

RFC 2350 BMKG-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.6.3 yang diterbitkan pada tanggal 16 Juli 2025.

1.2. Daftar Distribusi untuk Pemberitahuan

tidak ada

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :

<https://csirt.bmkg.go.id/rfc-id> (versi Bahasa Indonesia)

<https://csirt.bmkg.go.id/rfc-en> (Versi Bahasa Inggris)

1.4. Keaslian Dokumen

Kedua dokumen telah ditandatangani secara elektronik oleh Direktur Sistem Jaringan Komunikasi BMKG.

1.5. Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 BMKG-CSIRT;

Versi : 1.6.3;

Tanggal Publikasi : 16 Juli 2025;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Badan Meteorologi Klimatologi dan Geofisika - Computer Security Incident Response Team

Disingkat : BMKG-CSIRT.

2.2. Alamat

Jalan Angkasa I No. 2 Kemayoran, Jakarta Pusat, DKI Jakarta 10610

2.3. Zona Waktu

(GMT+07:00)

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikat Elektronik (BSrE), Badan Siber dan Sandi Negara

2.4. Nomor Telepon

08888196196

2.5. Nomor Fax

(021) 4241169

2.6. Telekomunikasi Lain

Telegram (@bmkkgcsirt)

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

csirt[at]bmkkg[dot]go[dot]id

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

Bits : 4096

ID : 0xCEA24612B62A7F79

Key Fingerprint : 4294 7833 E4F7 E536 503A 8B25 CEA2 4612 B62A 7F79

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

```
xsFNBGhcu7wBEACInbWXpbQ9fzOgkQdNFE9J4w9MFsr/4XxBk4Xe3dsiCdf7YvJ2
b9TgFVNC5AW5QJCw/9x9O5dYfrd4awSrtAH3zZZw1v9qllbcWtSaKmpzS3rAXX1R
Kx4vHvZ/rziafKwWNg9iiFmelfnEE4uKVUziw2F55RpriGFAh4xmXLjWgS7YLLd/
YQzXNfWqUwXLnSPC11mMaZKvG9Dr38jdEmQ6lv4d5EJ0pK3tZwuXVN2Pz4+fe8
MO
gdmthGwO1eklxZzUhvUPqMyui3q3nWNKE3Wz+nPG6j87okEs7k4Qc3Wk/V3MB9
3R
luWWYDWI7IR9jiq83eSJNDhjMXCy0rwWYwpYKdWvSO2uSitxxNfhCE93hTSbQiG
U
6KxKR2TJFXInNo/leuuvjD4qNK3lZ9O9dA0Q2K+nCF1/qxztrW/KiQc0d3kt6+7D
bCjvTB1lSr/5Kb68t7gQX80OKpG1gCqqWILYT8qEPjOWGd7PIRfBL01GM/29J1a4
7cGoOFpUJrgD58yuaNzMHfOn4CrGONeyeyESplez1LsXvKK9SIW0McaPbk1/g3V
N
fWPsQ8i1vfc6YyXpvK4Tnw4QVa3bRz3rYv9f8hneYiia4uTzGa5aDsx8g0/HaRyd
5fMWYm7+K2PeRfxr55N8BrysB93y82i546ks3s3g0WxrR31brolzavEocwARAQAB
zR1ibWtnlGNzaXJ0lDxjc2lydEBibWtnLmdvLmlkPslBjQQTAQgANxYhBEKUeDPk
9+U2UDqLJc6iRhK2Kn95BQJoXLU9BQkA7U4AAhsDBAsJCAcFFQgJCgsFFglIDA
QAA
CgkQZqJGErYqf3n4PA/Y7jmG9UT/JoWMv+yh5mjxiNS1QGt6Ksm0wkM+kV1e3T
W
WvPOcPRwM30osksynz/s60zxhF4k1/D5anFiR8EPArXONqvAKPNzy2FW6w3ilHbi
plqEkYandjV6kkJg99uFcdwQxijrTpOiKgvO0pPpABLoSRU+9JXxl/1HIH9zFx0
w3aUsL1oLAXRdAg8cEDb4R/QML494rN5+UE5icez8Viz5YWyW+dLxO0oeoBDMk
0a
y37beFHjOJWaKMpKtWOP6Z2+IIVuE5jy6cuHSRImAGtleftuGmJA+3/y2BMKNm9
Y
```

