RFC 2350 KOMDIGI-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 8 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.komdigi.go.id/dokumen/rfc-2350-komdigi-csirt/detail (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 KOMDIGI-CSIRT;
Versi	: 1.1;
Tanggal Publikasi	: 9 April 2025;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Kementerian Komunikasi dan Digital CSIRT
Disingkat : KOMDIGI-CSIRT.

2.2. Alamat

Pusat Data dan Sarana Informatika
Kementerian Komunikasi dan Informatika
Jalan Medan Merdeka Barat No. 9
Jakarta Pusat 10110

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 3848882

2.5. Nomor Fax

(021) 3848882

2.6. Telekomunikasi Lain

Whatsapp +62 8151 5000 2021

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

csirt[at]komdigi[dot]go[dot]id

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

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

xsFNBGeppK0BEADtxd2csFkLTNmStgUYmf0QyNGpOdL79nuxCs21jQcVgkZ67hn
m
MmAUFw0LtYM+pe6nKJOtv8BqzGxXo22FITgm0q3RGHHEJ6U4V4CLgmabHSWe
FiIz
SnakM0rZvfB6u4T0RfrUBby1omiypbkFlpee6C4Q4HaVmoCdDCfQzP70TS58CyNT
e1YivN5MdYAiMXd0uwRRmU23hX4MbhifqMEhwXTQ4MtQim482PsiXd30xQrLnu+
U
tf7m8v2dL6+dZN6OqLE4C0sl78LUMpw97NmPa6WGPHH2/h7ye9nSjFLnS02ks7d
D
xiSdwlY9aJhwRa+bAsz/o9DvN6jKzi9wwWAyKO2W6XIym5RjdFw5XDhTA03dtFQs
Q173uUP44x/Fom1gFLzEf1w2UTbnxf1fwWG5Cz+d/D2ssnwCneTbQO5LoyMNZg
wx
mAomLySw+MQo0f5lwFUWlRLW5qFHWprvZcuNfJtVYQrtux7oCXdq+/i0tCqanSsT
ujcolNPR6PM6y4HXsSrfaneUJ5BvJUwPmEDhI+XezlE2jI/JtPpdX5s+Ns7o9qWW
8l8t9nVqI7qWU+hf0yfWOrbSvvod8BdgFSBtmmPr5lGIPTiXKvkLfLV81xASWCOY
7OouQqnEB3An9y5kYRNFge+hhmMlPcT00wxoE4QD0LKUYC7Q2U1mfpc1VwAR
AQAB
zSNLT01ESUdJLUNTSVJUIDxjc2lydEBrb21kaWdpLmdvLmlkPsLBjQQTAQgANxY
h
BABkarpMDWvKBsfrL0qE/Cw9JDSbBQJnqaSvBQkHhM4AAhsDBAsJCAcFFQgJC
gsF
FgIDAQAACgkQSoT8LD0kNJvUqA/9E3x7a+qDuhYif4fNnZ8VqIykZ4OnSs5qCdFg
i7NKtuH5fBBR08N4o83rgxEJHjPq0+Iz/R+TRpWBh1HIm9/VVKFA0EvJhSCKQzIQ
2oa/Yi4C78D1J7lcQf2hT/6MowwFoKjCYfNd/E0smv5jJQM0lhantMmDF94qclvk
G5rxOiLuJEMCpuxAseOFnZ4pk+OF5xdegjODvpthpceq/IDQml73OFSUJKB5vRsy
WzNxXb9scT+s4ihKzgiEGJ9+fBWfd/sDyhYfaqLgVMUPvEKhj6K91MgJQRqadwQe
bKdLveHnVLLk82WEtcHTnNpE6AxybUQBLc9b73pLhxFWSjaAXmEJoY/FBa8wUY
xU
ezWTiio3Appns5FC8o3kMrscOQbNjTBNjR1tCRW12jI4MmQUdRlLGiuBxP5WGeu
a
qRS6O2r/RTBBS9VWSrxdRFWJcB7OK+sg8PBzSjMe1GpOQub5uIYSBRe/uSZbZ
X9l
dVkxibQS+3pvR725mebtRj15MGvy3yO8jOTAQE7qdGiR7JrllDe4zYU1AaB//JpR

