RFC 2350 Computer Security Incident Response Team (CISRT)

Rumah Sakit Santa Elisabeth Medan

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan berdasarkan RFC 2350, yaitu informasi dasar mengenai Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan.

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 01 September 2026.

1.2. Daftar Distribusi untuk Pemberitahuan

Menjabarkan pihak-pihak yang menjadi daftar distribusi untuk pemberitahuan RFC 2350, meliputi:

- Direksi RS Santa Elisabeth Medan.
- Tim Tanggap Insiden Siber Nasional (BSSN).
- Health-CSIRT Kementerian Kesehatan RI.
- Seluruh unit kerja dan konstituen di lingkungan RS Santa Elisabeth Medan. .

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt.rssemedan.id/rfc2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen/Kedua dokumen ini telah ditanda tangani dengan PGP *Key*/secara basah oleh Ketua/menggunakan Sertifikat Elektronik milik Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	:	RFC 2350 Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan;
Versi	:	1.0;
Tanggal Publikasi	:	01 September 2026;
Kedaluwarsa	:	Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan
Disingkat : Rumah Sakit Santa Elisabeth Medan-CSIRT.

2.2. Alamat

Jl. H. Misbah No. 7, Jati, Kec. Medan Maimun, Kota Medan, Sumatera Utara 20151.

2.3. Zona Waktu

Medan (GMT+07:00).

2.4. Nomor Telepon

(061) 4144737.

2.5. Nomor Fax

(061) 4153303.

2.6. Telekomunikasi Lain

081262023305

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

rselisabethmedan@gmail.com

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

Bits : 3072 bit
ID : 51E55088716A0FEC
Key Fingerprint : EA55 63C4 9B75 912A DCEE 63DC 51E5 5088 716A 0FEC

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

xsDNBGqWWVABDAC+bKncjZUag+Sr4k+fe7akb8NOjkxOkp/SjQkTV4029nor0
0Ec
ywP22b37M9w+YGTmLtFjxBbPKYi8iCsMnuf1cz9brcNQiDqQxVuAN6BteR5ag0
U0
DSgH4Lztj8dT272sM04sLiU+rtCRgx3Ug6uPHk2SSrKzvexxcPviPJfw/DyErVhJ
XCbggYQNB9MHNsz2FbinApJx/TdhpbAXn8RTIzGSKd8iw+z6zRtwiqUvL1Yhd
x1F
C3ow6NGxlpApXTpDD7gbiPWFMBPgf44p+XfamV0hH8RaUvYjwXH+umCffG
X63Utm
H3V41tOLsY4fjVQLcN7OywxvBTtFV1KkjvBN6MTHv88kkJ8wEJTUHbe5oOJ1
E2sJ

