RFC 2350 KPK-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 17 Oktober 2022.

1.2. Daftar Distribusi untuk Pemberitahuan

Satuan Kerja di lingkungan KPK.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :

https://csirt.kpk.go.id/sdm_downloads/kpk-rfc2350/ (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 KPK-CSIRT;

Versi : 2.0;

Tanggal Publikasi : 17 Oktober 2022;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Komisi Pemberantasan Korupsi - Computer Security Incident Response Team
Disingkat : KPK - CSIRT.

2.2. Alamat

KPK CSIRT
Jln. Kuningan Persada Kav. 4
Jakarta Selatan 12950

2.3. Zona Waktu

DKI Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 25578300 ext.(8192)

2.5. Nomor Fax

(021) 2557 8333

2.6. Telekomunikasi Lain

Telegram KPK-CSIRT

Whatsapp KPK-CSIRT

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

csirt[at]kpk[dot]go[dot]id

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

Bits : 4096

ID : 0xFD390BE6

Key Fingerprint : 3E6F 432C F68F 7A38 0C13 5427 793F 3BF6 FD39 0BE6

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

```
mDMEYsl6gBYJKwYBBAHaRw8BAQdArEeK0iaUdWXfiZPZ8Uuf4pUgPgNx7wswGhxt
dBPxPei0G0tQSyBDU0ISVCA8Y3NpcnRAa3BrLmdvLmlkPoiZBBMWcGBBFiEEPm9D
LPaPejgME1QneT879v05C+YFAmLCOoACGwMFCQEebq9AFCwkIBwIClgIGFQoJCAcC
BBYCAwECHgcCF4AACgkQeT879v05C+bPPAEakvXNY0pTjwgo7mCBxOD6e+HCPR4
v
AK8lhKLIQ2oWOtUA/0Aq53P+wG8YyL0QVxIHQVGiXJ2s8MVJW0JtvstCN1QFuDgE
Ysl6gBIKKwYBBAGXVQEFAQEHQHlLwJr9wGhYdpiM19QV1tMnDJke/T9QsrAFsMf
tHAtAwEIB4h+BBgWCgAmFiEEPm9DLPaPejgME1QneT879v05C+YFAmLCOoACGwwF
CQEebq9AACgkQeT879v05C+bzDgEAtllwUHvAo1YQiQ3wPya0yUO8LpyuEVmA8XOV
3EkV//wA/io6ubmMxD5VR7S5EKIk70Wol+DEPcfWWTqXy5VXQR0D
=dO7/
```

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

File PGP *key* ini tersedia pada :

https://csirt.kpk.go.id/sdm_downloads/pgp-key-csirt/

2.9. Anggota Tim

Ketua KPK-CSIRT adalah Direktur Manajemen Informasi Komisi Pemberantasan Korupsi. Yang termasuk anggota tim adalah seluruh staf Direktorat Manajemen Informasi dan Seketrariat Keamanan Informasi KPK.

2.10. Informasi/Data lain

Saat ini jam operasional mengacu pada katalog layanan IT.

2.11. Catatan-catatan pada Kontak KPK-CSIRT

Metode yang disarankan untuk menghubungi KPK-CSIRT adalah melalui e-mail pada alamat csirt[at]kpk.go.id atau melalui Signal/Whatsapp KPK-CSIRT yang siaga selama 24/7.

3. Mengenai Gov-CSIRT

3.1. Visi

Visi KPK-CSIRT adalah terwujudnya ketahanan siber pada sistem dan infrastruktur lembaga yang Handal dan Profesional.

3.2. Misi

Misi dari KPK-CSIRT, yaitu :

- a. Membangun pusat pengelolaan dan pelaporan insiden keamanan Teknologi informasi di lingkungan Komisi Pemberantasan Korupsi;
- b. Membangun koordinasi, kerjasama dan kolaborasi dengan pihak terkait dan negara lain untuk membangun pertahanan siber yang Tangguh;
- c. Menyediakan dan mengoptimalkan sumber daya pertahanan siber melalui proses pembelajaran dan peningkatan kualitas yang berkelanjutan.

