RFC 2350 GMEDIA-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 23 Januari 2025.

1.2. Daftar Distribusi untuk Pemberitahuan

Internal GMEDIA – PT Media Sarana Data dan Website CSIRT GMEDIA – PT Media Sarana Data.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt.gmedia.id/GMEDIA - RFC2350.pdf

1.4. Keaslian Dokumen

Dokumen telah ditanda tangani dengan PGP *Key* milik GMEDIA-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 GMEDIA-CSIRT;
Versi : 1.0
Tanggal Publikasi : 16 Januari 2025;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

GMEDIA - PT Media Sarana Data CSIRT (GMEDIA-CSIRT)

2.2. Alamat

Jl. Siliwangi No. 32G, Nogotirto, Kec. Gamping, Kab. Sleman, DI Yogyakarta 55592

2.3. Zona Waktu

Asia/Jakarta (GMT+7)

2.4. Nomor Telepon

(+62) 274-380-345

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

(+62) 811 274 345 (WhatsApp)

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

csirt[at]gmedia[dot]id

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

Bits : 4096
ID : F0D9A660ED1342DC
Key Fingerprint : E758EA441A381B54BCDF2F19F0D9A660ED1342DC

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

xsFNBGec12cBEAC4bKowIuNl6oGydedlayKspnOnD8aFlPMfLnWfPqafDR
MJk4Po
5OZsi8ifOmbL/H3z9Oksu5twB32rFbaNRiSEPofuEug3gIwNFLxWyfv/UcRAd
Ou5
Fu3W/QXKPonayhoz/fpa3/BUYWu7UpspwmhViTLjG9qMwY4zRHT59DtX7
De3YJZS
ZwLh+fYoKbrksC8Fr/xlLlIB/SCHPZBcA4iU5Dgk2EOwZzpBSzYavZpenAsbF
zax
HhfFo/SZHI2Z1uDcvmmTCxRoOviXlWRII3o2kPi1G5gtv5J6xmng4m+zFLqb
aEU2
G9TrB4GknwGDYQgESEcJnrr6kVD2XTDKFs/r42LxA8TaOPoa/qH4FFClnIz
IZ/V8
t4KN6kU2TbNQJmMojOmHIJ3bSClKa0+eOQHNgBOgkMQ38o6eDYnfvz80
JHi0u0D4
Y4Re1ufkWrPtRjxU9Rrngqh9+70Rjzaq9nNs/TtQ61Fcd3Wl3ZQgOPT0X3Iy8
cEX
ykF6aTE+92iJTYA0HdZNOexbVcfgz3Ro+JzvxHwvPm+gS4jqAiEO41yyauF
S17tv
QOHvBYUdDv8kxk1ZGZp+fEQKxQYmGi1auKBu9TiDK+uYFxs5udx/pyd3Bl
DEPlf3