7R494oyvbWE9qvyr5NckS5tEoHnHya8qeOsYf0ZJWUI0WRdiadVusrDJ8yLXLdKu
MU9VZ8BJNX4q7ZF1fAvvtuu+3zltZCyowq2pTIQEtD1FdbgcgAve+9PasHzFIKf6
vOnYE44oOzIV+3mlsUJwVZgOtXayN9mT89kAtIJcFSEebX2QCN62Vv/Jx409RIIdT
pAQQ1um/ZUYwCVNkaZ4o3zWLoINSOf9X6GZU42G6iERNsI7X+KDDOKP14cTL
8zo
LzhvRJyBMz6HrVC21pwz663Eo+2D5AOEwySvASIsPBhXDmavEjzW2pwJ0tKcGb
9W
jl8lughOI+PEGm5SulTGWkqP/VMLqhL//ZfmNf5Lc0A9xkBRIVP2mWSdWD/dvLTO
wU0EaFy7vQEQAMk0BiewPceZ4r9BXoq17vKkl4pvRipbOm4Tdjnz8DOstiAlCti
dpwTIAS3tv9WptPwLF001IDh7bU5Af0iNoCwlqj+fU9hyyPf3exRZ6wPDw52z9oc
C6QotIP723qrQqn0GLO4flsvOcsZoN5PzKNeHG4DEDkPmrvvWr6FwkaaHJMpcefa
3
x7foV/AKiXxjxtzHxpu7dry9cTobowqzEztDFMc4cf+rytfMtZAbiqnBp2z7q3
9gEmRxerr9GNCmA80AaYfqYML7zBr8hLalNhdNlr8eJU7idzJgSIOOsVR8BBjYPq
Vg1YXcPRhHq9cvi+PQi5SFz81Gj/iBApJIIJMSx+66xmRY52dFZXzcVBwMDYAp9F
3JZZt172Zt3U/mPdhJgJGwifElvSO414opdASLsqjW83xF3mW5fxLmpDKUZ9GQlw
wfKKLx39H8fcjNtVd7m7m4gnVqMPbyDvZfSaN2MXpyBHdPY9i6k6y2rfLy94Le2O
i4MGjRYyQaLYVZSeeOgCZQWhodrsfdPzSNjHV+NfoTjO/73KKEQeuyLLXoD23hK
0
Qwosy82ocY3TICTefOql+vIADj/Tiyz7znRIRh9btlvkujJeKZy3e1TtsEBHr7Fp
LHT5OD6AAs7MDWaXgQ0qltcOV0MWuntcZd8IDnn/6emjgrerC+W7WxzarABEBAA
HC
wXwEGAEIACYWIRCIHgZ5PflNIA6iyXOokYStip/eQUCaFy7vgUJAO1OAAIbDAA
K
CRDOokYStip/eeHhD/9SEKBGaVURd+6loXLiVGVJV6LzIYALi4ynj9yeF7RRuI9S
sE26KbaKP4cOb5ir3TOrKz+omDzNxwQPaSDg69S8tHzzC6svPcgL5WII6jK3Ytlg
gLNi/6GdFu7Fz5d+vVfLfe4K/NYeglsTz7cnRFLK+FtNGZxC1Fw16IDTQL4CdG
ikyn9qJsE90OQ+mloo2HPIhGxXk8nMNzporBmOJ3aTi7jj5qozZZU9iQv0HpnN1
uGZCnUC3ypn0ArtnY/e/6RJzUObBjc4/HcVt5XOG+IWvpw8fBY08Twqe3PpHJn/D
COTjSp3eE2DhvfDqfSl5vs28mhie5npyqOX0Ksdno/bcZ+ZBoEPCncSOx2qDwY
FyfS97hdaU2CiPd0sudrvkNapjdA43MZ3jKpGhaukeTfUlt7e8GNuSBNzZbcM3RU
uXVMPog8wEsK+oY/hGQrZaWQ0Md7/FhR+0anWB8jmrOfVUDkg3p/4I5Q5GMYO
1s
dAqSWwmcHoX1CpyhufYN1C+zdWvWn8Cl88qCjhU5hG5SDvQjSJ1jR9+inl2y398
A
HbAmy5LBjysMMwf6fTQ9CJhrazFpof3MVI9Li2HXAVHpBWtpIDVKkb48qUNRwH3
n
38nL0PXwH/Cg+MTX2WAtK4t9lgWqPNEzRVep9b/i3gTalZGr1zP2UppLbgvaJQ==
=luHe
-----END PGP PUBLIC KEY BLOCK-----

File PGP key ini tersedia pada :

<https://csirt.bmkg.go.id/pgp>

2.9. Anggota Tim

Penanggungjawab BMKG-CSIRT adalah Deputy Bidang Infrastruktur Meteorologi, Klimatologi, dan Geofisika, Ketua adalah Direktur Sistem Jaringan Komunikasi,

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikat Elektronik (BSrE), Badan Siber dan Sandi Negara

Sekretaris adalah Koordinator Bidang Keamanan Informasi. Untuk anggota adalah Fungsional ahli tertentu yang berada di Direktorat Sistem Jaringan Komunikasi.

2.10. Informasi/Data lain

Keterangan jam operasional mengacu katalog layanan Direktorat Sistem Jaringan Komunikasi BMKG.

2.11. Catatan-catatan pada Kontak Nama-CSIRT

Metode yang disarankan untuk menghubungi BMKG-CSIRT adalah melalui *e-mail* pada alamat csirt[at]bmkg[dot]go[dot]id atau melalui nomor telepon ke 08888196196 siaga selama 24/7.