3.3. Konstituen

Konstituen KPK-CSIRT meliputi :

- a. Pengguna layanan TIK di KPK

3.4. Sponsorship dan/atau Afiliasi

Pendanaan KPK-CSIRT bersumber dari APBN

3.5. Otoritas

- a. KPK-CSIRT memiliki kewenangan dalam penanganan gangguan keamanan siber, mitigasi, investigasi dan analisis dampak insiden dilingkungan KPK;
- b. koordinasi, kerjasama dan kolaborasi dengan pihak terkait dan negara lain untuk membangun ketahanan siber lembaga dan nasional.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

KPK-CSIRT melayani penanganan insiden siber dengan jenis berikut :

- a. Web Defacement;
- b. DDoS;
- c. Virus/Malware;
- d. Ransomware;
- e. Phising;
- f. SQL Injection.

Dukungan yang diberikan oleh KPK-CSIRT kepada konstituen dapat bervariasi bergantung pada jenis dan dampak insiden. Layanan penanganan insiden berdasarkan pada laporan konstituen.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa KPK-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 KPK-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik yang dikelola oleh masing-masing satuan kerja di KPK.

5.1.2. Penanganan Insiden Siber

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

5.2. Layanan Tambahan

Layanan tambahan dari KPK-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini diberikan oleh KPK-CSIRT berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (hardening), layanan ini hanya berlaku apabila syarat-syarat berikut terpenuhi :

- a. Pelapor atas kerawanan adalah pemilik sistem elektronik. Jika pelapor adalah bukan pemilik sistem, maka laporan kerawanannya tidak dapat ditangani;
- b. Layanan penanganan kerawanan yang dimaksud dapat juga merupakan tindak lanjut atas kegiatan Vulnerability Assessment.

5.2.2. Penanganan Artefak Digital

Layanan ini diberikan berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini diberikan berupa hasil dari sistem deteksi dini honeynet BSSN, bisa juga laporan masyarakat berupa hasil deteksi adanya celah keamanan, selanjutnya KPK CSIRT memberikan informasi statistik terkait layanan ini.

5.2.4. Pendeteksian Serangan

Layanan ini berupa kegiatan analisis untuk mendeteksi adanya serangan terhadap sistem elektronik.

5.2.5. Analisis Risiko Keamanan Siber

Layanan ini berupa kegiatan analisis untuk mendeteksi adanya serangan terhadap sistem elektronik dan dokumentasi kerentanan dan penilaian risiko keamanan informasi yang sesuai dengan standar ISO/IEC 27001.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

KPK-CSIRT memberikan wawasan, pemahaman, dan cara yang perlu dilaksanakan dalam rangka membantu penanganan Insiden Siber.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

KPK-CSIRT membangun tiga pilar utama dalam transformasi digital yakni People, Process, Technology untuk mendukung pembangunan kesadaran terhadap keamanan informasi yang berkelanjutan, dengan cara.

- a. Menyelenggarakan kegiatan sharing session keamanan siber di lingkungan KPK;
- b. kegiatan diseminasi di bidang keamanan siber kepada pihak yang menerima layanan.

6. Pelaporan Insiden

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

- a. Foto/scan kartu identitas
- b. Nama, email, nomor kontak
- c. Bukti insiden berupa foto atau screenshot atau log file yang ditemukan
- d. Atau sesuai dengan ketentuan lain yang berlaku

7. Disclaimer

KPK-CSIRT adalah sebuah fungsi dalam organisasi sebagai gerbang komunikasi atau Single Point Of Contact (SPOC) antara penyedia layanan dan pelapor aduan siber.

Hal yang ditangani adalah :

1. Menerima laporan aduan siber.
2. menindaklanjuti laporan aduan siber.