ENBXodSE8ATZZBke35gMOPYkDBCuA6lg0Dg7XNgDYrwIAwgk0RZRJJ3
PhwARAQAB
zRdDU0lSVCA8Y3NpcnRAZ21lZGlhLmlkPsLBhwQTAQgAMRYhBOdY6kQa
OBtUvN8v
GfDZpmDtE0LcBQJnnNdoAhsDBAsJCAcFFQgJCgsFFgIDAQAACgkQ8Nm
mYO0TQtzk
fhAAqkOHt7uee+TK4LDq9BL6/s/V+so6ElYqVWMX0TMtGLPYPVnVEphT97
Z7lPoW
vY2EUGS4c4s0Fe4LByy8MDukrtRAwO7bSQ7ddiP/CMVuqPiVjW3l00cHKH
/Ad9TM
TjQ/CBTq+Sr3/haP5clvpC1B2Ss22tm14V9ONE3GIErL4M2AE0Q/0/7ksDmz
6ScW
5fR2oetJ9k2QxbJUflFz8t76X2QSvNLHS+0WHQURosIMSwy2UbiBObXl8i8k
X5i5
fltCEVGSq7EaYBZFPdXBNmToOcwmUNRoXvY+Ngt6G8eqq7youBZ5/B8m
0/d67sEU
PyrHidog77FYoZaNs2qXbpI2kQ8yCV18p4OYDRBd7A4EB9dTK9r8PBuEgU
ajPJxX
zAj9++C6cYTYyBupVzzVlVJlHtKrkzt+PhBjUdcJWCc2FF+JCwWgh4QB7R+t
uuX9
dPAOSndd00kau8CAuMb2pKN4AR2AaLjPwhl7anEwmknRWqMW5Rn1uW
qg1Zf6gyVy
Ts2ydUQB9fcZhvQm3U2TzBJSOjc2d+Fv2u5eWSnWAlpNuFZQKKpIGRttD
BfNdcvp
/o1yLodYgDaHUsO9wc2LQz8MEWPaVGl1QXyfbShi1dJXBo/cHUEquBIAvB
iCjbgI
Zxv+OA8hdhVroBvp0+uR7cQanpb7n+cjEwgyJbxxCOQdU0zOwU0EZ5zXa
AEQALmE
g838hzDRci1A32AV6tPqBIrTno3vKfUF6Ulnbu4vpWIO8I0DFHLkfGcE9J2rp
Hgh
bnZl6Ldtmg3D3x0b5GK4zTMpFjt7GtuF75guwC9eMDpb1b0FAQV0NKyguP
2OMBlH
l08hJMyfDHMFMAQ+ieFsaPDGyHNVta7JydH4VsybSRg1XFCF5qaHm1akf
QiTqm8O
JrFsSjbbYPFAr53pos+jgNENYVVeEjBGdwYS3pjX0MWqEsxCdHIj0zOOA4I
9Q4Qt
7HFHpL/k1DzDoVxY1s0eZx8Uqwa79enpLS7uzUp0GaMWa1TUNAEEgSoR
MEWF8mgb
1uEWX8Hxp7G6NaAw30KlMuStyp11wHZqi/WaGGMJ9VyGoQnZWO02/7Lt
pG0sLajs
Bc56htOUu1kkFalVl0YK282FgUIIfiGvy4CSjZPZ9lM6MIyZxjin9AGo8UnvHL
VI
iBPL9Q4LoizD1mr62TD7d3ZqaELTey489lIOHAxUSBJtmbRWqZj8qXT17Zff
ILqZ

IuYpOZz7+ZDzNQoxpUsYFfga6/fg5XdU0Go2a9t8PgFO72sZjeIxHb5aBTTq
Hv7/
I05XeC2fehz4DeXGgB2EDeOk2gu3m/fsYctC0RZq3lLs2UTyIOv8BFkt7OKy
8IxU
nw8/FbsYc2bGRe4QxY2gfmFOe6LGyfCqGTBGKztrABEBAAHCwXYEGAEI
ACAWIQTn
WOpEGjgbVLzfLxnw2aZg7RNC3AUCZ5zXaQIbDAAKCRDw2aZg7RNC3M
dAD/9+p2bc
EzpS36jpPwhPtODX17tJpEn9a3rpfd4GwIJgF7HVyVDFSCir3T0t1d/NaNz9X
h9f
jUuK3sn6VtXpL6h9BHK0lEDEkc4XWn6sPHxRWmwf00IYAJnoNCRzAOjtKI
QZe2Vr
qeH9kNRu2mzxeKLSB+GKw9a4/lkcWzIHi0M5UvumagGVQk8bIFAFGDYo0
i7fe+df
h5f2UsJS30tx+n4apyfQEGhA0yhshhmy5sWV2B3wvMfL72rSkQVlz3ZK60Dj
PSrH
vkH8iZ1noQzC6j+tcYd6xnyZwZh/TxEpTORRuTPx4mS3n7osvAkHCOxMjNJ
rExR9
2mEY+nwegFiZ0eESj8qL3//3UwZeyZY1Np5tE2Kx/k4Nkb/69PXN5jrp85dxD
sxA
WfDYoHbkFpJkP33kMBcjR0mT0U+BfaQKxfno3EdojR3EufgxdY0a4HWERE
vNqzFS
gggD/CmBd8K5y5S8mM8GweWYh79Tet7SbJDFIZ9qdF9a1HomE33tckyE/
qT2TVLG
XSg/GolYBBP7WhppJXKCBtZWsyy53sHzjVeHXeHYXr3zQC5OChwQ63xA
0p0AOIU0
xyxeOIQi3EJ+q5AX973cI7edo47urg0aAYQiDkOV246OW+rkwlmolilVFX6XM
Hmc y4DWXXSGVZ1LOEf0nY8U8u012LYE25DnYjhW5Q==
=pEpJ

