

RFC 2350 CSIRT PANDI

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 20 September 2024.

1.2. Daftar Distribusi untuk Pemberitahuan

Dokumen ini didistribusikan hanya untuk kebutuhan internal PANDI.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada:
<https://pandi.id/regulasi>

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani oleh Ketua Tim CSIRT PANDI.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu:

Judul : RFC 2350 CSIRT PANDI

Versi : 1.0

Tanggal Publikasi : 20 September 2024;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

CSIRT Pengeola Nama Domain Internet Indonesia
Disingkat : CSIRT PANDI.

2.2. Alamat

Icon Business Park Unit L1-L2 BSD City, Sempora, Kec. Cisauk, Kabupaten
Tangerang, Banten 15345

2.3. Zona Waktu

Kabupaten Tangerang (GMT+07:00)

2.4. Nomor Telepon

+622130055777 (7 Hari Jam 09.00 – 17.00)

WA: +628118805530 (7 Hari Jam 09.00 – 17.00)

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

Melalui website <https://pandi.id/kontak>

2.7. Alamat Surat Elektronik (E-mail)

soc@pandi.id

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

Bits : 4096

ID : 0x975A98E25876648F

Key Fingerprint : 97F0 1AC5 C3DF 3DF2 E85D D51B 975A 98E2 5876 648F

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

Version: OpenPGP.js v4.5.5

Comment: <https://openpgpjs.org>

```
xsFNBGbs46MBEADRIWMMx/M0A9/PuePJbD4/AIKQm6COMDmskfKxCL4xcoKk
voZRuL3eJdla6Vn3OIn7ckpifHAz0tMqt4x5INRlc82UqHiTny3g0qsmYKjH
EMT2s85Qzv7WLXYH11JEuNoGYnloXyK+Pplzfdxo1rrtoJarBvFSkfz5Nal
sih5+m3mfkooRXJJqZN5UWOR58IRA7jB1EffqJte0eZIZoK5+yPk0WRIMuor
zPPYyV7fUSs/cZfvAZ+JUvcsLa2Ge90HAq9MdvNIVPwR9AVQydMsT9nQ/6G
wFGQuahI6EICfJCucAC2ImqUCgrloL1RceLFCIQ1rrWLUkO2G/d3nYt3ru/Sv
gEPktS5w3lpPdglGEinW7DNU/cNod3oLkS5zJ76Gf8QZ/6G7wuuWPvRpnPa3
Jv3eoZChfxJw2SUw2Ry7+Ed4K9DH9B9PDDd5p4eg18ZWzGJCfxmeBv6jifQ8
M1XCa9TwLzlvivVAEP0q8bLS14GtgbQTO1c1+y23KVElnAv9MyX9pip+TIER
2jDbMgjv7+gAp1CoAFsD7cM/fAkjbkn4pcjcqhI36ir2Kcbb/JNmllbK6PS
UE5+Yvsx1M5dYmP0aTnfDpLDckhlhoh/jZ66RxjabQkkDyAFEzjTphcQuxva
ITRu6ANei+dZvS2k/S0A6DEALYtw11tg95a+jQARAQABzQ48c29jQHBhbmRp
LmlkPsLBdQQQAQgAHwUCZuzjowYLCQclAwIEFQgKAgMWAqECGQCEGwMCHgEA
CgkQ1qY4lh2Zl86GA/9FfUus0Imrcz9GrBs8kh5wHFUyLQI98YN3UzCX+A8
u9eT1sK+fbUru1gACOEyVVEpsDzv2lArRucT3O0rP9T2gKc1CNo0twnf+sri
rmPfVAFQOhArdmUGUx/1JMwiYqzO/qgPW2CPlpHUyB09ypkyF2q0tWuO1Jn5
NWjVpb3bEXgipUzk7wxqQD1HfzIMv6ATmcmIU2IWNi4TQknE8mnH3y2+u6Fz
37zrW5Qo+qQGE9/t7usDctvldKtf8rK0Lula0PGBWz9uRQxQ8wyk5Z4d5MI
xjg+dWMw34Tmrz5hU0pJqldaOTLBPgub9L14e1HtXtox04bMnMpOAWgtgXsh
EdQLOtxc5g/xAUrypu6vbMMvtZZhIEEqQVEkDd1/QKUT5mXyA0xXAR6G4Bke
dWU+H8vnLXou7dxkitd6HShAzm0rmlkOtiOVP1O5ccL+XQzdZ96EvgbPJCOe
eV900EgjSUIzlonN6rKEV0L80fr9F3pNGiidURbgoOimYhb/CP2ZD3Lw/XeQ
wcyCTYjFznppD85oAsDIIes8ONqqMgiEArp jutmNg95uho6iXggIKP5g5P6c
JTUZDQV7ieOKnPJ5T/Jt6P8QvDNFO8k8B9jp0nZJOBwjcsrVSP9dwUTWa/Jac
xYRgGq7siUW2JBA/AyKhPOwpc4MIJVxPeqh04JkwFubOwU0EZuzjowEQALdr
M2KPiZnV0wsP8EkUczKz07NquwrGlfu+ysdBboANg1qgJ5qhLpFO3PzAgcZr
U2imVHskfmwkHBfrPuG0x7zmLCCGJ+duHvJWgE9SuCac9/CGbsXKk/3DsZl9
0OmIG1qS4TABljiAiFC5ALY6J5gsP7u+0W40yTCEYv+16IV5Pp/plJO6Atg2
RyPuxSn7D6KNuCo2vYwfkfRmCDCilxW46O9KtvwTPRy/axRu3OEDI3y62uyP
```

