DOKUMEN RFC 2350

SMHG-CSIRT

Sentra Medika Hospital Group

Computer Security Incident Response Team

1. Informasi Dokumen

Dokumen ini berisi deskripsi Sentra Medika Hospital Group Computer Security Incident Response Team, yang selanjutnya disingkat SMHG-CSIRT, berdasarkan format RFC 2350. Dokumen ini memuat informasi dasar mengenai SMHG-CSIRT, tanggung jawab, layanan yang diberikan, serta cara menghubungi SMHG-CSIRT.

1.1 Tanggal Terakhir Diperbarui

Dokumen merupakan dokumen versi 1.4 yang diterbitkan pada tanggal [ISI: tanggal penerbitan].

1.2 Daftar Distribusi untuk Pemberitahuan

SMHG-CSIRT tidak menyelenggarakan milis khusus untuk pemberitahuan perubahan dokumen ini. Pemberitahuan perubahan disampaikan kepada seluruh konstituen melalui kanal resmi internal (surel korporat dan Lark Chat), serta melalui pembaruan pada laman resmi SMHG-CSIRT. Pertanyaan mengenai pembaruan dokumen dapat disampaikan ke csirt[at]smhg[dot]co[dot]id.

1.3 Lokasi Dokumen

Dokumen ini tersedia pada:

https://csirt.sentramedikahospitals.com/senta-rfc2350

Selama laman resmi masih dalam proses penyiapan, dokumen dapat diperoleh melalui koordinasi dengan SMHG-CSIRT pada alamat surel: csirt[at]smhg[dot]co[dot]id

1.4 Autentikasi Dokumen

Dokumen ini ditandatangani secara digital menggunakan kunci OpenPGP SMHG-CSIRT sebagaimana tercantum pada butir 2.8. Berkas tanda tangan tersedia bersama dokumen ini pada laman resmi SMHG-CSIRT.

1.5 Identifikasi Dokumen

Judul	Dokumen RFC 2350 SMHG-CSIRT
Versi	1.4
Tanggal Dokumen	02 Juli 2026
Kedaluwarsa	Dokumen ini berlaku sampai digantikan oleh versi berikutnya
Klasifikasi	TLP:CLEAR — dapat disebarluaskan tanpa pembatasan

2. Informasi Kontak

2.1 Nama Tim

SMHG-CSIRT

(Sentra Medika Hospital Group — Computer Security Incident Response Team)

2.2 Alamat

PT Dharma Nugraha (Sentra Medika Hospital Group)

Jl. Raya Mayor Oking Jaya Atmaja No. 9, Cibinong, Kecamatan Cibinong, Kabupaten Bogor, Jawa Barat 16911

2.3 Zona Waktu

Jakarta (GMT+07:00) — Waktu Indonesia Barat (WIB)

2.4 Nomor Telepon

(+62) 21-87909999 ext 6200, 6201

(+62) 21-87909999 ext 6200, 6201 — darurat, on-call 24 jam / 7 hari

2.5 Nomor Faksimile

(+62) 21-87909377

2.6 Telekomunikasi Lain

Lark Chat — channel CSIRT SMHG (internal)

Sistem ticketing GLPI — https://smart.sentramedikahospitals.com (internal)

2.7 Alamat Surat Elektronik (E-mail)

csirt[at]smhg[dot]co[dot]id

2.8 Kunci Publik dan Sarana Komunikasi Terenkripsi

SMHG-CSIRT menggunakan kunci OpenPGP untuk autentikasi dan komunikasi terenkripsi dengan pihak eksternal, termasuk BSSN dan Health CSIRT.

Bits	4096
Tipe Kunci	RSA
User ID	smhg-csirt <csirt[at]smhg[dot]co[dot]id>
Key ID	0xB56E0B33FED2713C
Fingerprint	EFAB 865C 04AF BD99 7CF8 3212 B56E 0B33 FED2 713C
Dibuat	7 Agustus 2026
Masa Berlaku	sampai dengan 6 Agustus 2031
Subkunci Enkripsi	0x4BEF67A7E77310F4 (RSA 4096)

Blok PGP Public Key:

