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 1.6.1 yang diterbitkan pada tanggal 26 Februari 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/file
(versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Kedua dokumen telah ditandatangani dengan PGP *Key* milik BMKG-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 BMKG-CSIRT;
Versi	: 1.6.1;
Tanggal Publikasi	: 26 Februari 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 Jakarta

(GMT+07:00)

2.4. Nomor Telepon

08888196196

2.5. Nomor Fax

(021) 4241169

2.6. Telekomunikasi Lain

WhatsApp BMKG-CSIRT (Katalog Layanan CSIRT), Telegram BMKG-CSIRT (Katalog Layanan CSIRT)

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

csirt[at]bmkg.go.id

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

Bits	:	4096
ID	:	0xD77CB11C188D27C3
Key Fingerprint	:	BF93 8B46 46D2 23B5 C733 42F2 D77C B11C 188D 27C3

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

xsDNBGe+eVsBDADhUrj8Y0SNoXpIk+v5Z2G5L/db8k76QStBqQmTkjsQcPdcRmIH
MGWKGGYom49NvDr3vkUxtP/Wbg9igj7uHGcE+89v/JyjimBChcWz9oHEYSifDowo
ZP77XXtSvQjAUJLyHK7pxCzuVsAESWAlG/bR3KnizGAcxjj7WHt2rpxODZCZtTIf
eO58l9jSLddlTGtjk8EfzGNop26vemqaHajMmGPs4d8QTPAVluyPHaZWIwQo1UQZ
xRIIyHPbNnWCgUMPBVo7De4wDGm3+WWyM/YS93PXYzUFG1RfvldysGqAxBVH
9sZd
7MBet/AfxbhyjigVXSzYeYWPRlrSFvmjHzXk/HHnOTZrLDrAPvoViEmRYnpXW1kv
sh16uKE/mfgjSO+8oDXn1KpXLJKL4RG7hzlFQktIBIdOq582lE/gDcvCVii9Hlgi
xUNtOcnJK+tBNLxb2cwFjZjADpuxslRLCn7519HOEZCG+aasMBQtM2KFwz9hSEM
3
qg5Nna2LfCQzhoUAEQEAAc0dY3NpcnQgYm1rZyA8Y3NpcnRAYm1rZy5nby5pZD
7C
wQ0EEwEIADcWIQS/k4tGRtIjtcczQvLXfLEcGI0nwwUCZ755XAUJAJ40AAIbAwQL
CQgHBRUICQoLBRYCAwEAAAoJENd8sRwYjSfD8bEMAKbzcf+hlWMVyGBCj8NPr
h8W
ryrKudChQzOh9ADPedAgrYVxJKT/vkrGANen/DNSsG2SmPLrTqgUQ0xOaOmXMd
nD
dySiyjU9kx89hrul95FPLj+gmbYIMh1MwACghRMo9ynAbOfRbs8P0VxfcRy61FRD
7Km9FPS5OQsl9S6HzqGUflxZ/c/n2fIEQ/sgHm3J3t+VbFy7XUNDgdyZCL6PSBQF
PyunY6+xa4DRDefoJuolUEV6uBT48fS+hVzAEYYIL2LqUv/eZ9unOUm0yKPeHp7R
LAKiONTT0T67QZGrX3fHMG41Wji64Ro6m7FKZQVj33IChBfs+L/sKLvMPPJpXeD
H
nlPtGC890hjsGm86ynMLOy3U4TGr3caDI42iUekmopg/ZOp0bhk023u6oVdNfFMA