Vkqv66ZjOMIaHU6FDQisfzxHpM2zW1tIy8HAElcEhsXJNEDEbjs3fRAuE3IkuF
U/
1+vCPKlUWbg4Op7UoyM1YHuEp1Kx9hV7aFLSHUf6R/NscS331DSKVkRimmj
DHEbr
zHQlMW2HyJjMY90AEQEAAc1vQ29tcHV0ZXIgU2VjdXJpdHkgSW5jaWRlbnQ
gUmVz
cG9uc2UgVGVhbSAoQ0lTUlQpIFJ1bWFoIFNha2l0IFNhbnRhIEVsaXNhYmV0a
CBN
ZWRhbiA8cnNlbGlzYWJldGhtZWRhbkBnbWFpbC5jb20+wsENBBMBCAA3FiE
E6lVj
xJt1kSrc7mPcUeVQiHFqD+wFAmqWWVAFCQWjmoACGwMECwkIBwUVCA
kKCwUWAgMB
AAAKCRBR5VCIcWoP7Ei3C/48dFwOo1iltFpyrGkAqDzqxDyz8ubCCoOYs1FHJ
uei
fhDlsCG2XzFlQ8oCdNP+9bz+7ypwuuUHXaiAUNNS6gKTKIeMyuATstBTlMuq
VgjF
utoJAwYkm3U6wfViTvj1nV3qC73So6ALOds3k3rRsIr2OJmA8Lyc1S8qOyhsSAj
8
aGjnQaYZ9cSsUAbIppVT3nFHMVxvF/uyGzd0sPbKi1oCcH/rO522qeU+ksSM0V
ue
N3USnbUmwBumjvJ9PYHAO/m8tKWIVSSorF9NknAAk2kkq6zBGNPkY7ARak
GVwkf4
0sa+aZRFocaoUYaKeuO1f9oogtVSEC48Q7tgDLa7ETZ300uZC5bo+Z4dgcvnwB4
0
KhQu+votZINPAclhX8I/Ivk+tQVMOo4FxVypqQNmz3wqAtLW/bqU+dDX2kxIv
0Eo
7LfjOuyAqz9fNPzgA2r6znMTgXJM4PbPQrvYMUTF6OJWrKHt0BIX86BzvwPK
7EfA
oPlxsAlXPWoIrGVcnraEsGnOwM0EapZZUQEMAKtJaGuihF1r4/u3brmdx6fmazb
F
7NhYJhl1cKSUQgUQ3PPliRf3lDGOn1by6YwDsZtwIwg5q4RYTIqZYyDytRGGU
Gcw
DZsLTcO5dRzfnpElWsDmJDAgQhNjRVZa/PSyjIJIFKGpzhEwBMmAdudzu6Om
rDOF
l6Jwbx+0P0SpcBLnlo0Ike7JBNLH7nFYgjVMs0yFZe+c/AycjOaPkG0M/9ZABIg7
aBUfrVCASEyptbrf9GEB+UDiSlxGvSkketilPMg7qimAti73tCuorDOaEwzOlCdh
PDzgAL+1M0R0Ig+G2CP6W/EQ6LNTQu3cqW8cmcqldDJTGk/z/wabxfomeo/yB
XxH
Ex6iyXil8Lg/i3DDKyUM10iAlDyKqxyEO7bP1e13kblI525Lc4uEq8dYEeAHwlZE
LOMdoWMljC8Aq+Od6NLGrteHMZlGkYaPEZSOLVNq6UBF1qDAHyjMDwh2
6kCO5Hck
IwqN7MHIhUC9S6PJBrCzTv3vgGKWDjg3bDss5QARAQABwsD8BBgBCAAmF
iEE6lVj

xJt1kSrc7mPcUeVQiHFqD+wFAmqWWVEFCQWjmoACGwwACgkQUeVQiHFqD+zJ6wv/
QKWw/PhjE+sYZRJBgQZfsuqzIcZi7ZFYwZfUMq3dMu5cQPcwGo3SwRDCeR4u7jRX
QOhjqlu/oSw1Wf5q03HTET5EgdD5AYMm0MNZwQrVsfxbeHiURrk34k+apAU8Zoq2
/m8u6VJ1n51+JGNfd4RREspvspObZjkL0H/ZCI3PIj5V0wujqZAGnXOj0QcVucf/
wHSySZ19EWM25a3V4anYpy7XFWRWwBk7hJL6GcaVmv2+EkRMC1ZJEjDnFoDx0ZqF
5vLdeptlpRB9WNtgqCMbsYQEpENElznrN24TazkSEnmiMWDv6Zl7n8cTf3n7gDN+
jAoEXHYWe3L8oAVuQ3hFc9XkEmNwfqVzQT/bbBuiHSD3eCY/WVE1BD9VUmjNLSXs
TZ7wmCpnuv8kt+AT8Pl473fcuj/me3cKMK/zfgLS1FFVtdK/ANYGCWRNc+1GuZVH
fn8HBMd7TFOubgF0mA7RIpYkUcYywfQtRiZvQ0pwBA8wObInPApSaKXABYC0puYt
=hhiE
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirt.rssemedan.id/publicket.asc

2.9. Anggota Tim

Ketua Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan adalah Jabatan Ketua CSIRT dengan anggota tim adalah staf unit IT, teknisi jaringan, dan pengelola sistem informasi yang ditetapkan dalam SK Direktur RS Santa Elisabeth Medan.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan

Metode yang disarankan untuk menghubungi Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan adalah melalui e-mail pada alamat rselisabethmedan@gmail.com atau melalui nomor telepon (061) 4144737 ke Elisabeth-CSIRT/Unit IT pada hari kerja jam 07.15 - 19.15 WIB / siaga selama 24/7.