NGCiwbqQsfJRS8jxCAR0A0QDSqKs12rCepp1+zs9yHbqqhs5dvuthhbVh7tYbyd0
1PfjRONljOlvRfEAwL6L/+2UfjUJvgWJbWfraxa3KllDnPSN5zo6lh0utlwykzEz
Xf7J4WLOwU0EZ6mkrwEQALqRBZ8feUAQjT+DcETCBSMYIjLFxUmmlwvnZcpZO
pUU
7r2uCsdTMpeJ2x7/pmMJ2a3GoFW22+ArTbN4qL8yaWrl2AIzujzhenoLK3uyf5Fs
kKYsDglOdZR7HXOqw7NqC9g9KpmOfTdMtgZzUL7Ad9O8aJORLGLWLdIoJGnm
qG15
OLFX4x5g4bXh9qBwkXz9Ex6MqJckzNVpWh5NKDwu7Ys6rzVqO6hh9iV7dO7hHA
Yd
sJbV3lpT1xBW9zTDMr9hgdRABdnysL0PCq0nJA0wk/QAs1B9bKW66LUZSEcaiJh
u
kA1J0gwKhevocEKD6Cd3Rp1VRbb9WtXND65R9+ptAVpWzzM8IYg15p7NUpofW
BSL
3UDSe4T5OboxkM4d7RC8DVH2goZ/er082VEpSP4xItitu4iEGOOh7XMKhRelJT3w
fZd/FBc1m6IBO2KkAk8yiKt7GqvKZ9X4xxtcfoUeMmJ1lnhiu8MxyxkFWJ1E9gJz
UOkVEWnXxpb35aegsXJYPZV5oiChKIXB0V9EKn/4Kw3T4YtSYKTy2amW3zH/y2
+A
a4BGzCUK4dkIOzkofFNSmjOdq8R8CyRxh5ChOKNSqN9wmVfddfI70nG/XPpGN+
mc
LzSRcuOcBC3a+izeIaxG1TfW1sYEur03CvJeWhSF7oRF2itn+ttJ0lrbSjFbgv/v
ABEBAAHCwXwEGAEIACYWIQQAZGq6TA1rygbH6y9KhPwsPSQ0mwUCZ6mks
AUJB4TO
AAIbDAAKCRBKhPwsPSQ0m21uEACvsQzRNm+t7V4LmYFbZefRz1abToSY9SPf
YTGe
cZLw8nU2xiY4O8lnOsK1aZ4zcVEzBtO22Zf7QRvbZO4ETkoKKpAT/itZxhOidCz3
wwuJ81QwIAkdORz/Q5nlXLDvb57KHzzUeIKxg+9J91zO8QlaQqSw7dv/wKtWU+ee
BE+DF7XS8vWdaU0psfNBEoSt7TIOr8t+IPe0kGIC6z6obexnMDCj9du7n0exhcR1
vTJ7xAUu8poYn19+oREuY+jZ94nn+ygZDGsPV9aHfunRoseXtXDc6xiB8mhj6UsG
ONK2RvuxaKr9dktGQ00zpv3+d0Jgmeuc5MMoyJJO7ayOehsS1z5/OacYiQR4Fhi4
po0f4rl+I2Lx4ER0GVCGCByNJtqEfI9m/aXLZloyIgModhE2kUcSRjwDhJ0rwhAC
z9VRkBx8JzpO/2XX4QnTpL3wYpTdiZhebNE/n0fNcjKhHLp1N2ZVyVbPzLHxu2Yp
mOx9pSWYOkzxszUpOfuegVAmqgmK5yP7NX8yzItl2WoH0KonyMOAuIzeKs6fML
od
ueCQDMUD3GVjiU8FVE6eIhBbrUPg0ThuX36LNn8CjoJ2PVb3O16sGWf19m8RuI
dC
KDWJcvHd27ermChon/kpd5u61Ndfdn4IwxFHHH/C1F2zNUxU+SF1MMssnJIrgae3
SjX0yQ==
=5WiU
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada:
https://s.komdigi.go.id/publickey-csirt

2.9. Anggota Tim

Ketua KOMDIGI-CSIRT adalah Kepala Pusat Data dan Sarana Informatika Kementerian Komunikasi dan Digital. Yang termasuk anggota tim adalah perwakilan staf Pusat Data dan Sarana Informatika dan Satuan Kerja sebagai Agen Siber di

Kementerian Komunikasi dan Digital sesuai dengan SK KOMDIGI-CSIRT yang diperbaharui setiap tahun.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak KOMDIGI-CSIRT

Metode yang disarankan untuk menghubungi KOMDIGI-CSIRT adalah melalui *e-mail* pada alamat csirt[at]komdigi[dot]go[dot]id atau melalui nomor telepon (021) 3848882 dan WhatsApp ke 0851 5000 2021 pada hari dan jam kerja (siaga selama 24/7).

