RFC 2350 Health-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 30 November 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.kemkes.go.id/assets/rfc2350

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 Health-CSIRT;
Versi	: 1.0;
Tanggal Publikasi	: 10 Desember 2021;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan

2. Informasi Data/Kontak

2.1. Nama Tim

Health - *Computer Security Incident Response Team* Disingkat : Health - CSIRT.

2.2. Alamat

Kementerian Kesehatan RI
Jl. HR Rasuna Said Blok X-5 Kav 4-9 Setiabudi Jakarta Selatan

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 5221432 (hari kerja)
081317594106 (24/7)

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

-

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

csirt[at]kemkes[at]go[at]id

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

File PGP *key* ini tersedia pada :

https://csirt.kemkes.go.id/assets/publicpgpkemkes.asc

2.9. Anggota Tim

Penanggungjawab Health-CSIRT adalah Sekretaris Jenderal , Ketua adalah Kepala Pusat Data Informasi, Sekretaris adalah Koordinator Kelompok Substansi Pengelolaan Teknologi Informasi dan anggota adalah Pranata Komputer yang berada di Pusat Data dan Informasi beserta perwakilan dari satuan kerja di lingkungan Kementerian Kesehatan.

2.10. Informasi/Data lain

(Tidak Ada)

2.11. Catatan-Catatan pada Kontak Health-CSIRT

Metode yang disarankan untuk menghubungi Health-CSIRT adalah melalui *e-mail* pada alamat csirt[at]kemkes[dot]go[dot]id atau nomor telepon (021) 5221432 pada hari kerja jam 08.00 - 16.00 atau nomor telepon 081317594106 yang aktif 24/7.

3. Mengenai Health-CSIRT

3.1. Visi

Terwujudnya keamanan siber pada pengelolaan Teknologi Informasi dan Komunikasi di Kementerian Kesehatan

3.2. Misi

Misi dari Health-CSIRT, yaitu :

1. Membangun, mengoordinasikan, mengolaborasikan dan mengoperasionalkan pencegahan, penanggulangan dan pemulihan terhadap insiden keamanan siber di lingkungan Kementerian Kesehatan;
2. Membangun kerjasama dalam rangka pengamanan siber terhadap layanan TI di lingkungan Kementerian Kesehatan.
3. Meningkatkan kapasitas sumber daya manusia terhadap ancaman keamanan siber pada aspek pencegahan, penanggulangan dan pemulihan insiden keamanan siber di lingkungan Kementerian Kesehatan.

3.3. Konstituen

Konstituen Health-CSIRT yaitu pengguna layanan TI di lingkungan Kementerian Kesehatan RI.

3.4. Sponsorship dan/atau Afiliasi

Health-CSIRT merupakan bagian dari Sekretariat Jenderal Kementerian Kesehatan sehingga seluruh pembiayaannya bersumber dari APBN.

3.5. Otoritas

Health-CSIRT memiliki kewenangan dengan konstituennya dalam penanganan gangguan keamanan siber, mitigasi, investigasi dan analisis dampak insiden dilingkungan Kementerian Kesehatan. Health-CSIRT dapat berkoordinasi serta bekerjasama dengan pihak lain yang mempunyai kompetensi untuk insiden yang tidak dapat ditangani, seperti BSSN dan/atau Akademisi IT Security dan/atau Ahli Security lainnya.

4. Kebijakan – Kebijakan

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

Health-CSIRT melayani penanganan insiden siber dengan jenis berikut :

a. Web Defacement;
b. DDoS;
c. Malware;
d. Ransomware;
e. Phising;
f. SQL Injection.

Dukungan yang diberikan oleh Health-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

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

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, Health-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 Reaktif

Layanan rekatif dari Health-CSIRT merupakan layanan utama dan bersifat prioritas, yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik yang dikelola oleh masing-masing satuan kerja di Kementerian Kesehatan.

5.1.2. Penanganan Insiden Siber

Layanan ini berupa koordinasi, analisis, rekomendasi teknis, dan bantuan *on-site* dalam rangka penanggulangan dan penanganan insiden siber di Kementerian Kesehatan

5.1.3. Layanan Penanganan Kerawanan

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

5.1.4. Penanganan Artefak Digital

Layanan ini berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi dengan memberikan informasi statistik terkait layanan di Kementerian Kesehatan

5.2. Layanan Tambahan

Layanan tambahan dari Health-CSIRT merupakan layanan proaktif, yaitu :

5.2.1. Menyelenggarakan kegiatan workshop *vulnerability assessment* di lingkungan Kementerian Kesehatan

5.2.2. Menyelenggarakan layanan *Security Assessment* pada aplikasi tertentu di Kementerian Kesehatan

5.2.3. Menyelenggarakan sosialisasi keamanan siber di lingkungan Kementerian Kesehatan

6. Pelaporan Insiden

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

7. Disclaimer

Penanganan insiden tergantung dari ketersediaan *tools* yang dimiliki oleh Kementerian Kesehatan