

RFC 2350 RSKD-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen ini merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 28 September 2026.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi khusus untuk pemberitahuan pembaruan dokumen ini.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :

<https://www.rskdharmais.go.id/csirt/rfc2350.pdf> (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen ini telah ditandatangani dengan PGP Key milik RSKD-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 RSKD-CSIRT;

Versi : 1.0;

Tanggal Publikasi : 28 September 2026;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Rumah Sakit Kanker Dharmais Computer Security Incident Response Team
Disingkat : RSKD-CSIRT.

2.2. Alamat

Instalasi Sistem Informasi Rumah Sakit dan Rekam Medis
Rumah Sakit Kanker Dharmais
Jl. Letjen S. Parman Kav. 84–86, Slipi
Jakarta Barat, DKI Jakarta 11420
Indonesia

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

+62 21 5681570 ext. 4104 (hari kerja)
+62 812 2508 2350 (Hotline SIMRS, 24/7)

2.5. Nomor Fax

Tidak ada.

2.6. Telekomunikasi Lain

Tidak ada.

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

csirt[at]dharmais[dot]co[dot]id

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

Bits : 4096

ID : 0x38EF5CE4969B9E34

Key Fingerprint : 8FCA ED45 E7D6 F139 0EC0 AF04 38EF 5CE4 969B 9E34

Blok PGP Public Key :

