RFC 2350 HERMINA-CSIRT

1. Informasi Mengenai Dokumen

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

1.1 Tanggal *Update* Terakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 26 Agustus 2026.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

1.3. Lokasi Dokumen

Versi terbaru dari dokumen ini tersedia pada:
https://csirt.herminahospitals.com (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen ini diterbitkan dan disahkan secara resmi oleh Direktur Utama PT Medikaloka Manajemen berdasarkan Surat Keputusan Direksi Nomor: 545/KEP-DIR/MLM/VIII/2026 tentang Penunjukan Dan Pengangkatan Tim Hermina Computer Security Incident Response Team (HERMINA-CSIRT).

1.5. Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 HERMINA-CSIRT;
Versi : 1.1;
Tanggal Publikasi : 26 Agustus 2026
Kadaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Kontak

2.1. Nama Tim

HERMINA – Computer Security Incident Response Team (CSIRT), atau disingkat:
HERMINA-CSIRT

2.2. Zona Waktu

Jakarta (GMT +7)

2.3. Point of Contact

2.3.1. Alamat Kantor

Gedung Hermina Tower
Jalan HBR Motik Blok B-10 Kav 4
Jakarta Pusat 10610

2.3.2. Nomor Telepon/Whatsapp

085122527575

2.3.3. Nomor Faksimili

-

2.3.4. Alamat surat elektronik (e-mail) kedinasan

csirt@herminahospitals.com

2.4. Informasi kunci publik

Kunci Publik (Public Key) dan Informasi/Data Enkripsi lain Bits : 4096
Key ID : 1073F95588909FC1
Fingerprint : 0EFF 568D 37B0 54D1 AAEE B4AB 1073 F955 8890 9FC1

-----BEGIN PGP PUBLIC KEY BLOCK-----
xsFNBGqOP2YBEADTWXn1+9PFN8x42Wj7qkqavVUvhFO9vHZjH/o4r8/NY1Bp
EvjjBsvfTNbwf/daswId8NdqUk6noOEKvC6SbspoOVICIOwBZXyXYg8eYC21
HCfw7GBnW7Lf6As8xZdVxxoSwkWH0pg34PHreNTae2svG+XB0320tRB6iqW+
r5ph658Z6dQonLP2cNt5cJ8EXLbewfmFEV+alTvcIrxaZVtpOlmh1ZklyZke
9/ZOjoOAgJ4eUoU0BFYDM2ec5B5Qv5zNK7hxNQdtL1MV5BJQ5egfa/arDjCj
WW6fWY7RyzPRkp36OPwokPwKxyWDtjaqJTBzTsMqpfIktMa90Lto/fLWxk5X
26F8ldb8U9eTpXHbTUD3ad2b/MiiKPH+IbbMkEXkevoKkeDGKKXSQ/OLbpP9
aYlof/eNlShmTBoLcDGz5bctbq/pbyaUvhu0VYFQII149rd1H4ltaizEPckN
CwO8X6PIS9z5R1x8Nzg7R6+Jv1FFtm6Hx2E0Vv4Ds00UTreCt+rdZi+vS07K
P2G5gLjqHgM0AdcDMuCoC3A8V6bBCgQHh8sxMXuux3h4+XWrM1Dx51dQfFX0
zUlVS3euBzW0oHQmUHH4TAj7TpBng2yS7gtwT8ZukMX6/IFZt5IFf4GYeUpf
HkaEME1BTFvHF4VUqo8zzaG0NdpHjHZwzliAvQARAQABzSpIZXJtaW5hIENT
SVJUIDxjc2lydEBoZXJtaW5haG9zcGl0YWxzLmNvbT7CwYoEEAEIAD4FgmqO
P2YECwkHCAmQEHP5VYiQn8EDFQgKBBYAAgECGQECmwMCHgEWIQQO/1aNN7BU
0arutKsQc/lViJCfwQAA/oMP/33gV5Isrk2bV3X7fECML0ng8khZoXrves62
VS/+Pk2E4CmbZ9yIRMhy0WZq9fb/iR5DsMn45Qp7jkhoxZC0XO8NMzw5HOaz
W9ULlt7bIeM0C+datgJHsFowUukMaYHpcn37lcdm5jR98ODIkCxzdv/zuq3d
PuRoI2+SQIH99TlMEbUzNLuOnN5yzpPuO0qFH+dnBkWLemrwvCVtR8qtcOkT
R/14GVBD0tbwxb9nZykZhY5dQENzoDgKqrMT0+F5xuLsl+7LGK2FOPzwRugG
82T+mKRxxox7hl39NnrZvM1dRblL3rAudKk62FouYrcYWtYqYmkoa/M33Otp
QQmUY4K1LjA2+3ntRtThsqHuPktbsH/rL6qFZF+vSd3v25zr35j4WPgn4fhq
UA3kX1GSNdZdFASdcIEnR2nA5Bz8Ebb5xXXnS1iDRvCVQfoQtZdWTTnXlJTC
vt7K1rHBTSo+1gMonhMLZgcmOtqJO99HVbZlE0zBX5KN50gZiH1dFNykRyG5

