RFC 2350 KPK-CSIRT

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi tentang informasi dasar mengenai KPK-CSIRT, tugas fungsi/tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi KPK-CSIRT.

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 2.0 yang diterbitkan pada tanggal 28 Juli 2026.

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/rfc-2350/

1.4. Keaslian Dokumen

Dokumen telah ditanda tangani secara elektronik oleh Ketua Tim Tanggap Insiden Siber KPK (KPK-CSIRT)

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 KPK CSIRT;

Versi : 2.0;

Tanggal Publikasi : 28 Juli 2026;

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

Jln. Kuningan Persada Kav. 4

Jakarta Selatan 12950

2.3. Zona Waktu

DKI Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 2557 8333 ext.(8192)

2.5. Nomor Fax

(021) 2557 8333

2.6. Telekomunikasi Lain

(+62) 811-1705-0551

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

File PGP *key* ini tersedia pada :

https://csirt.kpk.go.id/rfc-2350/

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

mDMEZ76RPhYJKwYBBAHaRw8BAQdAU0myKztdCa2sd/VzSX0CY8beHVrnM+6PTAq1

i1r9UCW0G0NTSVJUIEtQSyA8Y3NpcnRAa3BrLmdvLmlkPoiZBBMWCgBBFiEEjw1Z

2OGKEqnyFxUzsvcT0PevIyQFAme+kT4CGwMFCQPCdZIFCwkIBwICIgIGFQoJCAsC

BBYCAwECHgcCF4AACgkQsvcT0PevIyTwaAEAlEHdsVk9XHPCxzUY9GFyBJgSejcg

/mONY1lbSWs5IkUA/3j1EwjKQGTaYnxzikBmx6yw59SaFXAUMJ/c4TkkBBMPuDgE

Z76RPhIKKwYBBAGXVQEFAQEHQKyroUAjc4Udrd2Yue2ut/LzlYA1dWIGGyvTGMGU

738EAwEIB4h+BBgWCgAmFiEEjw1Z2OGKEqnyFxUzsvcT0PevIyQFAme+kT4CGwwF

CQPCdZIACgkQsvcT0PevIyTElwEAyNRywpDsJgIb4U35OQlg0Omx/DWOYEdtHqnZ

xdUcQ1kA/1BwvrWBsHbfn1A2F8qj+vzDFPHdkVGMnHCBrykPDScJ

=t2yq

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

2.9. Anggota Tim

Ketua KPK-CSIRT adalah Direktur Manajemen Informasi, KPK. Yang termasuk anggota tim adalah Koordinator Penanggulangan dan Pemulihan Insiden, Unit User Handling, Unit Respon Insiden, Unit Pemulihan Layanan Operasional TI, Unit Tata Kelola dan Kepatuhan dan Narahubung.

2.10. Informasi/Data lain

-

2.11. Catatan-catatan pada Kontak KPK-CSIRT

Metode yang disarankan untuk menghubungi KPK-CSIRT adalah melalui *e-mail* pada alamat csirt[at]kpk[dot]go[dot]id atau melalui nomor telepon KPK CSIRT ke (+62) 811-1705-0551) pada hari kerja jam 08.00 - 17.00 WIB atau siaga selama 24/7.

3. Mengenai KPK-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 semua pengguna layanan teknologi informasi di lingkungan Komisi Pemberantasan Korupsi.

3.4. Sponsorship dan/atau Afiliasi

KPK-CSIRT merupakan bagian dari Pusat Data dan Informasi Komisi Pemberantasan Korupsi sehingga seluruh pembiayaannya bersumber dari APBN.

3.5. Otoritas

KPK-CSIRT memiliki kewenangan dengan konstituennya dalam penanganan gangguan keamanan siber. KPK-CSIRT dapat berkoordinasi serta bekerja sama dengan pihak lain yang mempunyai kompetensi untuk insiden yang tidak dapat ditangani.

4. Kebijakan – Kebijakan

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

KPK-CSIRT melayani penanganan insiden siber dengan jenis berikut :

1. Web Defacement;
2. DDoS;
3. Virus/Malware;
4. Ransomware;
5. Phising;
6. 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 :

1. Pelapor atas kerawanan adalah pemilik sistem elektronik. Jika pelapor adalah bukan pemilik sistem, maka laporan kerawanannya tidak dapat ditangani;
2. 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 artifak 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.

1. Menyelenggarakan kegiatan sharing session keamanan siber di lingkungan KPK;
2. 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 :

1. Nama, email, nomor kontak
2. Bukti insiden berupa foto atau screenshoot atau log file yang ditemukan dalam bentuk dokumen laporan format pdf.

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.