RFC 2350

KIM - CSIRT

Version 1.0

2024

Klasifikasi: Biasa

KIM-CSIRT, CSIRT di PT Kawasan Industri Medan

RFC 2350 KIM-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 15 Juli 2024

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt.kim.id/rfc/rfc2350id.html

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	:	RFC 2350 KIM-CSIRT
Versi	:	1.0
Tanggal Publikasi	:	25 Maret 2024
Kedaluwarsa	:	Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Kepanjangan dari	**:**	Kawasan Industri Medan - Computer Security Incident Response Team
Disingkat	**:**	**KIM - CSIRT**

2.2. Alamat

Jalan Pulau Batam No.1 Areal Kawasan Industri Medan Tahap II, Saentis Percut Sei Tuan, Deli Serdang 20371- Sumatera Utara

2.3. Zona Waktu

Medan, Indonesia (GMT+07:00)

2.4. Nomor Telepon

+6261 6871177

2.5. Nomor Fax

+6261 6871088

2.6. Telekomunikasi Lain

N/A

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

csirt@kim.co.id

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

Bits : RSA 3072
ID : 0x391176B5419D5A41
Key Fingerprint : 0C37 7F94 A472 F391 8C7C A6CE 3911 76B5 419D 5A41

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

xsDNBGaeBMMBDADPhJssmp8/Qzm4Heq9yEzyiLe6q2h7CNtNO91+VAwLwymyct+g
9ERQopM0rozZjGnXsPvhITi2ViSdX3syo6Fw7sSqyBiM+fA75+7ZxDi2qGc0V3gU
5yn7QOgUjNODnER4bHHLWQDS8LIq9YLc1V+sQx/tOwh44osC02rreUEw5I7V/owU
IeuskBRzqqqULcF8uOmMJaVdoc0X68DkxD+4cVEHlhfjPVlcVoT5uIlYP8Eh2S96
M/R2/v4iQnVtvDcMTDZ92mA1kPDWB153k6JC7bDfMN/CQK+M+KFFzbrbJc5bBWZJ
/0fYg9hBmoKLnN94BK1lx74kwueOOKQK2DBIyB0uzo1pNmrGAlgNyYGcuEr/CzSY
AbQoKfugOlWS7uhUqj2Ps5pO/82PXhYbyCQQOjqqQ68i3WytRJh3FgWV+pcVbhoH
QyXwRvtHmDx5VNkaIInEKL5Oj9hYsCt/dOHtVg8b2FlQ+TZOtBArBFNUgvn9pWbQ
eVkvnnRuU8gLfXsAEQEAAc0hY3NpcnRAa2ltLmNvLmlkIDxjc2lydEBraW0uY28u
aWQ+wsENBBMBCAA3FiEEDDd/lKRy85GMfKbOORF2tUGdWkEFAmaeBMMFCQWjmoAC
GwMECwkIBwUVCAkKCwUWAgMBAAAKCRA5EXa1QZ1aQQdTC/4hjZ8PTv1J8ZUsKugx
tb3LneB4d2NqQAsG4QlXAfF3XVVuVCIpDD0ub5MOgRDq9aF91cSZSafa3562M3mr
2QpfJYmTklYN6jt3zzvwbaK8bQ1QT9+cgFaH9oRAl2Y3lVC+eiXIelKjF5+6vEnW
DXn9JzNRrBI+rX8EO1VjhC9lGQTfeVTwQfRe5MHiuKU7Bueyry/VmmW6U0sKaUv6
nfnGFdiG+Jsz5POSN8ky1nsQN+McGmDVFVnADby7kp9NRTkRRpj9laUp7OyBrDhz
V0x6W8e3yhgsmRlEUzHSg5NjI6TbmtWuAdqnMaf45x2mK425g2WjRLzpSEDoVTEl
ZxJLY3+LGE/jre4bAttJ6mjlh1aEb+5l8eF2YXIOXbmb3QCQTsErdlAyx/vbJGrL
FDByOtLObC6gCHLDKcjXCTcqp3UkTOynTXz3Qm36WFFCTes2ROIz7mm3iSP26RNJ
0o9a0Yyh4wLbcYVchTHKYgE4P35rmsEnOmh2zFGIV9Y0WnvOwM0EZp4ExAEMAOjY
MFy9kkyT/hPtnlLEWm8u1VpWd+lc731AUKzgV5zJlzY6jnsvQGMsVHcfX9VN+Ryx
2EtrEUQHs9UH490fOfYHJ2MLR36OYzcEu0UVhD6p/dCKYTrjMG0JXHrrKawvjF7u
hVlGPTBN9kqEXjRLvrjrc8PErmPgd1gfVh8E11/tuDd5hjHA51eJ7X7lIHbRBGJ0
3pEZq/bQlyF7Z6qkyQPmMgFYiTt7EgOWgxZ4y9doLMXw3kh6Y6ZZpTcVQ5LCxRAf
Zw02ITbx9lY+oIMgaaVkZt1ML+3wpft+RnAvquF+BBC3kmybK5Y9bD+Rp7Bwf+Bx
6UltgKFbeckaXEo+VMAJHNFkxOCH+hNL1pHNc09U0sfGdq8m/SJ7y/ymVCd0/Htk
s590hD5w3LbPXjfqbr0iGrb9BtTgcywZV56rSCpZP4DtOUJC7f8SlQMjaqV3+ppI
r8TcJNCG+/1GkZKuhnvLfUwWcRfxHelK/5uC+cFIehurigToVw6HTv3RaBS5mwAR
AQABwsD8BBgBCAAmFiEEDDd/lKRy85GMfKbOORF2tUGdWkEFAmaeBMQFCQWjmoAC
GwwACgkQORF2tUGdWkG65gv+LyTq2N4xm/ADCv9WFEbgcc1dK1PMczetEXdvG2ue
8cmzp6Woipe1RPiVoSLLVnXqcU31kh+kLk8TnYH3k4r5DrdxTFktJ1mgS7wNtDnW
Se2ChHRvwwddQnB9aPkf4oOIXljTKoFjnvFrNM5w7FmxtKvBjZ44JSZJ3ZkXCgw1
UhxWy6JHRcZWvSTjYLjvHhpeE+h2dqHeD0fipVagu+3Qo5WP/ZZZFWgjGaCmTZxN
YtBRhs6uY5kIC6KjUbc8nrHb6ETtqInTTS9b4ZAX8QLWsA1AnLPoZ/HzpaZ5jnqh
YDDwCW5FG+BOSiOnP+FRNVlDfXi3WHGst5rSUj6Pd7HeXmk42v07ZWVionoj1MOz