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

xsFNBGp1SkIBEACQ0gWam0dlFmmQjmeXrGMb+Ege7V5V4TNdL4PoggKxAjG+laXj
fD641rbYfjuvbnTy2p6s9aFEbjDTxLf7IbM9w47L7NK2N/0fGmuk+KoBHJoN/eai
MSaLabRC4jXuHML1+HE/iS2MYw6+Up1iZl70pfa4wWC9ufEgabIIKgNeYlc2+c64
LD3lF4yi8XUJ1fuAVw9toOPxyR3MYqbyAg2xMCxn3LZdxOc/soMp+66N82+OiIR8
xnk6oFjVyObiFa2eM7RKutyxVasIWKR+wO3wz3uLdoOR2QbEyL0HQ7f80mLjnI8F
VT7BHzVC7NWAh+51LKVtMTpNXIyPXaJCs3xrPZVCjYoUC04lCXT1I9QhwAZXxBtL
QRM3MQWd3FtK44tiLua1O1fuqKiVPDa/s6x0JrQJkC3R+nFEZxWf4Bkx/v+JoKjf
ig0ddYMvtyTFByPScsHAym3gjAryVIfzsamF92DWOE+0CaMkZPmahFZy4zUOehhb
lkQl/d5xhqUudgXInoOtyWbVWZNeZVk37DNPhaUf2TTZsBBgbrNr5FZZKHeU8dAd
RWVAasDI1cp2g58bqA4gaLQVwfVT5gyUyY+Y6cIUtdo8irDVNVsz4UjuJWXqdJQm
4ek49C5IlwrVFbX2FbB6/ZW6SI8WAzvd3NvPG+DIMSmXJznjoxJq6SiakQARAQAB
zR1zbWhnLWNzaXJ0IDxjc2lydEBzbWhnLmNvLmlkPsLBjQQTAQgANxYhBO+rhlwE
r72ZfPgyErVuCzP+0nE8BQJqdUpDBQkJZgGAAhsDBAsJCAcFFQgJCgsFFgIDAQAA
CgkQtW4LM/7ScTymPxAAhFTKpxD2uh+9MzM8L+5y6QZfyFNimpe9SXnGg8dl1oV/
pP8dSLAsryt0XBnNPaZnmnKeuaWtnACK7SA8EAUB0j684kDnsKSa0ujF5vhYNgBF
YSm2OnIxg4EdPg0XOK7u9qs8PnvLlf7F9aITdqA2Ub7g6HZikqQMaDTCJM+HnOS8
Xs96MkHzBbNynFjSMBFlCAePYbfJeoaUupvmHvnFLx/HDdlkmetPlcUpn4031sMj
ryOxxIdYjS9fYLFVntmfhCQ3njCmenubxtX2gAw1qOwkl2o0sp56yg1lV+7FWf2Y
GbrApTHySsSLVeKwbyMItgJnM910D2iXCzqlKAyezGI61zw4+BZoNoQ6Dskm7YQj
EE/OVVkXlimI5ys4sMu9WijsyK4fT/AQXIrBlMOQu8y87qGV9HfuR8b8fArvtq+R
Hzg9Hh0xBUD+EnX/wyAN3RTkjtAi6T5ntDGLZMXVI6Y+UUyxoquOPi/F8Z4LVVOa
mBUppUqmsZAKWhkBi6rORHAS/Q3N88Qh9Yz2/fIPEvQhw0ZxZAkWoi2TYqJxdj39
MiN9ZUgqdL7Q7iqvuQC6bZDLRr1Bar3h8PAB7BJY3Oftq4PKsOgHxMHm39aVou4z
8L4BynlF9i2Ye/Syo9A85ewUAczDha3lI4tpEa/7F5jO/xrY0avM/ldkrx7jVzLO
wU0EanVKRAEQANMwBQ4w6AXnKbH6fGWSievHwptO9P6hu1Eq5vgpGW/aRWLT/OUC
M48d8HmyMazjXxMVgGiLwVWTQFqhPO8slvnl6XzQxbgSl+FMZcwV88gtDJdCc0Zg
9GoIjX6Uw/5HNTqX2q7RDCn6gnzzpLuwI319/cnkZV0v7f9RB4N8pKUHBb/xCHMk
t7r8TVgNcNroaEn/KK7pvbVBuGehQBRo7hzvsQUQnAK2QUpY5/LkblHrP0YU3SnV
Q20NbOPHvJzVAfOigaewRnCDc8K5TF0nK1Md0nw7yKUzdC/ZAJ33UMnyhzCxYvn4
ZRpddetV1IeR0Yk0EqERr2hd892KFnWaokNhj3ymVZBB+83Ys6AZcjlXiB52oCxQ
fUZ7r3Tj0G8bn6/dSFGYgc5vjQY4Q6V1VJm+ilalUk7wXaWSiq9k9NPKHA1Xlbza
```

