RFC 2350 MK-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 2.0 yang diterbitkan pada tanggal 21 Agustus 2025.

1.2. Daftar Distribusi untuk Pemberitahuan

Menjabarkan pihak-pihak yang menjadi daftar distribusi untuk pemberitahuan RFC 2350, disesuaikan dengan kebutuhan masing-masing CSIRT.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://pustik.mkri.id/ (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP *Key* milik MK - CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 MK - CSIRT;
Versi : 2.0;
Tanggal Publikasi : 21 Agustus 2025;
Kedaluwarsa :

2. Informasi Data/Kontak

2.1. Nama Tim

Kepanjangan dari Mahkamah Konstitusi Computer Security Incident Response Team. Disingkat : MK - CSIRT.

2.2. Alamat

Jalan Medan Merdeka Barat, nomor 6, Jakarta Pusat

2.3. Zona Waktu

Jakarta

2.4. Nomor Telepon

021- 23529000

2.5. Nomor Fax

021- 3520177

2.6. Telekomunikasi Lain

-

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

csirt@mkri.id

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

Bits : 4096
ID : 1F6EE3D77367AC4C
Key Fingerprint : E316 63C6 8491 C5EE EA10 2BBF 1F6E E3D7 7367 AC4C

Blok PGP Public Key Misalnya :
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Mailvelope v6.1.0
Comment: https://mailvelope.com

xsFNBGiQcesBEAC5fMP6GNh342PsjqKVywivuavUdJCoFdCW0oLtOxn/IgaO
QV9xtAjW9s5RxpvoDzQ9lcfOLeTktJ1q6SqeJ9IDHSQjEO+S00f7l8mr3sK3
ZrI73/Umu+YCkIhYwm7WAk6uQuhzHFHA9buLRFAEH1LHfo5Lqhf06ZYkbqOD
eTBiVzEhBf2SZzlTl0z5FV89Ey8tmiqjcynbvm/AHDKuOmR0NsMgYrhstrZR
RVn0fH3GswCwz38hmMhDPHQCeJiwqGg+NBiLMtpGWR9ECCa3AP+MnbJZcrFY
CLmpqAYbPY+sZnatA7sga+ybu6bPMdVCeql32uZXxa//yHM2SWnMJtPhyLm0
4JOvhJ50+A+XGr/1wsKL4roGwQElzS3tPKcLDuUVIo9xSr//ZRpvWJIPHA3Y
6qDLG50fQsPVSfqK/7na7T1YxPunWNDyWW8EUCYzvk7Meg4A4pEMNpd7xrNx
NN5dlG94fcKsMc3++LriP/ela4O0IEvBRrqQ12Do3iVAdII5ba+9nNdSIi1T
Dj1gKynyrlwg6rDPsuzWNb+rPZOO9UMgfLiR0Em0xnZaUx0lJdcp828yHgGv
TlXxWhmNFhFmCiDD0UE/XyXIhVbsMrWoQtfVdTDH/Yrsgixn0OMnUWKLVjVi
BxuUHf+3EkyR3kiLd4fIEqPxGROP1u85dsuW1wARAQABzRhNSyBDU0lSVCA8
Y3NpcnRAbWtyaS5pZD7CwYoEEAEIAD4FgmiQcesECwkHCAmQH27j13NnrEwD
FQgKBBYAAgECGQECmwMCHgEWIQTjFmPGhJHF7uoQK78fbuPXc2esTAAAcZ
QP
/1Kg5E9fjNFgrbr/dRfb3YcrA43aTyzg8bY4tDf9Uc3hF87brVXLK7Gd7YqP
wuvXuVX9tkBiiLNIB9ib3IzbFWYxOyih8c6hX8qCNTLA9FHxODP7wlIBp9Zn
lVMZsPBdjoRU4H+63XvTJoLuNn9I6cuVl+yMaT46XdMGrmdq+BazcFunJpF0
Jm8xZ2D2ympfzXnFYG+yxycDJo8UXgRxBQyWg2tnEx1MiZ0kbjRj7+eUbZdK
4CUoInNg0+sTNqLJTR3xYDv9+/Ndmi5d5dpYxCH881jGEK5GvKV2Tng8Su01
4+UODh6/jiyuMt3vV4NeU7l9VRM0ETJnHfQ5rF/nw5QghSiz7yi9zuXBji80
4ZIhY2mQMpRzabmWB7N8nxRsW5Rt17fHqODpNK7d0/lF5gSgArSQ4nVz6ws4
bcY/hhH6uUzVSxcBGvUiRCiYWKQ9+OygrNXGEjLvk9LaFCNfDKfyRNUZ/Aj2
/vRcrjXnfN2zMYs6Hlm7tma0jSwi3Ua98g28K87hsW77FHVPzcQTS6I5ks7D
//Tqi4Gj8JwVSnsLTO3jFE8Nk4u/K5dEK7nIVgPXICDklU7YMbBHfD40i+Rr
335Pe7SXNW9eLmd9PXIAfDHTCeRwYvs06GLXtjAxtGb82hf0B4ZFFSimrh8Q