3. Mengenai Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan

3.1. Visi

Visi **Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan** adalah menjadi tim tanggap insiden siber yang andal, responsif, dan terpercaya dalam menanggulangi serta memulihkan insiden keamanan siber untuk mendukung keandalan pelayanan kesehatan di RS Santa Elisabeth Medan

3.2. Misi

Misi dari **Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan**, yaitu :

Mengembangkan, mengoordinasikan, dan melaksanakan upaya pencegahan, penanggulangan, serta pemulihan insiden siber secara cepat dan tepat untuk menjamin kerahasiaan, integritas, dan ketersediaan data rekam medis serta sistem informasi pelayanan kesehatan di lingkungan RS Santa Elisabeth Medan.

3.3. Konstituen

Konstituen **Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan** meliputi :

a. Pemberian peringatan terkait keamanan Siber;
b. Perumusan panduan teknis penanganan Insiden Siber;
c. Pencatatan setiap laporan/aduan yang dilaporkan dan pemberian rekomendasi langkah penanganan awal kepada pihak terdampak;
d. Pemilahan (triage) insiden siber sesuai dengan kriteria yang ditetapkan dalam rangka memprioritaskan insiden siber yang akan ditangani;
e. Penyelenggaraan koordinasi penanganan insiden siber kepada pihak yang berkepentingan;
f. Penanganan kerentanan Sistem Elektronik;
g. Penanganan artefak digital;
h. Pemberitahuan hasil pengamatan potensi ancaman;
i. Pendeteksian serangan;
j. Analisis risiko keamanan siber;
k. Konsultasi terkait kesiapan penanganan insiden siber;
l. Pembangunan kesadaran dan kepedulian terhadap keamanan siber.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan **Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan** bersumber dari dana DIPA Rumah Sakit Santa Elisabeth Medan

3.5. Otoritas

Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan menerima otoritas penuh berdasarkan Surat Keputusan Direktur RS Santa Elisabeth Medan Nomor 871/Dir-RSE/SK/VII/2026 [cite: 1-12]. Berdasarkan mandate tersebut, Elisabeth-CSIRT berwenang untuk melakukan pemantauan keamanan siber, menginvestigasi insiden, melakukan tindakan isolasi darurat pada

sistem IT/jaringan yang terkompromi, serta menetapkan langkah penanggulangan dan pemulihan wajib bagi seluruh unit kerja dan civitas hospitalia di RS Santa Elisabeth Medan[cite: 1-12].

4. Kebijakan – Kebijakan

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

Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan melayani penanganan insiden siber dengan jenis berikut :

a. Serangan Ransomware / Malware pada SIMRS dan basis data rekam medis.
b. Kebocoran Data (Data Breach) pasien, rekam medis, maupun data pegawai.
c. Akses tidak sah (Unauthorized Access) dan upaya Phishing.
d. Gangguan ketersediaan layanan (Denial of Service / DDoS).

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan menjaga kerahasiaan seluruh informasi insiden, artefak teknis, serta data rekam medis pasien sesuai dengan peraturan perundang-undangan mengenai perlindungan data pribadi dan rahasia kedokteran. Informasi insiden hanya dibagikan kepada pihak internal berwenang, BSSN, dan Health-CSIRT untuk kepentingan penanggulangan insiden.

4.3. Komunikasi dan Autentikasi

Komunikasi operasional rutin dilakukan melalui saluran resmi. Untuk penyampaian informasi rahasia atau sensitif, **Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan** mewajibkan penggunaan enkripsi End-to-End menggunakan PGP Key resmi..

5. Layanan

5.1. Layanan

Layanan yang diberikan oleh **Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan** yaitu :

5.1.1. Penanggulangan Dan Pemulihan Insiden Siber

Melakukan verifikasi laporan, pengisolasian sistem terkompromi (containment), investigasi teknis, serta pemulihan operasional sistem informasi rumah sakit.

5.1.2. Penyampaian Informasi Insiden Siber Kepada Pihak Terkait

Pelaporan kronologi dan koordinasi teknis penanganan insiden kepada BSSN, Health-CSIRT Kementerian Kesehatan RI, serta Direksi RS Santa Elisabeth Medan.