lyr4bfhliIE0wPihbeKQZ5MRe2Uoci+ZWLbAEb5/yaZ5m7oht169qXSO+wPL
mKo2WLdHtt6PgDwvqBHRNQXYz5+UlzhudGfFlGQh+BLNGMA5Ko4odx5QqZQ3
2J74FD/fr5wFDfKvZF4dEY19eSz6QXTvNrxoXGaChjCzONLCzsFNBGqOP2YB
EAC43ocspZT/E2FiAXzAokeiB1alDw4P3GkN2Fx99xv9QDsz/R5OQmKWXgVp
r50f9oCVeIPVArYTO+a5F0SBRL/lk021WHKLeQ3Eeqrhxeyb9pttt5rWmZz+
GEAFSAIlgHwasZd7gUg1LdGKO+IQWVk8j/kcS4ClaXEQ2qBAJICGQRhaPaBZ
zjpeUK8K/sOZNXg+oi/TloHstfVVxOOBFzFyzS3tMY5EJzUeowOXIuwuzVPU
wrhno2V2o0IgxiMoBobQ4Jz0e0k9JZyIIPvUoLiotqujNoxuHzKTauc6rt6S
p9eqsslpK6Gc98xHv30G0gheCgzob5PVIJtqK0T/LhtH5D6iVrN8+KzS44d4
TP+0bnfdtNd3LJVa/Zc7Am27hr/J1gLlKwbL8toBVSCIay32Iwov37P4fnPD
XdYtOPWXGtJ1z+uRM3ihBI6N4XlOGiVrtVZo3PAD2Iz0dNfwa3D5zkrbaNcI
ag19AJCkuVc/JbM3P/dsea2Q7u6a9mFe2iswpYH2Dv7KgM7xkbdDO4UBDeBU
uiQ0BA8PkipAyAr+LsslX7nVJzXePqcfyg/UX9cUEQBpWTv3k3ESWwgAE7FC
b6ITqI+3iSoFCIgITO8WuDQlLv7TsdWpYVbWE3s2r0oMkg9tyoJ/GFcwcH13
1dreV4Vw1fjmwaX2RK5kg/gOQwARAQABwsF2BBgBCAAqBYJqjj9mCZAQc/IV
iJCfwQKbDBYhBA7/Vo03sFTRqu60qxBz+VWIkJ/BAAAXvxAArMKYHneIS7O7
8k92Ju4J+svUBXPRoA4Kj1psjZY3fLot/btvx38Ly+p0Rzt1VW88ocKtnWBy
u176SOlErrCzBYaFnYALxjiHr5e2GnPiol3M+94SPT4L1Mmj1JZV0gudcROT
PJn64SMXYCjZWDGX87LkUEn3i+KD+NbW2M0NP0ZvNDJPQgmV8/IO73Kng6BS
nMnuwQ645/np0WkWzohA8o5RuOb8pinvwRure+m2Fthr3xVKI+gO81zm60PT
bJlcAsnurjgARWhRxSCbHXJqOm2dcKKDWps8I6CUOoJXLfX3k/4gGw/il8eU
WrCuY06kSInQU3D4lL3ta37Z4rWzFk9umMyRRAgCoJ8lYHwnAZGBm4jD9SyQ
1rbNqdc2QP8mFPrByTlflN/aiaMX5ydWtNTmt5slylT/mUcgR5rkHMMXjZua
eXoJjoIEOfeUi0yI/e6w6AVKNmMC9Tfe3y2kAhEsN8xpEMdIZImAidGOxWLm
/ADb3jX16rs/i4paR6XjfYbcGwC7NWaEFYOFgLlcsKcyDEqFzB6MtxZlKvET
8N0uClnZG/8P9Crbeg9HvHWkUmHMy6aodZzOgSK8w4geaATIRPFrEf0g+KMt
1OAbrzOWqehC5I6sc3AMvhT3uUGAVMrY7ASmKfgem9tP/8m/BZ5mOQ6KeYpR
gzbWUeHftCI=
=CsQK