L9XRJLcHDG8jIMeNN8GZbE0nzsFNBGiQcesBEAC5NJZ9WnoPcZkNLHCtB+Ja
8R1rVtj6pceO7HUs1JfTlXJBGmx108GCat35fnotBv5dSGwLP5eHkoz0Y9Dw
/F6OZ4sCUp7o7jNNNYDpEoWFTR/TbuiIXyRrOyDqFZ8u8xO4higmp1zSg953
yNVA3SrG8kyGs236+FSc909pA11MD9aY+Rl6Pufj6tZ2Xory/iqKnsiMlyqp
BADphpHMwA1YdiZNBnC2f/ZTtKhFxByvWPptxS2Lw5Mh91PNVYHTFAnddxJ/
/xIrBL7rYy5EhbFus7fZC9q2+UpK9armLx0Z2KFDJaXcDJVQsp8fSQ333JMD
Cs3qlR3jE7/l6+TxBANVCuiIm/NtUfAzfo6MYtYpOUlGkCAJFU8XS9HZNX4U
hhuAx5MTB9P6Vb/hMFJXr4BVNYAprebjNZxKhpNvbrF8j4StCzy5P5jPVvZt
OPcPY9xqCbb20V/bAhPsANM0UTAHreptRhp4kAl6g47NTP+eyXx8Vq2KJ3sC
jGFj9TegD9KmSU46raECHWvrz1D5uk0RQJFnX9jYDKnkPhTJ7yt8nnjUOScU
h/St+WFM/86+qB81WdiF8fT3cH9XN/30663KwFhy6jmrjRrMQECu5JDgKmq4
Qmtgu0f3NokTbBifUqGzlJHNgds1Sl/mPSdu5F/TEXefewvvRhZqiyfjH2oz
OQARAQABwsF2BBgBCAAqBYJokHHrCZAfbuPXc2esTAKbDBYhBOMWY8aEkc
Xu
6hArvx9u49dzZ6xMAACbsg//WvsBwyRcZXpP6mIpRJjcFwx8g9OnN/7pX0FX
TlKnMe4+mwH5NagFNhbLzpP9fp9n6+kYQrtX+QMyOQu8ViR4azUVmlgvdOpQ
pvuBSFF0wbLGJRy/BCXnawfYXRlZQmQE/vLv35xcTEsgp6uCwnKBuvlr+uUf
oNZFF+pOw+dTxVZqLm1yLpgI2NH1Pc/KmH2kjD+RWmTiZQOe/Pef2qO/ySm/
yC4qYRN8jMWhkjOwAAZhUdEbdixfaH8n/Uhhr1Pul22+CWNNGyrjQNDFN392
ccCb+kntB36DzQ6rYGOzGCXSa491HNupLNZAao7KuO05x2DBFG5WEdGlMPy9
Z8FikxqqGaItJf/ocwXaOJLjeD2ycV2lmaHZRa4fJ5dzXFD6RtCMTKlX/UsZ
40c4SZUFBx3Vj3y9bBoeQzpxLihqKtFwLbIlzgXMd7UiTFlqJeZNOn6JGtcp
6iGhlFmTdIcu+GtDr1Bfzw+Tc92ffueRx/iXLw85mLY3riiQvk7wIvCNSQGU
YWl1kcDAuDmCPI8dktf7biasqYbtTyjMQte6pwpe13Mxt+WKpIDJN2bmP4hH
wmqiObP6U2Q0N9+IBqQE8V8qhzYIWLoJ1pOHAZjN3iUfK6uQgulnfTVE8+g4
uaQxmDoFdzczD5YPJbIeq3xeOqj63Jvg6vjFOUyGwVYNLHs=
=fl4a
-----END PGP PUBLIC KEY BLOCK-----
File PGP *key* ini tersedia pada :
https://websitecsirt.go.id /publickey.asc

