RFC 2350 RSUI-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi ~~1.0~~ 1.1 yang diterbitkan pada tanggal 21 Mei 2024 ~~02 Februari 2024~~.

1.2. Daftar Distribusi untuk Pemberitahuan

Pengguna layanan TI di lingkungan Rumah Sakit Universitas Indonesia.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://rsui-csirt.rs.ui.ac.id/

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP Key milik RSUI-CSIRT. 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 RSUI-CSIRT
Versi	: 1.1
Tanggal Publikasi	: 21 Mei 2024
Kadaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan

2. Informasi Data/Kontak

2.1. Nama Tim

Rumah Sakit Universitas Indonesia (RSUI) - *Computer Security Incident Response Team* (CSIRT)
Disingkat : RSUI-CSIRT

2.2. Alamat

Rumah Sakit Universitas Indonesia, Jalan Prof. Dr. Bachder Djohan, Kampus UI, Depok, Jawa Barat 16424

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

Telepon (021) 50829292 ext. 711111

2.5. Nomor Fax

Tidak Ada

2.6. Telekomunikasi Lain

Tidak Ada

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

csirt@rs.ui.ac.id

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

File PGP Key ini tersedia pada :

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: OpenPGP.js v2.6.2
Comment: https://openpgpjs.org

xo0EZkL71gEEAMlxanChWEMSs0ZmOay0TjjlTlU5cCOt2q7Az1lGX81wxr1+
2DG70No5cZfHLFVH3x5f1dxN1RNiqYoT5kyblqrVyQ4Wvi175Gr3Y+fhnWo/
ZfRxPlSqDr49R2iYQlCJk/T9RSrVD5j1Ig5F8rFVhwTp6YW1SGYho2izQSUS
zmV7ABEBAAHNKENzaXJ0IFJ1bWFoIFNha2l0IFVJIDxjc2lydEBycy51aS5h
Yy5pZD7CtQQQAQgAKQUCZkL71gYLCQcIAwIJEBQQ+s1/fcA1BBUICgIDFgIB
AhkBAhsDAh4BAAB76AQAtTCqm7SzggKRyFtU053G6Zm5OTPijXfuFnZdbygD
ig+c3t0JhE7mF9A88F33CAg6qyY4DFdqIJ3bQYtioCjvF8XRy+GHKVbP1Fil
9Ab8bRKBNgyAVBf3w21VfT3Mno38PxBIOkQ2i5/zlxWY3rKo+awGmqhXxv8C
oNSVjzYcJyLOjQRmQvvWAQQA7F2MgiFNxqd5R3MvnyuS/7iDbNoOmwa433VK
7a2VKKgGNj59ASSpBKelz/HWLcejf59QBda55eVrsW0v1vWN5CSFw8oNI+fH
MdzeWdnq8/90PLVoRSLSN/X/LRsPZLuoiPRcaT2VieRd0R4noVLteIa+Y7pR
XfKqGv0uHngcWaMAEQEAAcKfBBgBCAATBQJmQvvWCRAUEPrNf33ANQIbDAAA
cBAD/0E12GarYk4zrwOnKqz3IrArutv9u4JVVBYn8TK9FTJbm148e8hWD1gf
BCGoZNYY6iOUMzfXkI6VdiWrFzC+3IvN3HV4/isoAzvK29ohg60ee7OVPgdm
wtQhHOD9Coz06Nhqqci2xP8aeD8TApQNhxiqlxMaG7zFAb6QMN+fa3iD
=UBV9
-----END PGP PUBLIC KEY BLOCK-----

2.9. Anggota Tim

Penanggung jawab RSUI-CSIRT adalah Direktur Umum dan Operasional RSUI, Ketua pelaksana adalah Manajer SIMRS & IT RSUI dan anggota adalah staf Unit SIMRS & IT RSUI.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak RSUI-CSIRT

Metode yang disarankan untuk menghubungi RSUI-CSIRT adalah melalui e-ticketing: ticketing.rs.ui.ac.id, *e-mail* pada alamat csirt@rs.ui.ac.id atau telepon (021) 50829292 ext 711111 jam kerja.

3. Mengenai RSUI-CSIRT

3.1. Visi

Terwujudnya keamanan siber pada pengelolaan Teknologi Informasi dan Komunikasi di Rumah Sakit Universitas Indonesia.

3.2. Misi

Misi dari RSUI-CSIRT, yaitu :

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

3.3 Konstituen

Konstituen RSUI-CSIRT yaitu pengguna layanan TI di lingkungan Rumah Sakit Universitas Indonesia.

3.4. Sponsorship dan/atau Afiliasi

Seluruh pembiayaan RSUI-CSIRT bersumber dari sumber dana internal (DAMAS UI).

3.5. Otoritas

RSUI-CSIRT memiliki kewenangan dengan konstituennya dalam penanganan gangguan keamanan siber, mitigasi, investigasi dan analisis dampak insiden dilingkungan Rumah Sakit Universitas Indonesia. RSUI-CSIRT juga dapat berkoordinasi serta bekerjasama dengan pihak lain yang mempunyai kompetensi untuk insiden yang tidak dapat RSUI tangani, seperti BSSN dan/atau Akademisi IT Security, Vendor Perangkat Security dan/atau Ahli Security.

4. Kebijakan – Kebijakan

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

RSUI-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 RSUI-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

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

Seluruh informasi yang diterima oleh RSUI-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa RSUI-CSIRT dapat menggunakan e-ticketing atau 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. Respon Insiden

RSUI-CSIRT akan membantu konstituen untuk melakukan penanggulangan dan pemulihan insiden keamanan siber dengan aspek-aspek manajemen insiden keamanan siber berikut :

5.1.1. Triase Insiden (*Incident Triage*)

a. Memastikan kebenaran insiden dan pelapor
b. Menilai dampak dan prioritas insiden

5.1.2. Koordinasi Insiden

a. Mengkoordinasikan insiden dengan konstituen
b. Menentukan kemungkinan penyebab insiden
c. Memberikan rekomendasi penanggulangan berdasarkan panduan/SOP yang dimiliki RSUI-CSIRT kepada konstituen
d. Mengkoordinasikan insiden dengan CSIRT atau pihak lain yang terkait

5.1.3. Resolusi Insiden

a. Melakukan investigasi dan analisis dampak insiden
b. Memberikan rekomendasi teknis untuk pemulihan pasca insiden
c. Memberikan rekomendasi teknis untuk memperbaiki kelemahan sistem

RSUI-CSIRT menyajikan data statistik mengenai insiden yang terjadi pada sektor kesehatan sebagai bentuk sentra informasi keamanan siber pada sektor kesehatan.

5.2. Aktivitas Proaktif

Layanan ini diberikan berupa surat edaran, edukasi dan koordinasi secara teknis kepada para pengguna sistem elektronik. Serta, menganalisis dan memberikan rekomendasi dalam rangka penguatan keamanan (hardening) dalam segala aspek.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke e-ticketing :
ticketing[dot]rs[dot]ui[dot]ac[dot]id atau email ke csirt[at]rs[dot]ui[dot]ac[dot]id dengan melampirkan bukti insiden seperti: *logfile*, *timestamp*, *screenshot*, nama pelapor, nomor telepon.

7. *Disclaimer*

Penanganan insiden tergantung dari ketersediaan tools yang dimiliki oleh Rumah Sakit Universitas Indonesia.