-----END PGP PUBLIC KEY BLOCK-----

File PGP key ini tersedia pada :
https://drive.google.com/file/d/18cF2C5HKWPDl2x-jIlrc1E6C9GSroEGk/view?usp=sharing

3. Tentang HERMINA-CSIRT

3.1. VISI dan MISI

Visi

Visi Hermina CSIRT adalah Mewujudkan pengelolaan keamanan informasi di lingkungan Hermina Grup sesuai dengan prinsip keamanan informasi yaitu untuk menjamin ketersediaan (availability), keutuhan (integrity), dan kerahasiaan (confidentiality) aset informasi

Misi

Misi dari HERMINA-CSIRT, yaitu:

a. Menyelenggarakan kegiatan pengamanan informasi dan pencegahan insiden keamanan informasi.

b. Membangun kesadaran keamanan informasi pada sumber daya manusia di lingkungan Hermina Group.

c. Menyediakan dukungan TIK terhadap corporate service yang efisien.

d. Menjamin keamanan informasi pada aset informasi.

3.2. Konstituen *(Constituency)*

Konstituen Hermina-CSIRT mencakup:

1. Seluruh unit kerja kantor pusat PT Medikaloka Hermina Tbk.
2. Seluruh cabang Rumah Sakit Hermina Group di seluruh Indonesia beserta seluruh entitas anak perusahaan terkait.
3. Rumah sakit dan/atau fasilitas pelayanan kesehatan yang pengelolaannya dioperasionalkan oleh Hermina Group (berdasarkan perjanjian kerja sama operasional/manajemen yang sah), yang mendapatkan cakupan layanan, fasilitas, dan perlindungan keamanan siber terstandar.
4. Seluruh pemangku kepentingan, mitra pihak ketiga, dan infrastruktur sistem informasi yang terhubung secara langsung maupun tidak langsung ke dalam ekosistem jaringan dan Pusat Data Rumah Sakit Hermina.

3.3. Kewenangan *(Authority)*

Hermina-CSIRT memiliki kewenangan administratif dan teknis operasional dalam penanganan insiden serta mitigasi risiko keamanan informasi di seluruh lingkup konstituennya, yang meliputi:

1. **Kewenangan Administratif & Koordinasi:**
    - Menerima, memverifikasi, dan mengkoordinasikan pelaporan insiden keamanan siber dari seluruh cabang Rumah Sakit Hermina, entitas anak, serta rumah sakit yang dioperasionalkan oleh Hermina.
    - Mewakili atau mendampingi konstituen dalam pelaporan insiden dan koordinasi resmi kepada Badan Siber dan Sandi Negara (BSSN), Kementerian Kesehatan RI, Kementerian Komunikasi dan Digital, maupun CSIRT sektoral terkait.
2. **Kewenangan Teknis & Mitigasi Darurat:**
    - Melakukan pemantauan telemetri, audit log keamanan, dan penyelidikan forensik digital pada aset kritis, jaringan, serta Sistem Informasi Manajemen Rumah Sakit (SIMRS) yang berada dalam lingkup pengelolaan Hermina.
    - Mengambil tindakan penahanan darurat *(containment)*, termasuk pemutusan akses sementara, isolasi perangkat/jaringan, atau penghentian sementara layanan yang terinfeksi guna mencegah eskalasi ancaman siber dan melindungi integritas data rekam medis pasien di seluruh ekosistem Hermina Group.