5.1.3. Diseminasi Informasi Untuk Mencegah dan/atau Mengurangi Dampak dari Insiden Siber

Penerbitan imbauan keamanan (advisory), peringatan dini kerentanan siber, dan panduan teknis untuk mencegah atau mengurangi dampak insiden siber.

5.2. Fungsi

Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan memiliki fungsi-fungsi dalam menjalankan layanannya, antara lain :

5.2.1. Fungsi Utama

Fungsi utama yang diberikan **Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan** yaitu :

5.2.1.1. Pemberian Peringatan Terkait Keamanan Siber

Menyampaikan peringatan dini (early warning) dan informasi ancaman keamanan siber terbaru kepada seluruh unit kerja internal RS Santa Elisabeth Medan.

5.2.1.2. Perumusan Panduan Teknis Penanganan Insiden Siber

Menyusun SOP, pedoman teknis, serta standar operasional penanganan insiden siber di lingkungan rumah sakit.

5.2.1.3. Pencatatan Setiap Laporan/Aduan Yang Dilaporkan, Pemberian Rekomendasi Langkah Penanganan Awal Kepada Pihak Terdampak

Merekam setiap laporan insiden yang masuk dari konstituen serta memberikan arahan mitigasi awal bagi pihak terdampak.

5.2.1.4. Pemilahan (Triage) Insiden Siber Sesuai Dengan Kriteria yang Ditetapkan Dalam Rangka Memprioritaskan Insiden Siber yang Akan Ditangani

Memilah, memverifikasi, dan mengklasifikasikan tingkat keparahan insiden guna menetapkan skala prioritas penanganan.

5.2.1.5. Penyelenggaraan Koordinasi Penanganan Insiden Siber Kepada Pihak yang Berkepentingan

Mengordinasikan langkah penanggulangan insiden bersama jajaran Direksi RS, BSSN, dan Health-CSIRT Kementerian Kesehatan RI.

5.2.1.6. Penyelenggaraan Fungsi Lainnya Sesuai Kebutuhan

Melakukan tugas pendukung operasional keamanan informasi sesuai dengan kebutuhan strategis rumah sakit.

5.2.2. Fungsi Tambahan (Lainnya)

Fungsi tambahan yang diberikan oleh **Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan** yaitu :

5.2.2.1. Penanganan Kerawanan Sistem Elektronik

Melakukan identifikasi, analisis, dan penutupan celah kerentanan (vulnerability) pada sistem informasi dan aplikasi RS

5.2.2.2. Penanganan Artefak Digital

Pengumpulkan, mengekstraksi, dan menganalisis barang bukti atau artefak digital pasca-insiden untuk kebutuhan forensik siber

5.2.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Menyampaikan hasil pengamatan berkala terhadap potensi bahaya atau tren serangan siber yang menargetkan sektor kesehatan.

5.2.2.4. Pendeteksian Serangan

Pemantauan (monitoring) lalu lintas jaringan dan log sistem secara berkelanjutan untuk mendeteksi aktivitas mencurigakan secara real-time.

5.2.2.5. Analisis Risiko Keamanan Siber

Mengukur dan menilai tingkat risiko serta dampak potensial dari ancaman siber terhadap kelangsungan layanan rumah sakit.

5.2.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Menyediakan layanan konsultasi teknis bagi unit kerja internal dalam menyiapkan langkah mitigasi dan ketahanan siber.

5.2.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Menyelenggarakan program edukasi, literasi, dan sosialisasi keamanan siber bagi seluruh pegawai dan civitas RS Santa Elisabeth Medan.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke rselisabethmedan@gmail.com dengan melampirkan sekurang-kurangnya :

a. Foto/*scan* kartu identitas
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
c. Atau sesuai dengan ketentuan lain yang berlaku (co. Kronologi / Replikasi Insiden)

7. *Disclaimer*

Meskipun setiap langkah penanggulangan dan mitigasi dilakukan secara terukur dan hati-hati, Computer Security Incident Response Team (CISRT) Rumah Sakit Santa Elisabeth Medan tidak bertanggung jawab atas kerugian langsung maupun tidak langsung yang timbul akibat keterlambatan pelaporan insiden oleh pelapor atau akibat kondisi keadaan memaksa (force majeure).