```
7rNg/qHOoybUyfTMdI5D96qnyGnhSivSWYlKq3c8UZdvxMOjHQzYJUx2683Ek+9e
jYtN7dPv0Rt+nyf4NVkxhXfMgECHkNMoeYSmRjRtB0GCyDrLZwdyKiRdaOoOYz8C
KUMZ1Y2SBjiiXgzNbndi0yiCU/P9MuS7L0xMpNApcBclySj5cDDA0vIG/967hvJY
0zbTxHH6LisD7br2jOfMVCjOIUWT3NRUz6hbf7wrlj/PkLd68gzBhJ4NABEBAAHC
wXwEGAEIACYWIQTvq4ZcBK+9mXz4MhK1bgsz/tJxPAUCanVKRgUJCWYBgAIbDAAK
CRC1bgsz/tJxPGv5D/9fcOwtP9/udXC6gu8phzOKFJ1uR3gDLA+rUq1xRoY+Bq1v
ovI2MnmBGvIOge28C8+qB9faCtlUFXD6mZgScAyejznMlXhoPHE6a/++vwdtYzJ1
9fSNp4JbQOGUGRiKOKq2RaZEdPGT4w3+sNNTFQf0xd0XKqjhrmKtzVYsPLIfMNYv
ZNnKJyScznCeFCH/rCm6TMUPS55G0iIYkWcCbGxEmIk4t0kQ05Vef+apxY7L9LlG
TAAenP1DvGfm4i0xKaO1WFu+kGzaf2F/xYDHOd/N9ytJN1nJgLTSA4wU68bXG7RE
6Qg7irN7PCyctzFgFfAMXnnqyoHPL1m6CvyDqCgxm2cJtSXPH/xMXZ3Qa7DugCn3
sSf2ufjIrX8F4ia0gyW89yVyP87+5TYKazaiHF3AOO7twaraG40WPkb/jq/dNL7V
XdVf3wMkz9TKJkhMTTVUCnU0F4ovqH8Wz/MK1d8ejyU9h7hNtzRKQ+r6FRRIB8/e
KC/3JxyH9Ox+KGtPNtRAWKYqBFUe7J90T3l4xFO2W8fxW5+sxpW8HX09GUkHe6k1
sjQ3K4EtZ3oxdUNb67CGjr946ZmXJQjQFhxj9c/IVTNVRfTU+0PjzI5Ib71nVeuu
aR/idmtIC6oKb2LH6QhjbxXfFCpf+OzZnFSnTdUe6u76TLrsu9PJByUwSRbonQ==
=O7H5
-----END PGP PUBLIC KEY BLOCK-----
```

Berkas kunci publik tersedia pada:

a. https://csirt.sentramedikahospitals.com/sentra-pkey

b. https://keys.openpgp.org/vks/v1/by-fingerprint/EFAB865C04AFBD997CF83212B56E0B33FED2713C

Kunci juga dapat ditemukan pada keyserver keys.openpgp.org melalui pencarian alamat surel csirt[at]smhg[dot]co[dot]id

Komunikasi internal antaranggota tim menggunakan Lark Chat. Komunikasi eksternal yang memerlukan tingkat keamanan tinggi dilakukan melalui surel csirt[at]smhg[dot]co[dot]id dengan tanda tangan dan/atau enkripsi OpenPGP.

2.9 Keanggotaan Tim

SMHG-CSIRT dipimpin oleh seorang Ketua yang dijabat oleh IT Operation Manager Sentra Medika Hospital Group, dibantu oleh seorang Wakil Ketua yang dijabat oleh Kepala Seksi Infrastruktur Teknologi Informasi.

Keanggotaan tim terdiri atas unsur Unit Teknologi Informasi Sentra Medika Hospital Group yang mencakup fungsi sistem jaringan dan keamanan, infrastruktur teknologi informasi, sistem informasi, pengembangan SIMRS, serta penanggulangan dan pemulihan. Pada setiap cabang rumah sakit ditetapkan seorang narahubung yang menjadi titik kontak insiden keamanan siber pada unit yang bersangkutan. Tim didukung oleh fungsi administrasi dan dokumentasi.

Susunan keanggotaan tim beserta nama personel ditetapkan dalam Lampiran Keputusan President Director PT Dharma Nugraha Nomor 004.IT/KEP-PRESDIR/SMHG/VI/2026. Perubahan susunan tim ditetapkan melalui perubahan keputusan tersebut dan tidak mengubah dokumen ini.

2.10 Informasi/Data Lain

Informasi umum mengenai SMHG-CSIRT, termasuk versi terkini dokumen ini, kunci publik OpenPGP, dan kanal pelaporan insiden, tersedia pada laman resmi https://csirt.sentramedikahospitals.com. Tidak terdapat informasi lain yang perlu disampaikan pada butir ini.

2.11 Catatan-catatan pada Kontak SMHG-CSIRT

Metode kontak yang disarankan untuk pelaporan insiden adalah melalui surel ke csirt[at}smhg.co.id. Untuk insiden dengan tingkat keparahan tinggi atau yang memerlukan penanganan segera, pelapor dianjurkan menghubungi nomor telepon darurat (+62) 21-87909999 ext 6200, 6201 yang tersedia 24 jam / 7 hari, dan menyusulkan laporan tertulis melalui surel.