YrxPTOjXUglv3pktnc9SKNcQIDiVr5ysGEHWEIwbFOI/AhAHlaX6S4pQ43WM
r5MWwcyjq0yhDe/dvly6e6j8LssYotTTB9uh+2+nt1dce5ZBjOIGhq53qhS
S3zqsFKFKECqtoo3IU7+OenuHbrWHmb5NJVmHprCGyNVpp9ap83Zwk+r1m/r
GC7kJJ57U+6s7CATUbif7bG9LTP5irUYvRLQCTVPmSaP7HBQdOt53hbQsoqN
Q6OmMoX4WkNT44JmydmNK2NlnEWKSfzkwgnell/NLzzCGadB1MWbGB725QQM
LyBNSfrzieUKv6gMrYZc4WxuJgxYV+U+Z2ZEAhMphPWH57Qn1ukMBEp12yGM
WBx9ARrq03fmZWWzeOoN9R1e7kDMKOQUxuO9i+VLrgDdvXr2xA4gn09sEoqi
frRvADiu1X/LJ8LbJO3ABEBAAHCwV8EGAEIAAKFAmbs46MCGwwACgkQl1qY
4lh2ZI+QpxAAtolJ07Lt2iFisfZtlXowpNllwWloMaM9XglRWf9baRMAbZN
NXhArWFAudnKolKLNtwzD6psZIXhEKX1hcgqjk/AlYJNEhK+HcyCCWny5B2p
N1mLK/n4CWaIXGI1PBhtO/a3v6fVm8wai0X9LPvOHbjRARyYtPsFhEVMlc
CXC3+71vV+SwoR56BIXk3VSsKMxSLmOCGaE5sHFSPKTNp8k4bQaO9/ebQ7jS
EvGI3TfdDvjCKeEhUiUTS2V7YiYlWUUb5JYCLi8mFpwXFUb2HF94p7OIjM79
KYwiFs/GofmgPxQT4bdlkWHTdYZ00ncs4Qgo2drcODjZmVbFiz2hncslmPS
MthU7YnyFQuaNNQDA03qh4DDAIak4LOR1Bi6eBWYRrT1fO+hgQcAMER+ZoFg
IGNGBL9CxiGPEEYJ/0DD7eid3Z9+zoKzftMQj5Ju14fsnNz3MTM8NQ95MkOk
AkCY9I9Mv4CPsbqZ77HOogr8w5VuWFOntdI/G/WzDpVCqjAOPver6WSKQb
Rcdj9lo0EvFhjzFmpSp4OPDslYXjJ5MMUDTCFW0jWktBTTrNGJGfJ4ybmo+n
mppMEq3OKE126FtUeVMCBEWkoZq3YeiT9YhVJc4j/wVBgrmapZgPjksHuZcn
SFRSABodBsvvu+VXELhRKN/8M4F9o32dBYg=
=zipb
-----END PGP PUBLIC KEY BLOCK-----

File PGP key ini tersedia pada:

<https://pandi.id/regulasi>

2.9. Anggota Tim

Anggota CSIRT PANDI adalah Anggota sesuai dengan Surat Keputusan Dewan Pengurus Tentang Pembentukan Computer Security Incident Response Team (CSIRT) PANDI Doc. No: 4006.042/1100/3420/I.I/VI/2024 tanggal 25 Juni 2024.

2.10. Informasi/Data lain

-

2.11. Catatan-catatan pada Kontak CSIRT PANDI

Metode yang disarankan untuk menghubungi CSIRT PANDI adalah melalui *e-mail* pada alamat soc@pandi.id atau melalui nomor telepon +622130055777 ke helpdesk PANDI pada hari senin - minggu jam 09.00 – 17.00 WIB.

3. Mengenai PANDI-CSIRT

3.1. Visi

Visi CSIRT PANDI adalah menjadi tim respons insiden keamanan siber yang mampu melindungi dan mempertahankan integritas, kerahasiaan, dan ketersediaan informasi serta aset teknologi informasi PANDI secara proaktif dan responsif.