kJO9KSM6k/CmPBt4mtSHF1R3dT6t3pD2sZ2SlRwi2sOdI8dCyXK1Tcz4kqtJoXnu
C/HwiQtmmAltpWD6R3NKWA0juaQciJFqa5UA6cJ/e9AWYH4h6imPmWvN2c+U8WdK
omeK6eNrWzFVIp5ySRlvqQPh
=SsrU
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://kim.co.id/rfc/publickey.html

2.9. Anggota Tim

Ketua KIM-CSIRT adalah Kepala Divisi yang membawahi fungsi Teknologi Informasi dengan anggota tim sesuai dengan SK Direksi tentang Penetapan Anggota Tim Tanggap Insiden Siber (CSIRT - *Computer Security Incident Response Team*) PT Kawasan Industri Medan.

2.10. Informasi/Data lain

Tidak ada

2.11. Catatan-catatan pada Kontak KIM-CSIRT

Metode yang disarankan untuk menghubungi KIM-CSIRTadalah sebagai berikut:

e-mail	:	csirt@kim.co.id
telepon	:	+6261 6871177

Operasional KIM-CSIRTpada hari kerja, Senin s.d Jumat, Pukul 08.00 – 16.30.

3. Mengenai KIM-CSIRT

3.1. Visi

Terwujudnya peningkatan pelayanan Teknologi Informasi dan Transformasi Digital melalui peningkatan keamanan siber yang responsif dan efektif.

3.2. Misi

Misi dari KIM-CSIRT, yaitu :

a. Meningkatkan kapasitas dan kemampuan dalam praktik pencegahan, penanganan dan pemulihan insiden siber.
b. Memberikan edukasi dan praktik akan kesadaran keamanan siber pada entitas yang terlibat pada kegiatan operasional dengan tujuan meningkatkan ketahanan siber.
c. Membangun koordinasi, kerjasama dan kolaborasi dengan pihak terkait dalam rangka pengamanan siber terhadap layanan Teknologi Informasi.

3.3. Konstituen

Konstituen KIM-CSIRTmeliputi Pegawai PT Kawasan Industri Medan.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan KIM-CSIRT bersumber dari Anggaran Departmen Teknologi Informasi PT Kawasan Industri Medan

3.5. Otoritas

KIM-CSIRTmemilki wewenang untuk melakukan:

1. Melakukan pencegahan insiden, penanganan insiden, mitigasi insiden, investigasi insiden, analisa dampak insiden dan pemulihan pasca insiden keamanan siber.
2. Menentukan asesmen tingkat keamanan informasi pada proses bisnis yang sedang dan/atau yang akan berlangsung baik secara mandiri, atau dilakukan oleh pihak ketiga.
3. Melakukan pengawasan serta respon aktif terhadap operasional sistem informasi dalam rangka pemenuhan ketahanan siber.
4. Merencanakan dan mengimplemnetasikan mekanisme pertahanan berlapis siber (*cyber defense-in-depth*).
5. Memilki kendali penuh atas data dan sistem dalam pengelolaan dan distribusinya dalam hal penanganan insiden siber.

