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 1.4 yang diterbitkan pada tanggal 21 Maret 2024.

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 : 1.4;
Tanggal Publikasi : 21 Maret 2024
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	:	7976CFDF4B135077
Key Fingerprint	:	8C95 33C6 A8DD 5600 C6A2 7F05 7976 CFDF 4B13 5077

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

xsFNBGX7qpMBEACqr6LYbXPnL+m024TuokZMICWwJLbmiau+vcCOHJDX7miPf
F7V
zv25fx7wxrYDii6mWtpgHPXYS33Ix5J2/eC9cj2jcp+4xkcJSk0xvMzV4WO78WQU
hLyDCINuCTBHGvaGm7Pm2Oh6dxlzCXtsuK1NH0S3V8t7H8fF+ylJWMe+Nzpxhso
a
/icZek/FSatjqdbXunhkphHqTgBdGs8L6qEqDHKY1KIQCcEaln6ZlZmAvPrKLZzb
Rc8mEPoy2uKEQf1MTzvePtrHq0dPzqSEqj3WSQ7gAQdn+YUsboaCdrbduPxeCT
O6
aeMulpM+h5akCgim39Xj4R1TtEC7duhYH9yH3Wo8yBxFXqrseBEH83Gn7e8icfAY
7k5YCQmUzgv5F87+zBwQ9YQUeQ+VcvIj9wZhZ9Z2galJDKT+A+T/vPoBpBcNVG
2t
2+hG5XSriejt2J7QRwiykjpmt55QLRXB4Ex2cG/wG7Kpr7MVIuvXY9411qRAc7W2
q/IzZq4zwXNMVB1yk+I2pdQJaCY2FiRyvBC1AGqFgFko2PSHKkMuCyblBTL7/D2b
xBk8fSz/p4N9P5hV+0TcwNLbZ4MtYiYkkDjdK0yBaOesImdQ7rHbn02FtCVj2m8M
7O6s0STHbP4+6V72ppL2ICdF7sslNWF763LfkljBkZKvTOu1P3difrpjLwARAQAB
zR1CTUtHIENTSVJUIDxjc2lydEBibWtnLmdvLmlkPsLBjQQTAQgANxYhBIyVM8ao
3VYAxqJ/BXl2z99LE1B3BQJl+6qVBQkAnjQAAhsDBAsJCAcFFQgJCgsFFgIDAQA
A
CgkQeXbP30sTUHfbqRAAo+fmeCB1VmhjtKeY8a93scA2jurWriqO/XyoiVU/UxeK
nZntT7misrTkdqfJ5aKVmwPNJWuN2skwWEDaLW/7cn+5+49Y9Q2pr+1awKF8MuL
5
MG2JeP/gY64zhpR18nbVWm62KLD5+JwrFgOdgoPrBew3OcV6RfsLac3mNOxkng
WK
W60VoUOrjzL5wRk2LB0hVR8cPgvX6GXFU3W1/ICZ/AYOjiKvfJd5ASJB20v8rSPN

