RFC 2350 APJII-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 01 November 2024

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan pembaruan dokumen

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
>https://csirt.apjii.or.id/doc/rfc2350-id.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Kedua dokumen telah ditandatangani dengan PGP *Key* milik APJII-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 APJII-CSIRT;
Versi	: 1.0;
Tanggal Publikasi	: 01 November 2024;
Kedaluwarsa	: Dokumen ini valid sampai dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Asosiasi Penyelenggara Jasa Internet Indonesia – Computer Security Incident response Team
Disingkat : APJII-CSIRT

2.2. Alamat

Gedung Cyber, Jl. Kuningan Barat Raya No.8, RT.1/RW.3, Kuningan Bar., Kec. Mampang Prpt., Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12710

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

021 5296 0634

2.5. Nomor Fax

021 5296 0635

2.6. Telekomunikasi Lain

-

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

csirt[at]apjii.or.id

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

File PGP *key* ini tersedia pada :
https://csirt.apjii.or.id/doc/apjii-pub.asc

2.9. Anggota Tim

Ketua APJII-CSIRT adalah Kabid Keamanan Security. Yang termasuk anggota tim adalah BPH yang diberi mandat dan tugas oleh kabid keamanan security APJII

2.10. Informasi/Data lain

Tidak ada

2.11. Catatan-catatan pada Kontak APJII-CSIRT

Metode yang disarankan untuk menghubungi APJII-CSIRT adalah melalui *e-mail* pada alamat csirt[at]apjii.or.id atau melalui nomor telepon 021 5296 0634.

3. Mengenai Gov-CSIRT

3.1. Visi

Visi APJII-CSIRT adalah Terwujudnya keamanan siber dalam mendukung layanan TI berkualitas untuk Anggota APJII , dalam mewujudkan Indonesia Aman Berdigital

3.2. Misi

Misi dar APJII-CSIRT, yaitu :

a. Melaksanakan Kegiatan pengamanan siber terhadap layanan yang bersifat Digital
b. Meningkatkan kapasitas dan kemampuan sumber daya, pada aspek pencegahan penanggulangan dan pemulihan keamanan siber
c. Memberi literasi atau informasi yang masif tentang keamanan siber

3.3. Konstituen

Konstituen APJII-CSIRT yaitu penguna layanan digital dilingkungan APJII

3.4. Sponsorship dan/atau Afiliasi

APJII-CSIRT merupakan bagian dari Badan kepengurusan bidang keamanan cyber APJII, sehingga seluruh pembiayaan bersumber dari APPA.

3.5. Otoritas

APJII-CSIRT memiliki kewenangan dalam penanganan gangguan keamanan siber diruang lingkup lingkungan APJII dan juga APJII-CSIRT bisa melakukan koordinasi serta bekerjasama dengan pihak lain yang memiliki kewenangan dalam menangani dan menanggulangi insiden yang sedang dan akan terjadi

4. Kebijakan – Kebijakan

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

APJII-CSIRT melayani penanganan insiden siber dengan jenis berikut :

a. *Web Defacement;*
b. *DdoS;*
c. *Malware;*
d. *Phising;*
e. *Spamming;*

Dukungan yang diberikan oleh APJII-CSIRT kepada anggota bisa dalam berbagai cara tergantung jenis dan dampak insiden yang dialami oleh anggota, dan layanan penanganan insiden itu bisa dilakukan berdasarkan laporan dari anggota.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

APJII-CSIRT bekerjasama dan berbagi informasi dengan CSIRT atau organisai lain nya dalam lingkup keamanan siber, dan segala informasi yang diterima oleh APJII-CSIRT akan bersifat rahasia dan tidak akan di publikasi kan

4.3. Komunikasi dan Autentikasi

Dalam hal berkomunikasi biasa APJII-CSIRT menggunakan email tanpa enkripsi, dan telepon selular, akan tetapi jika informasi bermuatan sensitif/rahasi/terbatas bisa menggunakan enkripsi pgp pada email

5. Layanan

5.1. Layanan Utama

Layanan utama dari APJII-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini berupa pemberitahuan dan peringatan kepada anggota atau pemilik sistem elektronik dan informasi bahwa adanya insiden siber yang terjadi pada salah satu system mereka yang sedang berjalan.

5.1.2. Penanganan Insiden Siber

Layanan ini berupa koordinasi, analisa, dan rekomendasi teknis serta bantuan langsung untuk penanggulangan dan pemulihan insiden siber

5.2. Layanan Tambahan

Layanan tambahan dari APJII-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini berupa koordinasi, analisa, dan rekomendasi teknis untuk penguatan keamanan perangkat dan sistem informasi.

5.2.2. Penanganan Artefak Digital

Layanan ini merupakan penanganan dalam rangka pemulihan sistem elektronik yang terdampak atau juga berupa dukungan analisa dan investigasi

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Informasi hasil dari analisa dan pengamatan terkait ancaman insiden siber yang mungkin akan terjadi

5.2.4. Pendeteksian Serangan

Melakukan monitoring dan pendeteksian terhadap berbagai serangan yang terjadi di jalur jalur pertukaran data anggota

5.2.5. Analisis Risiko Keamanan Siber

Identifikasi kerentanan dan penilaian resiko kerentanan yang ditemukan dan akan diberikan rekomendasi untuk mengurangi resiko nya

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Memberikan konsultasi terkait kesiapan penganggulangan dan pemulihan keamanan siber.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Pemberian informasi dan sosialisasi serta pembinaan kepada seluruh anggota APJII yang bertujuan untuk meningkatkan kesadaran dan kepedulian tentang keamanan siber

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt[at]apjii.or.id dengan melampirkan sekurang-kurangnya :

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

7. *Disclaimer*

- ***Sampai saat ini APJII-CSIRT hanya merespon dan menangani insiden keamanan siber yang terjadi pada perangkat perangkat pertukaran data yang dikelola oleh APJII***

- ***Terkait penanganan insiden akan dilakukan sesuai dengan tools yang dimiliki***