-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirt.gmedia.id/public_key.asc

2.9. Anggota Tim

Ketua GMEDIA-CSIRT adalah Wahyu Arif Purnomo. Untuk anggota tim merujuk kepada Surat Keputusan Direktur nomor SKD I/SKD/MR/01/0624/0004, tentang Penetapan Tim Tanggap Darurat Keamanan Informasi (Tim TDKI) 2024

2.10. Informasi/Data lain

-

2.11. Catatan-catatan pada Kontak GMEDIA-CSIRT

Metode yang disarankan untuk menghubungi GMEDIA-CSIRT adalah melalui email di csirt[at]gmedia[dot]id, telepon di (+62) 274-380-345, atau WhatsApp di (+62) 811-274-345. Layanan ini tersedia 24/7 melalui Bagian Keamanan Siber.

3. Mengenai GMEDIA-CSIRT

3.1. Visi

Visi GMEDIA-CSIRT :

1. Menjadi garda terdepan dalam melindungi layanan digital GMEDIA – PT Media Sarana Data dari ancaman siber, dengan respons yang cepat dan efektif.
2. Mewujudkan keamanan siber yang proaktif dengan memastikan seluruh infrastruktur dan data pelanggan terlindungi secara maksimal.
3. Menciptakan ekosistem digital yang aman dan terpercaya, memberikan rasa aman kepada pengguna dan mitra bisnis GMEDIA – PT Media Sarana Data.

3.1. Misi

Misi dari GMEDIA-CSIRT :

1. Menanggulangi dan merespons insiden siber secara cepat dan efisien untuk meminimalkan dampak terhadap operasional dan data pelanggan.
2. Meningkatkan kesadaran dan pengetahuan keamanan siber di seluruh jajaran GMEDIA – PT Media Sarana Data melalui pelatihan dan edukasi rutin.
3. Mengembangkan dan memelihara kebijakan serta prosedur keamanan siber yang sesuai dengan standar industri dan regulasi untuk menjaga keberlanjutan layanan digital.

3.1. Konstituen

Pihak Internal dan Pelanggan / Instansi / Organisasi lain yang bekerja sama dengan GMEDIA - PT Media Sarana Data.

3.2. Sponsorship dan/atau Afiliasi

Pendanaan GMEDIA-CSIRT bersumber dari alokasi *budgeting Cyber Security* Internal GMEDIA – PT Media Sarana Data.

3.3. Otoritas

Otoritas diberikan oleh Direktur Utama melalui Surat Keputusan Direktur (SKD) nomor I/SKD/MR/01/0624/0004. GMEDIA-CSIRT memiliki kewenangan atas konstituennya dalam penanganan, mitigasi, investigasi dan analisis dampak insiden siber di lingkungan GMEDIA – PT Media Sarana Data.

4. Kebijakan – Kebijakan

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

GMEDIA-CSIRT melayani penanganan insiden siber dengan jenis berikut:

a. Web Defacement
b. DDoS / Brute Force Attack
c. Malware
d. Phishing
e. Ransomware
f. Data Breach
g. Social Engineering
h. Man in the Middle Attack (MitM) Attack
i. Cross-Site Scripting (XSS)
j. Cross-Site Request Forgery (CSRF)
k. Adware & Spyware

Dukungan yang diberikan oleh GMEDIA-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

Untuk komunikasi yang bersifat biasa, dapat menggunakan email csirt[at]gmedia[dot]id dan telepon (+62) 274-380-345. Namun, untuk komunikasi yang memuat informasi sensitif, terbatas, atau rahasia, disarankan menggunakan enkripsi PGP pada email.