4. Kebijakan – Kebijakan

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

KIM-CSIRTmelayani penanganan insiden siber dengan jenis berikut :

a. *Advanced Persistent Threat* (APT);
b. *Spam*;
c. *Phishing;*
d. *Malware*;
e. *Ransomware*; dan
f. *Web Attacks.*

Dukungan yang diberikan oleh KIM-CSIRTkepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

KIM-CSIRTakan melakukan kerjasama dan berbagi informasi dengan CSIRT lain atau organisasi lain dalam lingkup keamanan siber. Seluruh informasi yang diterima dan didistribusikan akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi bersifat publik/biasa ke KIM-CSIRTdapat menggunakan *e-mail* tanpa enkripsi data khusus dan telepon. Namun, untuk komunikasi bersifat rahasia/terbatas yang memuat informasi sensitif (bukan untuk konsumsi publik) dapat menggunakan enkripsi PGP/RSA pada *e-mail* dan lampiran *e-mail*.

5. Layanan

5.1. Layanan Utama

Layanan utama dari KIM-CSIRTyaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini akan dilaksanakan oleh KIM-CSIRTyang berupa peringatan akan adanya ancaman siber kepada pemilik/penyelenggara sistem elektronik.

5.1.2. Pengelolaan Insiden Siber

Layanan pengelolaan insiden siber mencakup siklus penuh penanganan insiden keamanan siber pada sistem dan infrastruktur TI.

5.2. Layanan Tambahan

Layanan tambahan dari KIM-CSIRTyaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini berupa koordinasi, analisis dan rekomendasi teknis dalam rangka penguatan aspek kendali keamanan (*security control*) baik dalam lingkungan teknis (*Technology Security Control*) ataupun non-teknis (*Policy/Governance/Compliance*).

5.2.2. Penanganan Artefak Digital

Layanan ini berupa penanganan artifak dalam rangka pemulihan sistem elektronik yang terdampak atau dukungan investigasi dalam rangka menjaga *chain-of-custody* dari sistem elektronik terdampak.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini berupa notifikasi dan pemberitahuna kepada entitas lain akan adanya potensi yang serangan dan ancaman dari pihak luar yang berhasil terdeteksi.

5.2.4. Pendeteksian Serangan

Layanan ini berupa pendeteksian serangan siber pada konsitutuen yang akan dikorelasikan untuk memperkuat visibilitas secara keseluruhan.

5.2.5. Analisis Risiko Keamanan Siber

Layanan ini berupa assesmen dan analisa atas kondisi terkini kendali keamanan baik secara teknis dan non-teknis. Termasuk dalam analisa risiko keamanan informasi, audit teknis keamanan informasi, assesmen keamanan informasi.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber (*Security Advisory*)

Layanan ini berupa pendampingan dan pemberian konsultasi terkait proses penanganan insiden siber berdasarkan praktik terbaik industri dan regulasi yang berlaku.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini diberikan kepada konstituen dalam rangka membangun *people-process-technology* untuk menunjang program edukasi kesadaran keamanan informasi yang berkelanjutan

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke corporate.secretary@kim.co.id dengan melampirkan sekurang-kurangnya :

a. Informasi Pelapor: Nama Lengkap, Jabatan, Nomor Telepon dan Konstituen asal
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* atau video *proof of concept* (POC) yang ditemukan
c. Bukti atau informasi lain sesuai dengan kebutuhan penanganan insiden atau ketentuan yang berlaku.

7. *Disclaimer*

a. KIM-CSIRTmelaksanakan kegiatan respon insiden dengan menerapkan prinsip kerahasiaan sebagai prinsip kerja, pembagian informasi ke para pihak akan dilakukan dengan menerapkan prinsip *need-to-know.*
b. KIM-CSIRTmenyediakan layanan konsultasi dengan lingkup terbatas dengan tujuan ketahanan siber bersama dengan usaha semaksimal mungkin, kami tidak dapat menjamin hasil akhir secara pasti dari pekerjaan yang tercantum pada daftar layanan.
c. KIM-CSIRThanya menyediakan sarana komunikasi melalui kanal yang tercantum pada RFC2350, kami tidak bertanggung jawab atas komunikasi yang mengatasnamakan KIM-CSIRTmelalui kanal lain.
d. Bagi konstituen, sampai saat ini KIM-CSIRThanya merepon dan menangani insiden keamanan yang terjadi pada sistem yang terafiliasi dengan KIM.
e. Apabila dibutuhkan, segala konsekuensi hukum yang disebabkan oleh insiden keamanan siber akan diteruskan ke institusi penegak hukum sesuai dengan peraturan perundangan - undangan yang berlaku.