RFC 2350 PDN-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 23 Desember 2024.

1.2. Daftar Distribusi untuk Pemberitahuan

- Instansi Pusat dan Pemerintah Daerah (IPPD) sebagai tenant PDN
- SOC *Managed Service* dan/atau KSO PDNS
- Dirjen dan Ses. ditjen APTIKA KOMINFO
- Sekjen KOMINFO
- Badan Siber dan Sandi Negara (BSSN)

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirtpdn.layanan.go.id/rfc2350-id.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 PDN-CSIRT;
Versi : 1.0;
Tanggal Publikasi : 23 Desember 2024;
Kedaluwarsa : valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

PUSAT DATA NASIONAL-*COMPUTER SECURITY INCIDENT RESPONSE TEAM*
Disingkat : PDN-CSIRT

2.2. Alamat

Direktorat LAIP
Gedung Utama Kementerian KOMINFO
Jl. Medan Merdeka Barat no. 9,
Jakarta 10110, Indonesia

2.3. Zona Waktu

Asia/Jakarta, WIB, (GMT+07:00)

2.4. Nomor Telepon

+62-21-3849366

2.5. Nomor Fax

+62-21-3849366

2.6. Telekomunikasi Lain

Telegram: +62 811-1193-226
Whatsapp: +62 815-7300-0232
Call center: 1500559

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

pdn-csirt[at]layanan[dot]go[dot]id

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

Bits : 255
ID : 0x73802BD6
Key Fingerprint : 1A35 DAEF E63B BE93 C314 3272 CE5D 2119 2BD6

-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: User ID: PDN-CISRT <pdn-csirt@layanan.go.id>
Comment: Type: 255-bit EdDSA (secret key available)
Comment: Usage: Signing, Encryption, Certifying User IDs
Comment: Fingerprint: E950F07C59022E0BB1BE79BB3F96F192CF89325A

mDMEZ4h6MRYJKwYBBAHaRw8BAQdA9Ezc8Rv9gOOBZcigDJhBPt0dmkhhTZEuMvng
gu2OMxq0I1BETi1DSVNSVCA8cGRuLWNzaXJ0QGxheWFuYW4uZ28uaWQ+iJMEExYK
ADsWIQTpUPB8WQIuC7G+ebs/lvGSz4kyWgUCZ4h6MQIbAwULCQgHAgIiAgYVCgkI
CwIEFgIDAQIeBwIXgAAKCRA/lvGSz4kyWp/EAP0dbcSgaYyfzyM2UqRQk7VgEkMZ
ZqKaisPlsYcyaWqlKAEAqw6z/7i+p6FBEZePm/Szawrm6b4eyUZgp0SvSSVBCgm4
OARniHoxEgorBgEEAZdVAQUBAQdAEUCaSu6gpQKebc7MREXOZBkt0Whn7b17rce2
TgHAv2YDAQgHiHgEGBYKACAWIQTpUPB8WQIuC7G+ebs/lvGSz4kyWgUCZ4h6MQIb
DAAKCRA/lvGSz4kyWlYOAP4rqB529vbbSJM+C/VjDkCyuLI1jTHXtHoVyrD3jLgl
OwEA78LDqPEmLVvpjlU174eHFmZMab4MSbmZYfTEct7ffAI=
=B4xm
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirtpdn.layanan.go.id/publickey.asc

2.9. Anggota Tim

Ketua PDN-CSIRT adalah Direktur Layanan Aplikasi Informatika Pemerintahan (LAIP), dan personil PDN-CSIRT merupakan personil pada lingkungan Ditjen APTIKA

2.10. Informasi/Data lain

-

2.11. Catatan-catatan pada Kontak PDN-CSIRT

Metode yang disarankan untuk menghubungi PDN-CSIRT adalah melalui *e-mail* pada alamat **pdn-csirt[at]layanan[dot]go[dot]id** atau melalui nomor telepon +62-21-3849366 pada hari dan jam kerja atau nomor narahubung +62815-1402-1890 atau +62 853-6120-8925 siaga selama 24/7.

3. Mengenai PDN-CSIRT

3.1. Visi

Mewujudkan layanan infrastruktur dan sistem elektronik pada Pusat Data Nasional yang aman dan handal sesuai dengan prinsip keamanan pada Infrastruktur Sistem Pemerintahan Berbasis Elektronik (SPBE) Nasional.

3.2. Misi

- Memastikan keamanan meliputi kerahasiaan, keutuhan, dan ketersediaan data serta informasi dalam pelaksanaan SPBE di PDN.
- Menerapkan keamanan pada infrastruktur PDN berdasarkan standar teknis dan prosedur keamanan SPBE.
- Melakukan edukasi dan pembinaan untuk meningkatkan kesadaran terhadap keamanan sistem elektronik di PDN.