3. Mengenai BMKG-CSIRT

3.1. Visi

Visi BMKG-CSIRT adalah meningkatkan pengalaman dalam peningkatan keamanan siber yang sejalan visi misi BMKG

3.2. Misi

Misi dari Nama-CSIRT, yaitu :

- a. Memberikan pelayanan teknologi yang bertujuan terbentuknya ketahanan dan kehandalan siber yang menunjang tujuan proses bisnis BMKG-CSIRT
- b. Memberikan edukasi dan kesadaran siber kepada pegawai serta pihak lain dengan tujuan meningkatkan ketahanan siber.
- c. Meminimalkan dampak insiden siber
- d. Memberikan informasi temuan kerentanan, potensi serangan serta informasi tentang threat atau intelijen siber lainnya yang bertujuan agar terbentuknya ekosistem ketahanan siber

3.3. Konstituen

Konstituen BMKG-CSIRT adalah Pengguna layanan TIK di BMKG

3.4. Sponsorship dan/atau Afiliasi

Pendanaan BMKG-CSIRT bersumber dari APBN (DIPA BMKG)

3.5. Otoritas

Otoritas dari BMKG-CSIRT meliputi :

- a. Melaksanakan program kesadaran siber bersama CSIRT lain
- b. melakukan pengawasan terhadap operasional sistem informasi dalam pemenuhan ketahanan dan keandalan siber yang menunjang tujuan bisnis prosesnya

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

Nama-CSIRT melayani penanganan insiden siber dengan jenis berikut :

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikat Elektronik (BSrE), Badan Siber dan Sandi Negara

- a. *Web Defacement*
- b. Malware
- c. DDOS
- d. Phising

Dukungan yang diberikan oleh BMKG-CSIRT pada konstituen dapat bervariasi tergantung jenis dan dampak insiden. (sesuai dengan SLA pada Katalog layanan Direktorat Sistem Jaringan Komunikasi BMKG)

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

BMKG-CSIRT melakukan kerjasama dan berbagi informasi dengan CSIRT maupun organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh BMKG-CSIRT akan dirahasiakan. Dalam pelaksanaan kerjasama wajib menyertakan formulir Non-Disclosure Agreement.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi bersifat biasa ke BMKG-CSIRT dapat menggunakan alamat email dinas tanpa enkripsi data (email konvensional). Namun untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat melalui email dinas dengan enkripsi kunci public menggunakan PGP.

5. Layanan

5.1. Layanan Utama

Layanan utama dari BMKG-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan berupa peringatan akan adanya ancaman siber kepada pemilik/penyelenggara sistem elektronik dan informasi monitoring terkait layanan TIK.

5.1.2. Penanganan Insiden Siber

Layanan ini diberikan berupa koordinasi, analisis, rekomendasi teknis, dan bantuan on-site dalam rangka penanggulangan dan pemulihan insiden siber.

5.1.3. Penanganan Kerawanan Sistem Elektronik (Vulnerability Handling)

Layanan ini diberikan berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (hardening). Namun, layanan ini hanya berlaku apabila syarat-syarat berikut terpenuhi:

- a. Pelapor atas kerawanan adalah pemilik sistem elektronik. Jika pelapor adalah bukan pemilik sistem, maka laporan kerawanan tidak dapat ditangani;
- b. Layanan penanganan kerawanan yang dimaksud dapat juga merupakan tindak lanjut atas kegiatan *vulnerability assessment*.

5.2. Layanan Tambahan

Layanan tambahan dari BMKG-CSIRT yaitu :

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikat Elektronik (BSrE), Badan Siber dan Sandi Negara

5.2.1. Penanganan Artefak Digital

Layanan ini diberikan berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi.

5.2.2. Pemberitahuan Hasil Pengamatan Terkait Dengan Ancaman Baru

ini diberikan berupa hasil dari sistem deteksi dini honeynet BSSN, BMKG-CSIRT memberikan informasi statistik terkait layanan ini.

5.2.3. Analisis Risiko Keamanan Siber

Layanan ini berupa dokumentasi kerentanan dan penilaian risiko keamanan informasi yang sesuai dengan standar ISO/IEC 27001.

5.2.4. Konsultasi Terkait Kesiapan Penanggulangan dan Pemulihan Insiden Siber

Layanan ini diberikan oleh BMKG-CSIRT berupa pemberian rekomendasi teknis berdasarkan hasil analisis terkait penanggulangan dan pemulihan insiden.

5.2.5. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

BMKG-CSIRT membangun People, Process, Technology untuk mendukung pembangunan kesadaran terhadap keamanan informasi yang berkelanjutan.

- a. Menyelenggarakan kegiatan workshop keamanan siber kepada pihak konstituen;
- b. Menyelenggarakan kegiatan Drill Test Insiden Keamanan Siber kepada pihak konstituen;
- c. Menyelenggarakan sosialisasi keamanan kepada konstituen.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt[at]bmkg[dot]go[dot]id dengan melampirkan sekurang-kurangnya :

- a. Nama Lengkap, NIP, Jabatan, no.HP, email dinas
- b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan

7. Disclaimer

Tidak ada

Jakarta, 16 Juli 2025

Plt. Direktur Sistem Jaringan
Komunikasi BMKG



Irwan Slamet