fingerprint : 2F0655B6D68BBDB11E311DA8D8933C8B70E79A10

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

mQINBGDexuYBEAC3EV3Q4WxEIf08d7uLaUMOaXApsrDibQGmyWyQYVADdVm0mB4f
nVgwcGyebSz2RMZO6zNUF66/HdXlpwMe5DoA3XAenSicj9378m8358XdY21wa/gP

```
mh8E6HZtHJMRLjA4YuLmaiZ9walhPm7BA3VHAol+7ud7re6SwrcoDKccxmFzA5JQ
nbFq8ANGrUQnmBYSo46zzFX35/gdUI9K1ZfOQADBgKMD1ER9rNIVbkyfg6jys/5y
ICyJxRR20mQZ5yACu2j6Er0qRuKikBCWRx6H7PtYGT4+1TgbbHk6d/XLzMLBW718
EEbThKCM8j/KnLY4ICNKCADMWIYLZ3oligcoks4dr5IkDflrwOjdljxCY9gB8pn
5mnimlYkHOC/Vbf6zI+LI73GqczJXVCMVNGkWSf2yiXlzpOeY/GmAqXRvz9mNCR
BM+KDe0jbX+IrkPcehD0R82glWfKgxdd9Ea7eWqdKnDFMKfM7ZloO/VcNGHLK43K
K35dwdt/Ubp3+tea0E5MT9zGK7XP2FJlsZmK4egbT8rICgeno/an85A0Wmn0iFO4
jKNj3D9a3m1hnD5VpxlfLxnaePL6RH14geM9IFmP6oa9Gy3l6Thzuar1nP7MlhtB
8dES1yIID9Oaa9S+F2slhx9uRz/nk4FXQ8Eev6SMB44wNS
-----END PGP PUBLIC KEY BLOCK-----
```

File PGP key ini tersedia pada :

<https://csirt.pom.go.id/public/assets/rfc2350/Publik-Key.asc>

2.9. Anggota Tim

Ketua BPOM-CSIRT adalah Kepala Pusat Data dan Informasi Obat dan Makanan. Yang termasuk anggota tim adalah sesuai SK No. HK.02.02.2.21.06.21.141 Tanggal 1 Maret 2021 Tentang Computer Security Incident Response Team Badan Pengawas Obat dan Makanan .

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak BPOM-CSIRT

Metode yang disarankan untuk menghubungi BPOM-CSIRT adalah melalui *e-mail* pada alamat csirt@pom.go.id atau melalui nomor telepon (021) 42889117 ke Pusdatin yang siaga selama Senin – Jumat, 08.00 – 15.00 WIB (tindaklanjut pada jam kerja).

3. Mengenai BPOM-CSIRT

3.1. Visi

Visi BPOM-CSIRT adalah terwujudnya keamanan/ketahanan siber di lingkungan Badan Pengawas Obat dan Makanan.

3.2. Misi

Misi dari BPOM-CSIRT, yaitu :

- a. Melakukan koordinasi, pencegahan, dan mitigasi keamanan informasi di internal Badan pengawas Obat dan Makanan serta koordinasi dengan lembaga insiden lain di Indonesia,
- b. Membangun kerja sama dalam rangka penanggulangan dan pemulihan insiden kemanan siber di lingkungan Badan Pengawas Obat dan Makanan,
- c. Meningkatkan kesadaran pentingnya keamanan informasi bagi sumber daya manusia di lingkungan Badan Pengawas Obat dan Makanan.

3.3. Konstituen

Konstituen BPOM-CSIRT meliputi Seluruh Unit Pusat dan UPT di Badan Pengawas Obat dan Makanan.

3.4. Sponsorship dan/atau Afiliasi

BPOM-CSIRT merupakan bagian dari Badan Pengawas Obat dan Makanan sehingga seluruh pembiayaan bersumber dari Satuan Kerja Pusat Data dan Informasi Obat dan Makanan.

3.5. Otoritas

BPOM-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden keamanan siber terhadap asset yang dikelola oleh BPOM. Dalam melakukan penanggulangan dan pemulihan BPOM-CSIRT berkoordinasi dengan konstituen, BSSN atau pihak lainnya untuk insiden yang tidak dapat ditangani.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

BPOM-CSIRT memiliki otoritas untuk menangani insiden yaitu :

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

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa BPOM-CSIRT 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 Reaktif

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

5.1.1. Layanan pemberian peringatan terkait dengan laporan insiden siber

Layanan ini dilaksanakan oleh Pusat Data dan Informasi Obat dan Makanan Badan POM berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik terkait layanan ini diberikan oleh BPOM-CSIRT.

5.1.2. Layanan penanganan insiden siber

Layanan ini diberikan oleh Pusat Data dan Informasi Obat dan Makanan Badan POM berupa koordinasi, analisis, rekomendasi teknis, dan bantuan *on-site* dalam rangka penanggulangan dan pemulihan insiden siber. BPOM-CSIRT memberikan informasi statistik terkait layanan ini.

5.2. Layanan Proaktif

BPOM-CSIRT secara aktif membangun kapasitas sumber daya keamanan siber melalui kegiatan :

5.2.1. Layanan analisis risiko keamanan siber

Layanan ini diberikan oleh Pusat Data dan Informasi Obat dan Makanan Badan POM berupa identifikasi kerentanan dan penilaian risiko atas kerentanan yang ditemukan.

5.2.2. Layanan pendeteksian serangan

Layanan ini diberikan oleh Pusat Data dan Informasi Obat dan Makanan Badan POM berupa investigasi apakah benar sebuah insiden terjadi dan seberapa luas insiden tersebut.

5.2.3. Pembangunan kesadaran dan kepedulian terhadap keamanan siber

Dalam layanan ini BPOM-CSIRT mendokumentasikan dan mempublikasikan berbagai kegiatan terkait keamanan siber dalam rangka pembangunan kesadaran dan kepedulian ke konstituennya.

6. Pelaporan Insiden

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

- a. Foto/*scan* kartu identitas
- b. Bukti insiden berupa foto atau *screenshot* atau *log file* yang ditemukan

c. Apabila dihubungi bersedia memberikan data-data terkait kebutuhan penyelesaian insiden

7. Disclaimer

BPOM-CSIRT memberikan respon terhadap pelaporan insiden 1x24 jam. Namun, terkait waktu penyelesaian insiden siber bervariasi sesuai dengan kondisi situasional insiden yang dihadapi.