Informasi sensitif wajib dikirimkan dalam bentuk terenkripsi menggunakan kunci OpenPGP SMHG-CSIRT pada butir 2.8.

Narahubung SMHG-CSIRT untuk koordinasi dengan BSSN dan Health CSIRT ditetapkan berdasarkan jabatan sebagai berikut:

Kedudukan	Dijabat oleh
Narahubung Utama	Ketua SMHG-CSIRT
Narahubung Alternatif	Wakil Ketua SMHG-CSIRT
Narahubung Teknis	Pengelola Sistem Jaringan dan Keamanan

Nama dan data kontak personel yang memangku jabatan tersebut tercantum dalam Lampiran Keputusan President Director PT Dharma Nugraha Nomor 004.IT/KEP-PRESDIR/SMHG/VI/2026 serta pada Surat Pernyataan Kesediaan menjadi Narahubung yang disampaikan kepada Badan Siber dan Sandi Negara. Seluruh korespondensi resmi tetap dialamatkan ke csirt[at]smhg[dot]co[dot]id

3. Mengenai SMHG-CSIRT

3.1 Visi

SMHG-CSIRT berkomitmen melindungi sistem informasi dan infrastruktur teknologi informasi Sentra Medika Hospital Group dari ancaman siber melalui deteksi dini, penanganan insiden secara efektif, serta peningkatan kesadaran keamanan siber di seluruh unit kerja dan 6 (enam) cabang rumah sakit dalam lingkungan SMHG.

3.2 Misi

Untuk mewujudkan visi tersebut, SMHG-CSIRT menjalankan misi sebagai berikut:

1. menyelenggarakan pencegahan, deteksi, penanganan, penanggulangan, dan pemulihan terhadap insiden keamanan siber di lingkungan Sentra Medika Hospital Group;
2. menjadi titik kontak tunggal (single point of contact) bagi konstituen dalam pelaporan dan penanganan insiden keamanan siber;
3. menjamin kerahasiaan, integritas, dan ketersediaan data pasien serta sistem informasi yang menopang pelayanan kesehatan;
4. menjadi titik koordinasi dengan Badan Siber dan Sandi Negara selaku Tim Tanggap Insiden Siber Nasional dan dengan Health CSIRT Kementerian Kesehatan selaku Tim Tanggap Insiden Siber Sektoral;
5. meningkatkan kesadaran dan kapasitas keamanan siber seluruh sumber daya manusia di lingkungan SMHG.

3.3 Konstituen

Konstituen SMHG-CSIRT adalah seluruh unit kerja, sistem informasi, infrastruktur teknologi informasi, dan sumber daya manusia di lingkungan Sentra Medika Hospital Group, mencakup 6 (enam) cabang rumah sakit berikut:

- RS Umum Harapan Bunda
- Sentra Medika Hospital Cisalak
- Sentra Medika Hospital Cikarang
- Sentra Medika Hospital Cibinong
- Sentra Medika Hospital Minahasa Utara
- Sentra Medika Hospital Gempol

Cakupan konstituen meliputi sistem elektronik terpusat maupun terdistribusi, termasuk Sistem Informasi Manajemen Rumah Sakit (SIMRS) Teramedik dan Rekam Medis Elektronik.

3.4 Sponsorship dan/atau Afiliasi

SMHG-CSIRT disponsori sepenuhnya oleh PT Dharma Nugraha (Sentra Medika Hospital Group) selaku organisasi induk. Seluruh kebutuhan sumber daya manusia, anggaran, sarana, dan prasarana bagi penyelenggaraan SMHG-CSIRT dijamin oleh pimpinan organisasi sebagaimana dinyatakan dalam Surat Pernyataan Pimpinan Organisasi Nomor 007/S.Per-Dirut/PTDN/VI/2026 tanggal 12 Juni 2026.

SMHG-CSIRT berafiliasi dan berkoordinasi dengan Badan Siber dan Sandi Negara (BSSN) selaku Tim Tanggap Insiden Siber Nasional serta dengan Health CSIRT Kementerian Kesehatan selaku Tim Tanggap Insiden Siber Sektor Kesehatan.

3.5 Otoritas