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

```
mQINBGq5D0IBEAC/SB6vMRE7Lzkh5iR6K682D/coXpjJtZEnIRpavPIrXazN9BG5
x/kFeSzzWFFkK3/sJO38hyiYmkPhABIE/po0WUiG7qyJdOAC586FGo6LsJ7BKyFj
CaYza7EJJnYajqix57tzlfdOz3Bgs1LI1UKNtdDRoxvJWIFZpDZQnEHZHhWCF6w
6zjh1vZdTXvcmFygLNIsUc+JU2SqgoYEGXzltkaeDC5BjnrPnm+LmaH3HTWGiqVF
Hu126Z6oKZbfpgvSuMcuRkXNNZ/qzjuLwawPoh8L+Jkb908QrZdtiWAt9YJ13to5
PbdY4YbR8TzdM2t1uM6hFEFRn+vEhW22auZUcm6v8UPDji6zDeqi7K8SuLs5oI52
uF3KBYRy9bPpJKRIRJtzmC0BnPVefy8r5IBjXmiuK7lqzbRCVqyJumZEDqDn+pbm
SZlmy7so/Y0a5CANCg6zeAxZ003t6BRSTbDR3bG+JngjbgF82pDfWETaAokvJlvC
20t+XNGJUv1SUmyuttnY6owzJYos3pTO9erzd1ScmBScDQZNkVYPUX5jgf7ev2bM
ERG0DzlfPjHJagu/EYvnS/ZJdGbAufK7/u+3zkKrfkp8580BtBV8PtT1FIMS/KoK
3inihpXb1aAybJroS06/B3oljV6oW9GE9cZ4M3uniSS6nG7o4h1913RM9wARAQAB
tCFSU0tELUNTSVJUIDxjc2lydEBkaGFybWFpcy5jby5pZD6JAnAEEwEKAFOWIQSP
yu1F59bxOQ7ArwQ471zklpueNAUCarkPQhsUgAAAAAAEAA5tYW51MiwylJUrMS4x
MiwWLDmCGwMFCQeGHxYFCwkIBwIGFQoJCAAsCBBYCAwECHgECF4AACgkQOO9c5Ja
b
njTpMw/7BT0pWV1MfhimpdcXua5KETUPoy410jsvdsFwQbsHCUPe5ddUmwEi92EW
dTJpgrv0A3fxm8UosQ+YLcd06dMCKOmHP0qnnbNPT1v1DOH8qG2IAbRdYz9S8nrB
fMJaun0ROpzDq/D6NQOvdLRKcRp7P3qaRgrXzxtjpJYcSzN/8AiSZPZ+mGgPIirU
/8apCZtADCDAACLnacioDgNIXuKXnWMNy+TqfKsfGAwCFokJhUjMmCZ9wruRxlJF
uKrjsMeo9vGJBCDYfk81Zi4lyl/+ISKjpwJnUzt4aTja/2PxuZSRJbo71n8TZGUv
sA9xWOouKXDlaSR+urXLVg13LYk6Cl149LrXJ7Q0w2bcl4IU7ixESxtETcQ9cuO7
bcalTpEcF5GP/RvpL1aQP+tvghKsQpWoyl30PU0RG+3i5gP20fPqH3aGfQ8pr4Rz
RV99uOzjPvE5PZbwCVyL7JwCHnyA4R4aNFGxEUUs20ZtXxK5q3O+CelV0geyHCg
/Ufju7fuuUoFE7wUIhh3xBzBdfviPT/TZ+3yGW43aJMoY5Nc3E37Jn9vK353XPcc
Id5NTId+w6HC3bN4Xrr/NRTHjscqzmFJMVtjkrYL5jNQKgNSVz3bNqOyoAUiDb9K
C7drg+D273At92DgDCxnlDf/ysd5kpqC9DdtFMSc7QO818rT77q5Ag0EarkPQgEQ
ALXr5gxJ7+D4TtUlom7qf9p4iww4gnyAjDNEsEPyV0JSVF2NxijtZUbLgNg4TFDE
```

```
2AiTuwepTKMiG1pGPYmX+02u+pvU5nHltLNoHt5jr5wv/m4YJqKqP+E0igafgCgu
JIIUrwKPYELSLaZ3yhqHdTCKs1R5DgPFoF84mDHR+fl+hTtccOD6wcM4hICTPdyo
eNabcqZIOz/GGkp7oAeiBjNPX4Jmss5S7bQfgW3kllAvq2C78ZtZd6n7Y7N8Fv5l
IDE7sUwJSlyGLNCnEhrC8NqN9vviD0JBdGw20Em/wBGBiCrq4Ddp1XXywiagtou6
KztzlthOaGLWjtF5MgZ96nyqeCvvhxNg4EzTkoSdrEEHY+BOxuCcIsFQeRlySjdh+
L6NOvv4p2M/IUDyPpPyHraieFf6/fVzsJNQ6EIPxRbL/bSlajuZrcN61RvahOMYu
nK3DGvUMj0DUbCzf4TtdXNJVsWc0hGFFUDeeBXadYUrKyrkpwMwNroNQa3F3z6q/
LxbahDvaF5DnRmrnxYxLU/7EPDBfnzqrNbhYCKWHtklhqglVDH9/w0ol8WbKbe1G
wPZ+bicTKwNEshUwCsT/odberMaYje95wAixmyPB4w9afmO7gOG/byB/FObTKa6B
X+yqdOmDB+P9fYYCdu4dPY/tLa7/TZUxqBE8A5hezqt5ABEBAAGJAIGEGAIEKAEIW
IQSPyu1F59bxOQ7ArwQ471zklpueNAUCarkPQhsUgAAAAAAEAA5tYW51MiwyLjUr
MS4xMiwwLDMCGwwFCQeGHxYACgkQOO9c5JabnjRxRxAArN3Zt9uIRLqkohx0Yc+V
hHLhODR9dKTq97norrFMMAZITpzUA6+jczxcBG6vfe150x+D1xruxHB29IRC5f3g
KG94vWhzknici2OijMn/pgoMm4GSTXhCgINPKOTjP8NCDxarq9wy1UhgMEe6u/zG
Sflppq8QtBtdUrw29EVhiYOx+I7YRk57w8SsfRMYB72zX5+JFbmfJIYA9CIZocsv
rpVD15YUbnAK08fxEkLK882TS7iddU7RJg+XhMUPr5atqCdvmHWirtDxSh802pG6
UhnmlLoTuHTk7GzVrvX9FLEHeINQPM0+JrHGgthqElahPZ4rqGU9AThQaL8gWDy5S
KwhW2EvHZitqchqbo/MFBMxoEst+LNsU1CQBWdo2sYaTHCwBP/+DCpGIH9A5wmui
VXhhZdHAI1URDK0jOb2Rk9avHIQpUBWg0j5CCecZU2ukOlyJKTWKJHpbI2TZqvBs
vyp8AzajPeR+u6RLKDh1Y25d8FOo63p4PuZnhScc4S7HJpZ1Dgpl5lajlyLE8XK9
6MzEN8M4w56HVouUhh2WpFbVvevdmpKMrFL+IPYe0AxxR1CU7mzeqcUcdHAcuW7jV
wLczBpry4mwZJVvoMXUuccWhK7DT2YkH01oEC6cECc9ju+1iDTDuZbKzpUwsLKWL
hULhuQjrtR4IUSe1ARB1Mwk=
=wCun
-----END PGP PUBLIC KEY BLOCK-----
```

File PGP key ini tersedia pada :

<https://www.rskdharmais.go.id/csirt/publickey.asc>

2.9. Anggota Tim

Ketua RSKD-CSIRT adalah Kepala Instalasi Sistem Informasi Rumah Sakit dan Rekam Medis, dengan Pelindung Direktur Utama dan Penanggung Jawab Direktur Layanan Operasional. Anggota tim terdiri atas Sekretaris, Tim Legal dan Kepatuhan, Tim Komunikasi Publik dan Narahubung, Tim Monitoring dan Pemantauan, serta Tim Respon Insiden, sebagaimana ditetapkan dalam Keputusan Direktur Utama Rumah Sakit Kanker Dharmais Nomor HK.02.03/D.XII/9736/2025 tanggal 4 Agustus 2025 tentang Tim Computer Security Incident Response Team (CSIRT) Rumah Sakit Kanker Dharmais.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak RSKD-CSIRT