3.4. Sumber Pembiayaan

Anggaran Departemen TI dan Bisnis Digital, sesuai dengan persetujuan pembentukan tim Hermina CSIRT

4. Kebijakan

4.1. Tipe Insiden dan Tingkatan Dukungan

HERMINA-CSIRT memiliki otoritas untuk menangani insiden yaitu:

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

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

4.2. Kerjasama, Interaksi dan Pengungkapan Informasi

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

4.3.Komunikasi dan Autentikasi

Untuk komunikasi biasa, HERMINA-CSIRT dapat menggunakan alamat e-mail dan telepon, jika informasi yang disampaikan bersifat rahasia dapat menyampaikan melalui alamat email dengan menggunakan informasi kunci publik

5. Layanan

5.1. Triase Insiden

Triase insiden pada HERMINA-CSIRT memiliki beberapa tahap diantaranya adalah Identifikasi, Investigasi, penghapusan dan pemulihan. Identifikasi dan investigasi dilaksanakan oleh Tim SOC. Tim SOC bertugas untuk menganalisa dan mengidentifikasi semua trafik yang melintasi jaringan komputer Hermina yang bersumber dari log diantaranya perangkat jaringan, server, dan perangkat keamanan informasi. Sedangkan tahap penghapusan dan pemulihan dilakukan untuk menangani insiden yang terjadi dan melakukan pencegahan agar insiden tersebut tidak terjadi lagi dimasa yang akan datang.

5.2. Koordinasi Insiden

Koordinasi Insiden HERMINA-CSIRT dilakukan antara konstituen dan Tim HERMINA-CSIRT yang berada dibawah Departemen TI dan Bisnis Digital (Dep TI Bisdig) baik melalui email, telepon maupun layanan Service Desk TI Bisdig. Adapun komunikasi dengan pihak luar dapat dilakukan melalui e-mail dan telepon

5.3. Penyelesaian Insiden

Penyelesaian Insiden dilakukan dengan Keputusan Direktur Penanganan Gangguan Keamanan Informasi Di Lingkungan PT Medika Loka Manajemen

5.4. Kegiatan Proaktif

5.4.1. Sosialisasi Security Awareness

Layanan ini diberikan oleh DepTI Bisdig berupa sosialisasi kepada seluruh staf di lingkungan Hermina Group yang bertujuan untuk meningkatkan kesadaran dan kepedulian para pegawai tentang keamanan informasi.

5.4.2. Layanan Service Desk

Layanan ini merupakan portal antara DepTI Bisdig dengan Konstituen HERMINA-CSIRT. Service Desk ini digunakan untuk mempermudah koordinasi dan juga dilakukan untuk penanganan insiden keamanan informasi.

5.4.3. Rapat Koordinasi Keamanan Informasi Dep TI Bisdig

Kegiatan ini meliputi penyusunan kebijakan dan/atau standar keamanan informasi di lingkungan Hermina group, pembentukan Organisasi Keamanan Informasi unit, peningkatan awareness staf terhadap Keamanan Informasi, penerapan pengendalian Keamanan Informasi, dan evaluasi penerapan Sistem Manajemen Keamanan Informasi.