SMHG-CSIRT memperoleh otoritas dari President Director PT Dharma Nugraha berdasarkan Keputusan President Director PT Dharma Nugraha Nomor 004.IT/KEP-PRESDIR/SMHG/VI/2026 tanggal 10 Juni 2026.

Berdasarkan keputusan tersebut, SMHG-CSIRT berwenang mengambil tindakan pencegahan, deteksi, respons, penanggulangan, dan pemulihan terhadap insiden keamanan siber dalam lingkungan Sentra Medika Hospital Group, termasuk melakukan isolasi sistem, akun, atau perangkat yang terdampak sesuai Standar Prosedur Operasional yang berlaku.

4. Kebijakan-Kebijakan

4.1 Jenis-jenis Insiden dan Tingkat/Level Dukungan

SMHG-CSIRT berwenang menangani jenis insiden berikut:

a. Web Defacement;
b. Denial of Service dan Distributed Denial of Service (DoS/DDoS);
c. Malware;
d. Ransomware;
e. Phishing dan rekayasa sosial (social engineering) terhadap staf rumah sakit;

f. SQL Injection dan kerentanan sistem (vulnerability) pada aplikasi dan infrastruktur;
g. Akses tidak sah (unauthorized access) ke sistem informasi dan data pasien;
h. Kebocoran data (data breach), khususnya data rekam medis dan data pribadi pasien;
i. Gangguan layanan kritis yang berkaitan dengan SIMRS Teramedik;
j. Insiden keamanan pada perangkat jaringan dan infrastruktur.

Jenis insiden pada huruf a sampai dengan huruf f selaras dengan jenis insiden yang dilayani Health CSIRT Kementerian Kesehatan selaku Tim Tanggap Insiden Siber Sektor Kesehatan, sedangkan huruf g sampai dengan huruf j merupakan cakupan tambahan sesuai karakteristik konstituen Sentra Medika Hospital Group.

SMHG-CSIRT memberikan dukungan penuh untuk penanganan insiden yang berdampak pada sistem kritis (SIMRS, data pasien, dan jaringan utama), serta dukungan terbatas untuk insiden pada sistem non-kritis. Tingkat dukungan dan target waktu respons mengikuti klasifikasi pada butir 6.3.

4.2 Kerja Sama, Interaksi, dan Pengungkapan Informasi/Data

SMHG-CSIRT bersedia berbagi informasi terkait insiden siber dengan BSSN, Health CSIRT Kementerian Kesehatan, dan pihak berwenang lainnya, dengan tetap menjaga kerahasiaan data pasien sesuai Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan peraturan perundang-undangan bidang kesehatan.

SMHG-CSIRT berkoordinasi dengan Badan Siber dan Sandi Negara (BSSN) selaku TTIS Nasional, dengan Health CSIRT Kementerian Kesehatan selaku TTIS Sektoral yang dibentuk berdasarkan Keputusan Menteri Kesehatan Nomor HK.01.07/MENKES/542/2025, serta dengan CSIRT lain yang terkait dalam kerangka penanganan insiden siber nasional.

Dalam pertukaran informasi, SMHG-CSIRT menerapkan Traffic Light Protocol (TLP) versi 2.0 sebagai berikut:

Penanda	Ketentuan Penyebarluasan
TLP:RED	Hanya untuk penerima yang disebutkan secara langsung. Tidak boleh diteruskan kepada pihak mana pun, termasuk di dalam organisasi penerima.
TLP:AMBER+STRICT	Terbatas pada organisasi penerima saja. Tidak boleh diteruskan kepada klien atau pihak ketiga.
TLP:AMBER	Terbatas pada organisasi penerima dan kliennya, sebatas keperluan penanganan insiden.
TLP:GREEN	Dapat dibagikan dalam komunitas terkait, tetapi tidak melalui kanal publik.
TLP:CLEAR	Dapat disebarluaskan tanpa pembatasan.

Informasi yang tidak diberi penanda diperlakukan sebagai TLP:AMBER.

4.3 Komunikasi dan Autentikasi