2.9. Anggota Tim

Ketua MK - CSIRT adalah Nanang Subekti. Yang termasuk anggota tim terlampir di SK

2.10. Informasi/Data lain

-

2.11. Catatan-catatan pada Kontak MK - CSIRT

Metode yang disarankan untuk menghubungi MK - CSIRT adalah melalui *e-mail* pada alamat office@mkri.id atau csirt@mkri.id atau melalui nomor telepon 021- 23529000 pada hari kerja jam 08.00- 15.30.

3. Mengenai Gov-CSIRT

3.1. Visi

terwujudnya pengelolaan keamanan informasi dan komunikasi dalam mendukung peradilan yang modern dan terpercaya.

3.2. Misi

a. Menjamin pengamanan informasi dan komunikasi serta melakukan pencegahan insiden keamanan informasi dan komunikasi.
b. Membangun kesadaran keamanan informasi dan komunikasi pada sumber daya manusia di lingkungan Mahkamah Konstitusi.
c. Membangun kerjasama dan koordinasi dengan pihak terkait untuk pertahanan siber yang tangguh

3.3. Konstituen

Konstituen MK - CSIRT meliputi :

a. Hakim Konstitusi
b. Pegawai Mahkamah Konstitusi
c. Seluruh Masyarakat Indonesia

3.4. Sponsorship dan/atau Afiliasi

Pendanaan MK - CSIRT bersumber dari APBN

3.5. Otoritas

Otoritas MK-CSIRT berlaku atas seluruh aset TIK MK, meliputi sistem, aplikasi, jaringan, pusat data, layanan komputasi awan yang dikelola/diadakan MK, perangkat pengguna, serta nama domain dan layanan terkait mkri.id dan subdomainnya. Otoritas ini juga mencakup personel MK, pihak penyedia layanan, dan mitra kerja yang terafiliasi sepanjang berhubungan dengan pengolahan data atau layanan MK.

4. Kebijakan – Kebijakan

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

MK - CSIRT melayani penanganan insiden siber dengan jenis berikut :

a. *Web Defacement;*
b. *Distributed Denial Of Service (DDOS);*
c. *Malware;*
d. *Ransomeware.*

Dukungan yang diberikan oleh CSIRT – MK kepada konstituen dapat bervariasi bergantung dari jenis dampak insiden

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

Komunikasi operasional dengan MK-CSIRT untuk informasi umum dilakukan melalui email dan telepon pada bagian kontak. Untuk materi yang bersifat sensitif/terbatas/rahasia, korespondensi wajib menggunakan email resmi MK dengan

enkripsi kunci publik (PGP/S-MIME) dan tanda tangan digital, yang fingerprint-nya diverifikasi oleh penerima. Artefak teknis dikirim melalui kanal berkas aman yang disetujui (SFTP/MFT); bila belum tersedia, gunakan ZIP terenkripsi (AES-256) dengan kata sandi dikirim terpisah serta sertakan hash SHA-256. Identitas pelapor diverifikasi out-of-band (call-back), MK-CSIRT tidak pernah meminta kata sandi/OTP, dan pada keadaan darurat aktivasi respons dilakukan via telepon terlebih dahulu sebelum rincian teknis dikirim melalui email terenkripsi.