evyoJEk15k5jC+jJA+hlfMNlJntShVmT4hsHu9VNqgebrk44dN8Tu39HqMA0zA64
YWi6LJ9ebY//WmVsAON0MuxQhYjj5jItRH96kcTKK87AzQRnvnlcAQwAxAlIqVAG
cOTfpWL3JMswpH3amSCFD1UnycarNraaNLZis21YerYg9eDmi0BD0CSuewVHV/R
v
ZJnwEZnG74IEcq481cc32J+kxGKTWfZwh7B0NLW1hdb9b8vcY+rdCTpEffmw+xX6
HxNiZQkUx1ffrQylmLGi9BVNbd0XI1DztiXIt8FQ9vbTt0/06Q3Cwjh+aNKVjCe+
yUYj9H5Ai/HbeHVAhu2susXZnWhVqB9+iaxgumggv0pisGfDway9MtAjMzXAtEwT
ZTjC0YTbeLiGU4mdjePuskNV+8/FV6GHqxxYfFi1Gt9Pk2F8PFyfGIwC+tgXEBPW
wgVndxd6tGQcY1Ey+tXnVMkpoARqTJOs4/o8rVQNRvhpuIXcAG54hdRMrtYlWO2b
a8hAK1XIxWJSDukVKzx+7exNx6rbCLPUwrKT3WMRCdW+ni+4NlGA/eLitV5zq0ry
68abD45F66+YMJcsPi3meDxjTMbLOM2eLlmiiq6kwL1QVHrrKG/dxexZABEBAAHC
wPwEGAEIACYWIQS/k4tGRtIjtcczQvLXfLEcGI0nwwUCZ755XQUJAJ40AAIbDAAK
CRDXfLEcGI0nw56/DADKuhc+PkIUeTOQ2UtH86bFK2jI01gZf71pw07dtoCJvJY6
ldiFVxWveysSU9KzyV0Q5K25ulsMeCN9JHyMiAVVKezN73HkXDqCcR+LKR6gjMu
U
RZKzepQNBvUKKb/AIN9xpjeNVWgGO7bq8c0EPSOXHUT9tkvpfhltzUc1DTryeXq4
ArfX6TLyJvI+arB5Yv5Vf0rN5XI/Pdfsc5AcHOvkMOn5dD2VB0jNynCJFwLNElt6
WgKufL70JNr1WHU1yT7OrPYisb/V0AKd1wzy2CP8RlUzVPVzLCslEn675n84ROjD
NLBSPi/C8SPg979fnYiizu4g4iOHrbpN7PDv6LRr8CMmhVBW1iL5/AF3w6IYynM7
l38BOV5TNljQe0zVEnOkl9h2GYfaYEIKTdj8cIzmswQxzpiGegkVhwy4yjMJVfn0
0AA7xzsbwZIsrOtn07/2iP3p8JfYhPFLOuYBzaPQXmLkLz/TkHN5Fu16/ik3BYTH
Yjvlx1dGcLzhD8gi884=
=/Cqo
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirt.bmkg.go.id/storage/public-key/Publik-Key-BMKG-CSIRT.asc

2.9. Anggota Tim

Penanggungjawab BMKG-CSIRT adalah Deputi Bidang Infrastruktur Meteorologi, Klimatologi, dan Geofisika, Ketua adalah Direktur Sistem Jaringan Komunikasi, Sekretaris adalah Koordinator Bidang Kemanan 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 BMKG-CSIRT

Metode yang disarankan untuk menghubungi BMKG-CSIRT adalah melalui *e-mail* pada alamat csirt[at]bmkg.go.id atau melalui nomor telepon ke 08888196196 pada
Senin-Kamis, 07.00 - 21.00 WIB
Jumat, 07.00 - 21.00 WIB
Sabtu, 09.00 - 16.00 WIB

3. Mengenai Gov-CSIRT

3.1. Visi

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

3.2. Misi

Misi dari BMKG-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 meliputi :

a. Autonomous System Number
b. Pengguna layanan TIK di BMKG

3.4. Sponsorship dan/atau Afiliasi

Pendanaan BMKG-CSIRT bersumber dari APBN (DIPA BMKG)

3.5. Otoritas

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 Jenis-jenis Insiden dan Tingkat/*Level* Dukungan

4.1. Jenis-jenis insiden dan tingkat/level dukungan

BMKG-**CSIRT** melayani penanganan insiden siber dengan jenis berikut :

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) dan aplikasi sibatik.bmkg.go.id. 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:

5.2.1. Penanganan Artefak Digital

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

5.2.2. Pemberitahuan Hasil Pengamatan Terkait Dengan Ancaman Baru Layanan 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.

1. Menyelenggarakan kegiatan workshop keamanan siber kepada pihak konstituen;
2. Menyelenggarakan kegiatan Drill Test Insiden Keamanan Siber kepada pihak konstituen;
3. 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.