3.2. Misi

Misi dari CSIRT PANDI, yaitu :

- a. Deteksi dan Respons Insiden

- Mengembangkan dan menerapkan mekanisme deteksi dini untuk ancaman keamanan siber
- Menyediakan respons cepat dan efektif terhadap insiden keamanan untuk meminimalkan dampak terhadap organisasi
- b. Pemulihan dan Pencegahan
 - Mengimplementasikan langkah-langkah pemulihan yang efisien untuk mengembalikan operasi normal setelah insiden keamanan
 - Mengidentifikasi penyebab utama insiden dan menerapkan langkah-langkah pencegahan untuk mengurangi risiko insiden serupa dimasa depan
- c. Kesadaran dan Pelatihan Keamanan
 - Meningkatkan kesadaran keamanan siber di seluruh organisasi melalui program edukasi dan pelatihan berkelanjutan
 - Mengembangkan budaya keamanan siber yang kuat di antara karyawan dan pemangku kepentingan
- d. Kolaborasi dan Kemitraan
 - Bekerjasama dengan tim keamanan internal lainnya, pemangku kepentingan eksternal dan komunitas keamanan siber untuk berbagi informasi dan praktik terbaik
- e. Kepatuhan dan Manajemen Risiko
 - Memastikan kepatuhan terhadap semua peraturan, kebijakan, dan standar keamanan siber yang berlaku
 - Mengidentifikasi, menilai dan mengelola risiko keamanan siber secara proaktif untuk melindungi aset informasi organisasi
- f. Pengembangan dan Inovasi
 - Mengadopsi teknologi terbaru dan inovasi dalam strategi keamanan siber untuk meningkatkan kemampuan deteksi dan respons
 - Mendorong penelitian dan pengembangan dalam bidang keamanan siber untuk tetap berada di garis depan dalam menghadapi ancaman yang terus berkembang

3.3. Konstituen

Konstituen CSIRT PANDI yaitu unit kerja Internal PANDI.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan CSIRT PANDI bersumber dari internal organisasi PANDI.

3.5. Otoritas

CSIRT PANDI memiliki kewenangan mengenai penanganan insiden siber di lingkungan internal PANDI. CSIRT PANDI dapat berkoordinasi dan bekerja sama dengan pihak lain dalam rangka penanganan insiden siber Ketika eskalasi penanganan insiden diperlukan.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

CSIRT PANDI melayani penanganan insiden siber dengan jenis berikut:

- a. DDoS
- b. Phising
- c. Malware/Virus
- d. SQL Injection

Dukungan yang diberikan oleh CSIRT PANDI dapat bervariasi bergantung pada jenis dan dampak insiden bagi perusahaan. Layanan penanganan insiden berdasarkan laporan dari konstituen.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

CSIRT PANDI akan melakukan kerjasama dan berbagi informasi dengan Nat-CSIRT atau CSIRT organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh CSIRT PANDI akan dirahasiakan sesuai dengan kebijakan klasifikasi informasi PANDI.

4.3. Komunikasi dan Autentikasi

Komunikasi dapat dilakukan dengan no telp dan email untuk komunikasi dengan urgensi biasa. Kemudian untuk sidatnya terbatas/rahasia, dapat dilakukan dengan enkripsi PGP pada email.

5. Layanan

5.1. Layanan Utama

Layanan utama dari CSIRT PANDI yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dapat berupa pemberian peringatan adanya insiden siber kepada internal PANDI.

5.1.2. Penanganan Insiden Siber

Layanan ini dapat berupa penanganan insiden yang terjadi di Internal PANDI

5.1.3. Penerimaan Aduan Insiden Siber

Layanan ini dapat berupa penerimaan laporan hingga koordinasi penanganan insiden di PANDI.

5.2. Layanan Tambahan

Layanan tambahan dari CSIRT PANDI yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini berupa melakukan analisis kerawanan pada system elektronik yang dikelola oleh PANDI.

5.2.2. Penanganan Artefak Digital

Layanan ini berupa pencarian jejak digital dari suatu insiden yang terjadi.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini menginformasikan terkait hasil deteksi anomaly dari SOC.

5.2.4. Pendeteksian Serangan

Layanan ini menilai risiko yang terdapat di PANDI sesuai standar ISO27001.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan ini berupa edukasi dan penyiapan/penyusunan dokumen mengenai penanganan insiden siber di PANDI.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini memberikan pemahaman terkait ancaman siber di lingkungan internal PANDI.

6. Pelaporan Insiden

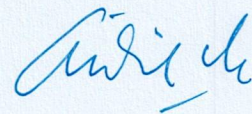
Laporan insiden keamanan siber dapat dikirimkan ke soc@pandi.id dengan melampirkan sekurang-kurangnya :

- a. Deskripsi Insiden
- b. Aset terkait insiden
- c. Bukti insiden berupa foto atau *screenshot* atau *log file* yang ditemukan

7. Disclaimer

Pengelolaan insiden siber bergantung dengan ketersediaan sumber daya yang dimiliki organisasi.

Tangerang, 20 September 2024



(Aidil Chendramata)