5. Layanan

5.1. Layanan Utama

Layanan utama dari GMEDIA-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Peringatan diberikan kepada seluruh stakeholder di lingkungan GMEDIA – PT Media Sarana Data dengan memperhatikan tanggung jawab masing masing stakeholder yang ada di lingkungan GMEDIA – PT Media Sarana Data.

5.1.2. Penanganan Insiden Siber

Layanan penanganan insiden siber yang dilakukan oleh GMEDIA-CSIRT berupa monitoring, analisis, rekomendasi teknis dan koordinasi serta pendampingan dalam rangka penguatan keamanan siber.

5.1.3. Penerimaan Aduan Insiden Siber

Layanan yang diberikan oleh tim GMEDIA-CSIRT untuk menerima, mencatat, dan menanggapi laporan atau aduan terkait insiden keamanan siber yang dialami oleh Konstituen GMEDIA – PT Media Sarana Data. Layanan ini bertujuan untuk memastikan bahwa setiap insiden siber yang terjadi dapat ditangani secara cepat, tepat, dan sesuai dengan prosedur yang berlaku.

5.2. Layanan Tambahan

Layanan tambahan dari GMEDIA-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Penanganan kerawanan sistem elektronik merujuk pada langkah-langkah yang diambil untuk mengidentifikasi, menganalisis, dan mengatasi kerentanannya yang dapat dimanfaatkan oleh pihak yang tidak berwenang. Kerawanan ini bisa mencakup celah keamanan pada perangkat keras, perangkat lunak, jaringan, atau aplikasi yang digunakan dalam sistem elektronik.

5.2.2. Penanganan Artefak Digital

Penanganan artefak digital, berupa data atau informasi yang ditemukan selama penyelidikan terhadap insiden siber, yang dapat digunakan untuk mengidentifikasi, menganalisis, dan memahami serangan. Penanganan artefak digital melibatkan pengumpulan, pengawetan, dan analisis data tersebut untuk mendukung penyelidikan lebih lanjut.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Pemberitahuan hasil pengamatan potensi ancaman berupa proses penyampaian informasi terkait potensi ancaman keamanan siber yang terdeteksi dalam sistem atau jaringan kepada pihak terkait. Ini termasuk memberikan informasi yang relevan tentang potensi serangan atau kerawanan yang dapat membahayakan sistem atau data.

5.2.4. Pendeteksian Serangan

Pendeteksian serangan melalui proses untuk mengidentifikasi serangan siber yang sedang berlangsung atau yang telah terjadi pada sistem atau jaringan. Tujuan utama dari pendeteksian serangan adalah untuk mengetahui adanya ancaman sebelum menyebabkan kerusakan lebih lanjut.

5.2.5. Analisis Risiko Keamanan Siber

Analisis risiko keamanan siber dengan proses mengidentifikasi, mengevaluasi, dan mengelola risiko yang terkait dengan potensi ancaman terhadap sistem atau data. Analisis ini membantu organisasi memahami sejauh mana ancaman dapat memengaruhi operasional dan keamanan informasi mereka.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Konsultasi terkait kesiapan penanganan insiden siber melibatkan komunikasi dengan ahli keamanan atau tim eksternal untuk memastikan bahwa organisasi siap menangani insiden siber dengan efektif. Hal ini mencakup evaluasi kesiapan teknis dan prosedural dalam menghadapi insiden yang mungkin terjadi.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Pembangunan kesadaran dan kepedulian terhadap keamanan siber adalah upaya untuk meningkatkan pemahaman dan tanggung jawab seluruh anggota organisasi mengenai pentingnya menjaga keamanan informasi dan sistem. Ini mencakup pelatihan, sosialisasi, dan kampanye untuk mencegah pelanggaran keamanan.

6. Pelaporan Insiden

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

a. Foto/*scan* kartu identitas
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
c. Atau data pendukung lainnya yang sesuai dengan ketentuan lain yang berlaku

7. ***Disclaimer***

Penanganan insiden tergantung dari ketersediaan tools yang dimiliki oleh GMEDIA – PT Media Sarana Data.