3.3. Konstituen

- Seluruh IPPD pemilik/penyelenggara SPBE yang berjalan di PDN.
- Seluruh pengguna Sistem Elektronik di lingkungan Direktorat Jenderal Aplikasi Informatika yang berjalan di PDN.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan PDN-CSIRT bersumber dari APBN

3.5. Otoritas

- bertanggung jawab sesuai dengan skema *Shared Responsibility* layanan PDN
- bertanggung jawab infrastruktur, network, monitoring tools
- bertanggung jawab terhadap asset/ sistem elektronik yang milik dari LAIP/Kominfo yang ada di PDN.
- bertanggung jawab terhadap Sistem Elektronik Direktorat LAIP
- berkoordinasi dengan:
    - tim CSIRT Nasional/Sektoral, tim CSIRT dari IPPD, dan tim CSIRT penyedia layanan,

- *Security Operations Center* (SOC) dengan manage service PDN, Penyedia PDNS
- Network and System Administrators dengan manage service PDN, Penyedia PDNS, penyedia JIP
- *Legal and Compliance Teams* dengan Bagian Hukum dan Kerjasama, Sesditjen Aptika,
- *Public Relations* (PR) dengan Bagian Hukum dan Kerjasama Sesditjen Aptika,
- Manajemen Eksekutif dengan Dirjen Aptika, Direktur LAIP, Sesditjen Aptika, dan
- pihak lain yang terkait

4. Kebijakan – Kebijakan

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

- Serangan terhadap *confidentiality*/kerahasiaan data
- System Availability Attack (DDoS, Ransomware)
- System Integrity Attack (MITM, SQL Injection, dll)

dukungan penyelesaian insiden meliputi:

- Mengenali insiden,
- Pembatasan kerusakan,
- Mengidentifikasi pelaku insiden,
- Memperbaiki kerusakan/pemulihan,
- Menyusun rekomendasi,
- Berkomunikasi/berkoordinasi pihak terkait,
- Membuat laporan akhir

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

- PDN-CSIRT bekerjasama dengan BSSN dan CSIRT dari IPPD serta SOC dari *Managed Service* PDN meliputi:
  - Membentuk Hubungan dan Kanal Komunikasi yang Aman
  - Menerapkan Prosedur Pelaporan Insiden
  - Berbagi Informasi Ancaman (*Threat Intelligence Sharing*)
  - Kolaborasi dalam Penanggulangan Insiden
  - Berbagi Pelajaran dan Rekomendasi
  - Partisipasi dalam Komunitas CSIRT
  - Menerapkan Kerangka Hukum dan Regulasi
- Informasi akan dirahasiakan sesuai dengan klasifikasi informasi yang *Traffic Light Protocol (TLP)*, yang mengklasifikasikan informasi berdasarkan tingkat kerahasiaan sebagai berikut:
  - TLP:RED : Hanya dibagikan dengan penerima yang dituju.
  - TLP:AMBER : Dapat dibagikan dalam organisasi yang dibatasi.
  - TLP:GREEN : Dapat dibagikan di komunitas CSIRT.
  - TLP:WHITE : Dapat dibagikan secara publik.

4.3. Komunikasi dan Autentikasi

- Informasi biasa melalui email dan telepon biasa
- Informasi terbatas/rahasia melalui saluran terenkripsi

5. Layanan

5.1. Layanan reaktif, yaitu:

- Pemberian peringatan (alerts and warning);
- Penanggulangan dan pemulihan insiden siber (incident handling);
- Penanganan kerawanan (vulnerability handling); dan
- Penanganan artefak (artifact handling).

5.2. Layanan proaktif, yaitu:

- Pemberitahuan hasil pengamatan potensi ancaman; dan
- Pendeteksian serangan.

5.3. Layanan manajemen kualitas keamanan, yaitu:

- Analisis risiko (risk analysis); dan
- Edukasi dan pelatihan (education/training).

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan melalui email: **pdn-csirt[at]layanan[dot]go[dot]id** dengan melampirkan sekurang-kurangnya :

a. Identitas pelapor yang jelas berupa foto/*scan* kartu identitas
b. Bukti insiden, dapat berupa video, foto, *screenshoot,* atau *log file*
c. dokumen lain terkait sesuai dengan ketentuan lain yang berlaku

7. Penafian / *Disclaimer*

Dokumen ini disusun berdasarkan panduan RFC 2350 dan bertujuan memberikan gambaran umum tentang kebijakan, prosedur, dan layanan yang disediakan oleh PDN-CSIRT. Meskipun setiap upaya telah dilakukan untuk memastikan bahwa informasi dalam dokumen ini akurat dan mutakhir, dokumen ini tidak menjamin kelengkapan, ketepatan, atau ketepatan waktu informasi yang diberikan.

PDN-CSIRT berhak untuk memperbarui atau mengubah kebijakan dan prosedurnya tanpa pemberitahuan sebelumnya.

PDN-CSIRT tidak bertanggung jawab atas kerugian atau kerusakan apa pun yang timbul dari penggunaan informasi ini, baik secara langsung maupun tidak langsung. Pengguna didorong untuk menghubungi PDN-CSIRT untuk klarifikasi lebih lanjut atau informasi terbaru.