6. Alamat Pelaporan Insiden (alamat online atau alamat lain)

Alamat pelaporan insiden dalam konstituen HERMINA-CSIRT dapat melalui alamat https:// servicedesk [dot] herminahospitals [dot] com/ atau melalui email csirt [at] herminahospitals [dot] com dengan melampirkan bukti insiden, sebagai berikut :

1. logfile dan timestamp
2. tangkapan layar/ screenshot
3. identitas pelapor
4. kronologi insiden dan penanganan yang sudah dilakukan

7. Penyangkalan dan Batasan Tanggung Jawab (Disclaimers & Limitations of Liability)

7.1. Batasan Kapasitas, Kapabilitas, dan Sumber Daya

1. Penanganan insiden teknis (analisis forensik mendalam, deskripsi data, rekayasa balik *malware*) sangat bergantung pada ketersediaan lisensi perangkat lunak, kapabilitas teknis internal, serta alat (*tools*) forensik yang dimiliki saat insiden terjadi.
2. Dalam hal insiden berskala masif, kompleksitas tinggi (*zero-day*, *advanced persistent threat*), atau di luar kompetensi internal, HERMINA-CSIRT berhak merekomendasikan eskalasi atau melibatkan pihak ketiga/instansi pemerintah (seperti BSSN atau CSIRT Sektoral Kesehatan) tanpa jaminan ketersediaan solusi instan.

7.2. Prioritas dan Alokasi Penanganan Insiden (Triase)

1. HERMINA-CSIRT berhak menentukan prioritas penanganan insiden berdasarkan tingkat keparahan (*severity level*) dan dampak operasional terhadap layanan rumah sakit (khususnya integritas SIMRS dan keselamatan pasien).
2. Pelaporan insiden dengan tingkat urgensi rendah dapat mengalami penyesuaian waktu respons (*lead time*) sesuai ketersediaan beban kerja tim.

7.3. Kanal Pelaporan Resmi dan Kelengkapan Artefak

1. HERMINA-CSIRT hanya memproses dan merespons laporan insiden yang dikirimkan melalui kanal resmi (Portal Service Desk dan email resmi CSIRT). Pelaporan melalui jalur personal, pesan singkat pribadi, atau media sosial staf tidak dianggap sebagai laporan resmi dan tidak mengikat SLA penanganan.
2. Efektivitas investigasi bergantung pada kelengkapan artefak yang diserahkan pelapor (log, *timestamp*, riwayat perubahan). HERMINA-CSIRT tidak bertanggung jawab atas keterlambatan mitigasi yang diakibatkan oleh ketiadaan bukti pendukung atau manipulasi log oleh pihak pelapor.

7.4. Batasan Tanggung Jawab atas Kerugian (Liability Limitation)

1. HERMINA-CSIRT berupaya semaksimal mungkin (*best-effort basis*) dalam memitigasi insiden. Tim tidak bertanggung jawab secara hukum maupun finansial atas:
   a. Kerusakan permanen data rekam medis atau sistem yang disebabkan oleh serangan sebelum tindakan mitigasi berjalan.
   b. *Downtime* operasional, degradasi performa, atau kerugian finansial yang timbul sebagai konsekuensi langsung dari tindakan darurat (*containment*), seperti isolasi jaringan atau pemutusan akses sistem kritis demi keselamatan ekosistem yang lebih luas.

7.5. Tanggung Jawab Pemilik Aset dan Mitigasi Mandiri

1. Tanggung jawab utama pencadangan data (*backup & disaster recovery*), penerapan *patch* keamanan rutin, dan penegakan izin akses (*privilege access*) pada unit kerja/cabang tetap berada pada pemilik sistem lokal atau penanggung jawab TI cabang masing-masing.
2. Tindakan penahanan sementara oleh HERMINA-CSIRT tidak menggantikan kewajiban konstituen lokal untuk menjaga kontinuitas bisnis unitnya.

7.6. Force Majeure dan Keterbatasan Hukum Eksternal

HERMINA-CSIRT dibebaskan dari tuntutan kegagalan penanganan insiden yang diakibatkan oleh kondisi kahar (*force majeure*), pemadaman infrastruktur publik nasional, atau kendala regulasi yang berada di luar kendali operasional tim.