5. Layanan

5.1. Layanan Utama

Layanan utama dari MK - CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini berupa penyampaian informasi secara proaktif mengenai potensi ancaman, kerentanan, atau aktivitas siber berbahaya yang dapat memengaruhi aset teknologi informasi dan komunikasi di lingkungan MKRI. Peringatan disampaikan melalui media komunikasi internal atau resmi, dan dapat berbentuk email, notifikasi sistem, atau laporan singkat. Tujuannya adalah untuk memberikan waktu respons yang cukup kepada unit terkait guna melakukan mitigasi dini sebelum insiden terjadi.

5.1.2. Penanganan Insiden Siber

Merupakan layanan tanggap cepat terhadap insiden keamanan siber yang terjadi di lingkungan MKRI. Tim CSIRT akan melakukan identifikasi, analisis, mitigasi, dan pemulihan terhadap insiden seperti malware, kebocoran data, akses ilegal, atau gangguan layanan TI. Penanganan dilakukan secara terstruktur dan terdokumentasi agar penyebab insiden bisa ditangani secara tuntas dan tidak berulang.

5.2. Layanan Tambahan

Layanan tambahan dari MK - CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini mencakup identifikasi dan analisis terhadap kerentanan (vulnerability) dalam sistem elektronik yang digunakan oleh MKRI. Termasuk di dalamnya adalah pemindaian rutin terhadap perangkat lunak/aplikasi internal, konfigurasi sistem, serta pemberian rekomendasi teknis untuk perbaikan (patching atau reconfiguring).

5.2.2. Penanganan Artefak Digital

CSIRT MKRI menyediakan layanan analisis forensik terhadap artefak digital yang berkaitan dengan insiden siber, seperti log file, dump memori, file mencurigakan, atau salinan sistem. Tujuannya adalah untuk mengidentifikasi jejak serangan, pola akses, dan sumber potensi kompromi untuk mendukung investigasi serta tindakan korektif.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Tim CSIRT melakukan pengamatan secara berkala terhadap sumber-sumber ancaman, baik dari log internal, threat intelligence feeds, maupun sumber eksternal. Hasil pengamatan dikompilasi dalam bentuk laporan atau notifikasi kepada pihak terkait di MKRI untuk meningkatkan kesiapsiagaan terhadap jenis serangan tertentu yang sedang berkembang.

5.2.4. Pendeteksian Serangan

Layanan ini mencakup aktivitas monitoring sistem dan jaringan secara aktif guna mendeteksi indikasi serangan, seperti port scanning, brute force login, DDoS, malware beaconing, dan lain-lain. Teknologi seperti IDS/IPS, SIEM, dan honeypot dapat digunakan untuk mendukung aktivitas ini. Temuan dari deteksi ini menjadi dasar pelaporan insiden atau tindakan pencegahan lebih lanjut.

5.2.5. Analisis Risiko Keamanan Siber

CSIRT melakukan penilaian terhadap risiko keamanan sistem informasi MKRI, baik melalui metode kualitatif maupun kuantitatif. Layanan ini melibatkan identifikasi aset penting, ancaman yang mungkin terjadi, dan kelemahan sistem yang ada. Hasil analisis digunakan untuk menentukan prioritas mitigasi dan penguatan pengamanan.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Tim menyediakan layanan konsultasi kepada unit kerja di MKRI dalam menyusun, menguji, dan meningkatkan prosedur respons insiden. Layanan ini dapat berupa asistensi penyusunan SOP penanganan insiden, simulasi insiden (tabletop exercise), atau audit kesiapan.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

CSIRT MKRI secara aktif melakukan kegiatan edukasi dan kampanye kesadaran keamanan siber bagi pegawai dan stakeholder internal. Bentuknya antara lain pelatihan daring/luring, publikasi buletin keamanan, poster, webinar, serta konten interaktif untuk meningkatkan pemahaman terhadap praktik keamanan dasar seperti penggunaan kata sandi yang kuat, phishing, dan keamanan data pribadi.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@mkri.id 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

7. *Disclaimer*

-