Metode yang disarankan untuk menghubungi RSKD-CSIRT adalah melalui e-mail pada alamat [csirt\[at\]dharmais\[dot\]co\[dot\]id](mailto:csirt[at]dharmais[dot]co[dot]id) atau melalui nomor telepon +62 21 5681570 ext. 4104 pada hari kerja Senin–Jumat pukul 07.30–16.00 WIB. Untuk kondisi darurat, RSKD-CSIRT dapat dihubungi melalui Hotline SIMRS +62 812 2508 2350 yang siaga selama 24/7.

3. Mengenai RSKD-CSIRT

3.1. Visi

Visi RSKD-CSIRT adalah terwujudnya penyelenggaraan Sistem Elektronik Rumah Sakit Kanker Dharmais yang aman, andal, dan tangguh terhadap insiden siber untuk mendukung pelayanan kesehatan yang bermutu dan keselamatan pasien.

3.2. Misi

Misi dari RSKD-CSIRT, yaitu :

- a. Menyelenggarakan pemantauan dan deteksi dini terhadap ancaman dan insiden siber pada Sistem Elektronik Rumah Sakit Kanker Dharmais;
- b. Melaksanakan penanggulangan dan pemulihan insiden siber secara cepat dan terkoordinasi untuk meminimalkan gangguan pelayanan;
- c. Melindungi kerahasiaan, keutuhan, dan ketersediaan data kesehatan serta data pribadi pasien;
- d. Meningkatkan kapasitas sumber daya manusia dan kesadaran keamanan siber di lingkungan Rumah Sakit Kanker Dharmais;
- e. Menjalin koordinasi dan berbagi informasi dengan TTIS Sektor Kesehatan, TTIS Nasional, dan pihak terkait lainnya.

3.3. Konstituen

Konstituen RSKD-CSIRT meliputi :

- a. Seluruh unit kerja dan pegawai di lingkungan Rumah Sakit Kanker Dharmais;
- b. Seluruh Sistem Elektronik yang diselenggarakan oleh Rumah Sakit Kanker Dharmais, meliputi SIMRS, Rekam Medis Elektronik, aplikasi layanan publik, jaringan, dan pusat data rumah sakit.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan RSKD-CSIRT bersumber dari DIPA Badan Layanan Umum (BLU) Rumah Sakit Kanker Dharmais.

3.5. Otoritas

RSKD-CSIRT dibentuk berdasarkan Keputusan Direktur Utama Rumah Sakit Kanker Dharmais Nomor HK.02.03/D.XII/9736/2025 tanggal 4 Agustus 2025 tentang Tim Computer Security Incident Response Team (CSIRT) Rumah Sakit Kanker Dharmais. RSKD-CSIRT berwenang melakukan deteksi, analisis, respons, serta pemulihan terhadap insiden keamanan informasi dan Sistem Elektronik di lingkungan Rumah Sakit Kanker Dharmais, serta berkoordinasi dengan TTIS Sektor Kesehatan (Kementerian Kesehatan) dan TTIS Nasional (BSSN) dalam penanganan insiden yang memerlukan eskalasi.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

RSKD-CSIRT melayani penanganan insiden siber dengan jenis berikut :

- a. Web defacement;
- b. Distributed Denial of Service (DDoS);
- c. Malware, termasuk ransomware;

- d. Phishing;
 - e. Kebocoran data, termasuk data pribadi pasien;
 - f. Akses tidak sah dan eksploitasi kerentanan aplikasi (antara lain SQL injection).
- Dukungan yang diberikan RSKD-CSIRT kepada konstituen dapat bervariasi bergantung pada jenis dan dampak insiden. Prioritas penanganan ditentukan melalui triase berdasarkan dampak terhadap pelayanan pasien, data kesehatan, dan Sistem Elektronik kritikal. Insiden yang berada di luar kapasitas RSKD-CSIRT dieskalasikan kepada TTIS Sektor Kesehatan dan/atau TTIS Nasional.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

RSKD-CSIRT melakukan kerja sama dan berbagi informasi dengan TTIS Sektor Kesehatan (Kementerian Kesehatan), TTIS Nasional (BSSN), CSIRT lain, serta organisasi terkait dalam lingkup keamanan siber.

Seluruh informasi yang diterima oleh RSKD-CSIRT akan dirahasiakan. Informasi hanya dibagikan kepada pihak yang berkepentingan sesuai kebutuhan penanganan insiden dan ketentuan peraturan perundang-undangan, termasuk ketentuan perlindungan data pribadi.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, RSKD-CSIRT menggunakan e-mail tanpa enkripsi dan telepon. Untuk komunikasi yang memuat informasi terbatas/rahasia, RSKD-CSIRT menggunakan e-mail yang dienkripsi dengan PGP.