3xicCuKcZWrl4UHpoqahyW0gBatF1acaB5ev40v3J9KGjXN9Dxt0wKURV8fKKfmY
onSQecHn+tr/b0tJHVC7KAoTTMkj7wzEhQyZaUxjmIcXDNFe2t9szllm/F38VbYW
DG2VTFBO5S9uYitg8qS0FnyXRJ0ZjiFaZRtQ+k8ctRa2tfYV1B5V/q930/ACTaZ7
ERtqhc+U5F4DLNUndjT4gvxeXY6jjUS6nwJ0e9TFR9URxYSCdjuEHCWzOLOjK7aI
4YXO/k4crhPzVvomjc39AtHzDHQ+FtZF6kfWbbqq123eUYJoDunLMV4mo0bY24IQ
JB0wIxe4RqD/CdwKQyxokXpnPKFZj/+fgDcM2WYxVfJ+AkJMqd4ad9qbhNF0i1Bl
7P2JPmJ+I4JXRgmmBq/1w3AYmGSc7rg54xqfNyYMI1z/kndJw+Mfjsggr3Kox6DO
wU0EZfuqlgEQAMQzwtrIYgi1Ct8+L0hJKf+7DUyiq1Qghl6/ZMv7a5d0gVxYvnq5
9luCdmnSY/DkJsqmPyKkWSjqLFbHRaap564oNdx551SH0V5XaOHHLoslUB/Vnu4
8
fWdLlk4+VjkuI9pTYLO3sfIb8Y5eKKCBe/Zy+wXD9ZbUPvZokJq6zoRKEeVm58wp
eg2xh9ZpXa6Twy1iigOWvD3heihiq34S+lqpQ2H6CGFAoav/22/PWVfa2q8971/y
dBBwstUkwSEAGS7Oy1tOBj2QG5tp/3iQnlDRrLkcI7ETEV0BHmpJFo75UAYqxkR5
JiaOC5dtuUvHaPaFH6mXbsmYdzyB1WCumLelXX4R8xQ8KL+IX3EFkhaN8IbL2rj0
zYxTTz7Vs2bKLe+f8aGFRXpa6TK+3rF8yNWeKC0f46LPop/FfFgpo+lI7PyAWdQh
kyGTTSjpk7KoIWARICiE5SGo0w68sS7A3G9PQEnmtybLJ2i0ZWoY/3tnewjCJ2CY
0WVzlBdPc4+UzNtmr2vfc5OM1pt8tesUw/ImxCXXVPMHbR2bVbVheZo4+b44MnB
V
N+5tGo4XRNmpTlh0nSajzisP6i1B/9vpEwqSXbZZlIGISBjcwOtUhSywbTGSQZAD
9vrJWIas4yC7w/6wp6MUeCXgCSDEa61TLY+yHvq7V52VscXGs3qru1NnABEBAA
HC
wXwEGAEIACYWIQSMlTPGqN1WAMaifwV5ds/fSxNQdwUCZfuqmAUJAJ40AAIbD
AAK
CRB5ds/fSxNQdyHOD/oDWehkCI/88ZjVZx+zuzuhscGABoHyDQag1UVrOkrT1vu8
cP+ex0ihs4ElTD4j9B5BukI6uUKxaJpGwUDqwnEhT0HWB3/Ks7YcJyhAjtfFhdp0
VfEzni0AcYud5nQREPd2s7184R9uiwrzmg0JGTLT/CAOof5kHwRFZQlq+tU7nyPG
25mHyaskZ2hf0Z8WBzT57+9/TqrgQuGQ2y8JlJsV4LKSAjTCBtyxgnttHaX/5N9V
FLMpo/mW/e1vYJS98iNQqZ6LXKT5gaXDO2/TurcHTS/ajAt5/rNSq03qrYXgSEUn
cqwa7xkKXwu9/+0bFhS6KseiC6J8IsQexs27414W9KZaNOmtPkCvP0RCQACJIYO
J
4nHzAnXf4JBHY+yLzi2Ox+NZY+pTgUaGIbmI1kDZP5Ej/4mYVehom7f+mYKg1gP4
N7GxdTEZuxfHHgCetveCq9k4wmZCm9yRLzcD6rICgUDWBGEnbOXERzxZgTatR
oy2
i23b70uhVvZmvccrfKIMpX/cuVaJnYI39+RoFkOuSbNxf/lhvtjadK5jn70LISxM
uOKURjLv5/xCikOBEcaq/hmxj7K8/mggy1raWjt5FcayfidPrH82x77Y2DuGsswo
WJIEMCPtxVBCTipBGf6teWn/3KtSOX7Keeq0ktK/LsEsVE566zze97uCcB2RmQ==
=qoaz
-----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 Instrumentasi Kalibrasi Rekayasa dan Jaringan Komunikasi, Ketua adalah Kepala Pusat Jaringan Komunikasi, Sekretaris adalah Koordinator Bidang Manajemen Jaringan Komunikasi. Untuk anggota adalah Fungsional ahli tertentu yang berada di Pusat Jaringan Komunikasi.

2.10. Informasi/Data lain

Keterangan jam operasional mengacu katalog layanan Pusjarkom 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 Pusjarkom 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.