Seluruh informasi yang diperoleh dalam proses penanganan insiden diperlakukan sebagai informasi rahasia dan hanya digunakan untuk keperluan penanganan insiden serta pelaporan kepada pihak berwenang.

Informasi sensitif disampaikan melalui kanal terenkripsi. Autentikasi komunikasi eksternal menggunakan tanda tangan digital OpenPGP sebagaimana tercantum pada butir 2.8. Untuk komunikasi yang tidak sensitif, surel biasa dapat digunakan.

5. Layanan

Layanan SMHG-CSIRT mengikuti klasifikasi layanan Tim Tanggap Insiden Siber sebagaimana diatur dalam peraturan Badan Siber dan Sandi Negara, dan diselenggarakan bagi konstituen sebagaimana dimaksud pada butir 3.3.

5.1 Layanan Utama

5.1.1 Pemberian Peringatan Terkait Keamanan Siber

Layanan ini berupa penyampaian peringatan dini, security advisory, dan notifikasi ancaman kepada pemilik sistem elektronik dan unit kerja di lingkungan Sentra Medika Hospital Group, termasuk penerusan peringatan yang diterima dari BSSN dan Health CSIRT Kementerian Kesehatan.

5.1.2 Penanganan Insiden Siber

Layanan ini berupa penerimaan laporan, triase, analisis, penanggulangan, pemulihan, dan evaluasi pasca-insiden, termasuk koordinasi dan bantuan di lokasi apabila diperlukan. Prosedurnya diatur dalam Standar Prosedur Operasional Nomor SMHG.IT.010, dan kewajiban pelaporan ke pihak eksternal diatur dalam Nomor SMHG.IT.011.

5.2 Layanan Tambahan

5.2.1 Penanganan Kerawanan Sistem Elektronik

Layanan ini berupa koordinasi, analisis, dan rekomendasi teknis atas kerawanan pada perangkat lunak maupun perangkat keras, serta verifikasi kerawanan yang berpotensi dieksploitasi, dalam rangka penguatan keamanan. Prosedurnya diatur dalam Standar Prosedur Operasional Nomor SMHG.IT.008.

5.2.2 Penanganan Artefak Digital

Layanan ini berupa pengumpulan, pengamanan, dan analisis artefak digital yang diduga digunakan atau dihasilkan dalam suatu insiden, guna mendukung pemulihan sistem terdampak dan penelusuran penyebab insiden. Prosedur dan rantai penguasaan barang bukti diatur dalam Standar Prosedur Operasional Nomor SMHG.IT.013.

5.2.3 Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini berupa penyampaian potensi ancaman terhadap sistem elektronik kepada konstituen, yang diperoleh dari pemantauan perangkat keamanan, informasi mitra, dan perkembangan ancaman pada sektor kesehatan.

5.2.4 Pendeteksian Serangan

Layanan ini berupa analisis data pemantauan untuk mendeteksi serangan, aktivitas mencurigakan, atau pelanggaran kebijakan keamanan pada sistem elektronik. Prosedurnya diatur dalam Standar Prosedur Operasional Nomor SMHG.IT.006.

5.2.5 Analisis Risiko Keamanan Siber

Layanan ini berupa identifikasi dan penilaian risiko keamanan siber beserta rekomendasi tindak lanjutnya. Prosedurnya diatur dalam Standar Prosedur Operasional Nomor SMHG.IT.009.

5.2.6 Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan ini berupa pemberian wawasan, pemahaman, dan langkah yang perlu disiapkan unit kerja dalam menghadapi dan menangani insiden siber.

5.2.7 Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini berupa diseminasi dan pembinaan keamanan siber bagi seluruh sumber daya manusia di lingkungan Sentra Medika Hospital Group, termasuk tenaga medis dan tenaga penunjang.

- koordinasi pemulihan pasca-insiden.