5. Layanan

5.1. Layanan

Layanan yang diberikan oleh RSKD-CSIRT yaitu :

5.1.1. Penanggulangan Dan Pemulihan Insiden Siber

Layanan ini berupa tindakan penanggulangan dan pemulihan atas insiden siber pada Sistem Elektronik Rumah Sakit Kanker Dharmas, meliputi identifikasi, penahanan (containment), pemberantasan (eradication), pemulihan, dan evaluasi pascainsiden.

5.1.2. Penyampaian Informasi Insiden Siber Kepada Pihak Terkait

Layanan ini berupa penyampaian informasi mengenai insiden siber kepada pihak terkait, baik internal (Direksi, pemilik sistem, dan unit terdampak) maupun eksternal (TTIS Sektor Kesehatan dan TTIS Nasional) sesuai ketentuan pelaporan.

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

Layanan ini berupa penyebaran informasi peringatan, imbauan, dan rekomendasi keamanan kepada konstituen untuk mencegah dan/atau mengurangi dampak insiden siber.

5.2. Fungsi

RSKD-CSIRT memiliki fungsi-fungsi dalam menjalankan layanannya, antara lain :

5.2.1. Fungsi Utama

Fungsi utama yang diberikan RSKD-CSIRT yaitu :

5.2.1.1. Pemberian Peringatan Terkait Keamanan Siber

Pemberian peringatan kepada konstituen terkait ancaman, kerentanan, atau insiden siber yang berpotensi berdampak pada Sistem Elektronik Rumah Sakit Kanker Dharmais, berdasarkan hasil pemantauan internal maupun informasi dari TTIS Sektor Kesehatan dan TTIS Nasional.

5.2.1.2. Perumusan Panduan Teknis Penanganan Insiden Siber

Penyusunan dan pemutakhiran panduan teknis serta SOP penanganan insiden siber yang berlaku di lingkungan Rumah Sakit Kanker Dharmais.

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

Pencatatan setiap laporan/aduan insiden siber yang diterima, serta pemberian rekomendasi langkah penanganan awal kepada pihak terdampak.

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

Pemilahan insiden berdasarkan jenis, dampak, dan urgensi, dengan prioritas pada insiden yang mengganggu pelayanan pasien atau mengancam keamanan data kesehatan.

5.2.1.5. Penyelenggaraan Koordinasi Penanganan Insiden Siber Kepada Pihak yang Berkepentingan

Koordinasi penanganan insiden dengan unit kerja terkait di internal rumah sakit, penyedia layanan, TTIS Sektor Kesehatan, dan TTIS Nasional.

5.2.1.6. Penyelenggaraan Fungsi Lainnya Sesuai Kebutuhan

Penyelenggaraan fungsi lain sesuai kebutuhan, antara lain audit atau penilaian keamanan (security audit or assessment) terhadap Sistem Elektronik Rumah Sakit Kanker Dharmais.

5.2.2. Fungsi Tambahan (Lainnya)

Fungsi tambahan yang diberikan oleh RSKD-CSIRT yaitu :

5.2.2.1. Penanganan Kerawanan Sistem Elektronik

Pemindaian kerentanan secara berkala terhadap aset Sistem Elektronik, analisis dampak kerentanan, dan koordinasi penerapan patch atau langkah mitigasi.

5.2.2.2. Penanganan Artefak Digital

Akuisisi dan preservasi data, log, dan artefak digital yang diperlukan dalam proses investigasi insiden siber.

5.2.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Penyampaian hasil pengamatan terhadap potensi ancaman siber yang dapat berdampak pada Sistem Elektronik Rumah Sakit Kanker Dharmais kepada pihak terkait.

5.2.2.4. Pendeteksian Serangan

Pemantauan jaringan, sistem, dan aplikasi untuk mendeteksi aktivitas mencurigakan, anomali, dan serangan siber.

5.2.2.5. Analisis Risiko Keamanan Siber

Analisis risiko keamanan siber terhadap aset Sistem Elektronik sebagai dasar penentuan prioritas pengamanan.

5.2.2.6. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Penyelenggaraan edukasi, literasi, dan pelatihan keamanan siber bagi pegawai Rumah Sakit Kanker Dharmais.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke [csirt\[at\]dharmais\[dot\]co\[dot\]id](mailto:csirt@dharmais.co.id) dengan melampirkan sekurang-kurangnya :

- a. Identitas pelapor (nama, unit kerja/instansi, dan nomor kontak);
- b. Bukti insiden berupa foto, tangkapan layar (screenshot), atau log file yang ditemukan;
- c. Kronologi insiden dan Sistem Elektronik yang terdampak.

7. Disclaimer

Tidak ada.