3. Mengenai KOMDIGI-CSIRT

3.1. Visi

Visi KOMDIGI-CSIRT adalah terwujudnya ketahanan siber pada Kementerian Komunikasi dan Digital yang Handal dan Profesional.

3.2. Misi

Misi dari KOMDIGI-CSIRT, yaitu :

a. Membangun pusat pencatatan, pelaporan, dan penanggulangan insiden keamanan informasi di lingkungan Kementerian Komunikasi dan Digital;
b. Membangun kapasitas Sumber Daya Keamanan Siber pada Kementerian Komunikasi dan Digital

3.3. Konstituen

Konstituen KOMDIGI-CSIRT meliputi :

a. Unit Kerja dan Satuan Kerja di lingkungan Kementerian Komunikasi dan Digital
b. Unit Pelayanan Teknis di lingkungan Kementerian Komunikasi dan Digital.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan KOMDIGI-CSIRT bersumber dari APBN

3.5. Otoritas

a. KOMDIGI-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada Kementerian Komunikasi dan Digital.
b. KOMDIGI-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya.

4. Kebijakan – Kebijakan

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

KOMDIGI-CSIRT melayani penanganan insiden siber dengan jenis berikut :
a. *Web Defacement*;

b. *Distributed Denial of Service* (DDoS);
c. *Malware*;
d. *Ransomware*.
Dukungan yang diberikan oleh KOMDIGI-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa KOMDIGI-CSIRT dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada e-mail.

5. Layanan

5.1. Layanan Utama

Layanan utama dari KOMDIGI-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini diberikan oleh KOMDIGI-CSIRT berupa pemberian peringatan adanya terkait adanya insiden siber atau potensi ancaman kepada pemilik sistem elektronik terkait.

5.1.2. Penanganan Insiden Siber

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

5.2. Layanan Tambahan

Layanan tambahan dari KOMDIGI-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini diberikan oleh KOMDIGI-CSIRT berupa hasil *vulnerability assessment* (VA) / *penetration testing* (PT) terhadap suatu web aplikasi baik yang belum launching public maupun pemantauan secara rutin setiap bulan. Tindak lanjut dari layanan VA/PT ini berupa pembimbingan teknis untuk menutup celah kerentanan yang kami sebut sebagai kegiatan Klinik Siber.

5.2.2. Penanganan Artefak Digital

Layanan ini diberikan oleh KOMDIGI-CSIRT berupa penelusuran artefak digital di dalam sistem / server untuk keperluan investigasi terhadap suatu insiden yang terjadi. Penelusuran artefak dilakukan demi mencegah terjadinya pemanfaatan residu – residu sisa insiden yang terjadi sebelumnya oleh threat actor.

5.2.3. Pendeteksian Serangan

Layanan ini diberikan oleh KOMDIGI-CSIRT berupa pemantauan traffic anomaly menuju data center PDSI Kementerian Komdigi sebagai Upaya deteksi dini terhadap serangan agar dapat segera diambil langkah mitigasi yang cepat dan tepat.

5.2.4. Analisis Risiko Keamanan Siber

Analisis Risiko Keamanan Siber dilaksanakan oleh KOMDIGI-CSIRT setiap 3 bulan dalam bentuk laporan Manajemen Risiko Keamanan Siber yang diserahkan kepada Inspektorat Jenderal.

5.2.5. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

KOMDIGI-CSIRT siap siaga memberikan layanan konsultasi terkait Kesiapsiagaan Penanganan Insiden Siber melalui e-mail atau WhatsApp.

5.2.6. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

KOMDIGI-CSIRT melakukan kegiatan Pembangunan kesadaran dan kepedulian terhadap keamanan siber (*Security Awareness*) yang dilaksanakan setidaknya 2 kali dalam setahun dan sosialisasi melalui email, portal berita intranet dan poster – poster.

6. Pelaporan Insiden

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

a. Foto/*scan* kartu identitas
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan

7. *Disclaimer*

Terkait penanganan jenis malware tergantung dari ketersediaan tools yang dimiliki.