6. Pelaporan Insiden

6.1 Kanal Pelaporan

Surel	csirt[at]smhg[dot]co[dot]id
Telepon	(+62) 21-87909999 ext 6200, 6201 — darurat 24 jam / 7 hari
Lark Chat	Channel CSIRT SMHG (internal)
Sistem Ticketing	GLPI — https://smart.sentramedikahospitals.com (internal)

6.2 Informasi yang Diperlukan

Pelapor diharapkan menyertakan informasi berikut:

- nama pelapor dan unit kerja;
- tanggal dan waktu kejadian;
- deskripsi singkat insiden;
- sistem atau aset yang terdampak;
- tindakan yang sudah dilakukan (apabila ada);
- informasi kontak yang dapat dihubungi untuk tindak lanjut.

Laporan agar dilengkapi bukti insiden berikut:

1. logfile beserta timestamp;
2. tangkapan layar (screenshot);
3. identitas pelapor;
4. kronologi insiden dan penanganan yang sudah dilakukan.

Formulir Aduan Insiden Siber tersedia melalui sistem ticketing GLPI dan dapat diminta melalui csirt[at]smhg[dot]co[dot]id.

6.3 Waktu Respons

Laporan yang masuk dikategorikan menurut jenis laporan (Tier 1) dan kelompok layanan atau ancaman (Tier 2). Klasifikasi tingkat keparahan beserta target waktu respons untuk setiap kategori mengikuti Standar Prosedur Operasional Penanganan Insiden Keamanan Siber Nomor SMHG.IT.010:

Kategori Tier 1	Kategori Tier 2	Tingkat	Target Respons
Laporan Insiden	Sistem informasi klinis dan data pasien	**Tinggi**	≤ 1 jam
	Perangkat lunak berbahaya pada sistem inti		
	Akses tidak sah ke sistem inti		
	Gangguan ketersediaan layanan kritis		
	Perangkat lunak berbahaya pada perangkat pengguna	**Sedang**	≤ 8 jam
	Rekayasa sosial		
	Anomali akses dan aktivitas		
Laporan Kerentanan	Kerentanan sistem produksi	**Sedang**	≤ 8 jam
	Kerentanan perangkat jaringan dan infrastruktur		
Permintaan Informasi dan Konsultasi	Konsultasi dan permintaan penjelasan	**Rendah**	≤ 3 × 24 jam
	Laporan tanpa dampak layanan		

Perincian objek terdampak pada setiap kategori diatur dalam Standar Prosedur Operasional Nomor SMHG.IT.010 dan tidak dimuat dalam dokumen ini. Waktu respons dihitung sejak laporan diterima dan diverifikasi sebagai insiden pada tahap triase. Untuk insiden yang memenuhi kriteria pelaporan eksternal, SMHG-CSIRT melaporkan kepada BSSN dan Health CSIRT paling lambat 3 × 24 jam sejak insiden diketahui, sesuai Standar Prosedur Operasional Nomor SMHG.IT.011.

7. Penafian (Disclaimer)

Informasi dalam dokumen ini disediakan tanpa jaminan apa pun, baik tersurat maupun tersirat. SMHG-CSIRT tidak bertanggung jawab atas kerugian yang timbul akibat penggunaan informasi dalam dokumen ini di luar lingkungan Sentra Medika Hospital Group.

Keamanan sistem elektronik pada masing-masing unit kerja dan cabang rumah sakit tetap menjadi tanggung jawab penyelenggara sistem elektronik yang bersangkutan. SMHG-CSIRT berperan melakukan koordinasi, pendampingan, dan penanganan insiden sesuai kewenangan pada butir 3.5.

Pelaporan insiden hanya dilayani melalui kanal resmi yang disediakan pada butir 6.1.

Meskipun telah diupayakan penyusunan yang cermat, SMHG-CSIRT tidak menjamin ketiadaan kesalahan dalam dokumen ini. Apabila ditemukan ketidaksesuaian, mohon disampaikan ke csirt[at]smhg[dot]co[dot]id.

Cibinong, 06 Juli 2026

Ketua SMHG-CSIRT,

Yosi Apriius

Yosi Aprilius, S.SI, MM

IT Operation Manager

Sentra Medika Hospital Group