RFC 2350 Wantimpres-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 13 Oktober 2025.

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://wantimpres.go.id/wp-content/uploads/2025/10/rfc2350-id.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen telah ditanda tangani secara elektronik oleh Ketua Wantimpres-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 Wantimpres-CSIRT
Versi	: 1.0
Tanggal Publikasi	: 13 Oktober 2025
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan

2. Informasi Data/Kontak

2.1. Nama Tim

Dewan Pertimbangan Presiden

Disingkat : Wantimpres-CSIRT

2.2. Alamat

Jalan Veteran III No. 2, Jakarta Pusat 10110

2.3. Zona Waktu

Jakarta, GMT+07:00

2.4. Nomor Telepon

(021) 3444801

2.5. Nomor Fax

Tidak ada.

2.6. Telekomunikasi Lain

Tidak ada.

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

csirt.wantimpres[at]setneg.go.id

2.8. Kunci Publik (*Public Key*)

Berikut ini PGP Public Key Wantimpres-CSIRT

Key ID	B0BE03F656B96608
Fingerprint	395B AD93 6F40 708D 4CAF 29D9 B0BE 03F6 56B9 6608
Public Key	-----BEGIN PGP PUBLIC KEY BLOCK----- xjMEaOX2IBYJKwYBBAHaRw8BAQdAXcqYKggR/nvSykRpMHwSxjoP9g/RQOWH D6uX158LdaLNMFdhbnRpbXByZXMtQ1NJUlQgPGNzaXJ0LndhbnRpbXByZXNA c2V0bmVnLmdvLmlkPsKMBBAWCgA+BYJo5fYgBAsJBwgJkLC+A/ZWuWYIAxUI CgQWAAIBAhkBApsDAh4BFiEEOVutk29AcI1MrynZsL4D9la5ZggAAPWUAP9U JuILTBk12SLPGb3e0GonRSqwOkkTKi9T7H/EiU5mhwD+Kr/d/13Hp2WNvEsm nV61+AMHbIyhhTs3BsnlUbNEzQnOOARo5fYgEgorBgEEAZdVAQUBAQdAcJGE 5wp60IHIp3JztVZ7NX5UT17PgonAhy01XOWFuWgDAQgHwngEGBYKACoFgmjl 9iAJkLC+A/ZWuWYIApsMFiEEOVutk29AcI1MrynZsL4D9la5ZggAAI9VAP9y iB4XbJZKcMU3f6SiPxHH/9gJOQIHF4dDpts8nrLp3QD+LI77m7qS4DbBEevJ wv46iQILsPsd9NNRbVOfPry/JA4= =6Ty5 -----END PGP PUBLIC KEY BLOCK-----

File PGP Public Key juga tersedia pada:
https://wantimpres.go.id/wp-content/uploads/2025/10/public-key.asc

2.9. Anggota Tim

Keanggotaan tim sesuai dengan Surat Keputusan Sekretaris Dewan Pertimbangan Presiden.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak Wantimpres-CSIRT

Metode yang disarankan untuk menghubungi Wantimpres-CSIRT adalah melalui *e-mail* pada alamat csirt.wantimpres[at]setneg.go.id atau melalui nomor telepon Dewan Pertimbangan Presiden ke 021 3444801 pada hari kerja jam 07.30 - 16.00 (Senin-Kamis) dan 07.30-16.30 (Jum'at).

3. Mengenai Wantimpres-CSIRT

3.1. Visi

Visi Wantimpres-CSIRT adalah mewujudkan ekosistem layanan TI Wantimpres yang tangguh terhadap ancaman dengan respons insiden cepat, pemulihan efektif, dan mitigasi risiko proaktif.

3.2. Misi

Misi dari Wantimpres-CSIRT yaitu:

1. Memelihara keamanan sistem elektronik;
2. Melakukan penanganan insiden siber yang mengganggu sistem elektronik;
3. Melakukan pemulihan sistem elektronik pasca terjadinya insiden siber;
4. Melakukan mitigasi risiko dan potensi terjadinya insiden siber;
5. Meningkatkan kesadaran dan kompetensi pegawai di bidang keamanan informasi;
6. Menjalin kerja sama strategis dengan pemangku kepentingan terkait untuk memperkuat sistem keamanan informasi.

3.3. Konstituen

Konstituen Wantimpres-CSIRT meliputi semua pengguna layanan teknologi informasi di lingkungan Dewan Pertimbangan Presiden.

3.4. Sponsorship dan/atau Afiliasi

Wantimpres-CSIRT merupakan bagian dari Sekretariat Dewan Pertimbangan Presiden sehingga seluruh pembiayaannya bersumber dari APBN.

3.5. Otoritas

Wantimpres-CSIRT memiliki kewenangan dengan konstituennya dalam penanganan gangguan keamanan siber. Wantimpres-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

Wantimpres-CSIRT menangani insiden seperti kebocoran akun/identitas, malware/ransomware, phishing, penyalahgunaan hak akses, kebocoran/eksfiltrasi data, serangan DDoS, web defacement, dan eksploitasi kerentanan aplikasi/infrastruktur.

Dukungan kami mencakup triage dan validasi (Tier-1), analisis teknis serta containment/mitigasi (Tier-2), hingga forensik, eradikasi, dan pemulihan layanan (Tier-3), termasuk koordinasi dengan pemilik sistem, vendor, dan otoritas terkait. Prioritas penanganan ditetapkan berbasis dampak dan urgensi.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Wantimpres-CSIRT berkolaborasi dengan unit internal, penyedia layanan, mitra strategis, CSIRT instansi lain dan CSIRT sektoral/nasional. Seluruh pertukaran informasi mengikuti asas *need-to-know.* Data sensitif dan identitas pelapor dilindungi dan hanya diungkap secara minimal, teranonimisasi, atau sesuai perintah/peraturan perundang-undangan yang berlaku.

4.3. Komunikasi dan Autentikasi

- **Klasifikasi Publik/Umum:** dikirim melalui email **tanpa enkripsi** ditujukan ke alamat csirt.wantimpres[at]setneg.go.id.
- **Terbatas/Rahasia/Sangat Rahasia**: dikirim melalui email **terenkripsi** menggunakan Kunci Publik PGP (lihat bagian 2.8 Kunci Publik) ditujukan ke alamat csirt.wantimpres[at]setneg.go.id.

5. Layanan

5.1. Layanan Utama

Layanan utama dari Wantimpres-CSIRT yaitu :

5.1.1. Penanganan Insiden Siber

Wantimpres-CSIRT melakukan rangkaian tindakan terkoordinasi untuk menghentikan dampak insiden (*containment*), menghapus akar penyebab (*eradication*), dan memulihkan layanan serta data ke kondisi aman (*recovery*).

5.1.2. Pemberian Peringatan Terkait Insiden Siber

Wantimpres-CSIRT menyampaikan informasi insiden kepada pemangku kepentingan yang berwenang dengan prinsip *need-to-know* .

5.2. Layanan Tambahan

Layanan tambahan dari Wantimpres-CSIRT yaitu :

5.2.1. Pembangunan kesadaran dan kepedulian terhadap keamanan siber

Wantimpres-CSIRT meningkatkan literasi dan perilaku aman melalui berbagi program termasuk kampanye komunikasi, pelatihan, simulasi phishing, materi praktis (kata sandi kuat, MFA, klasifikasi dan penanganan data, serta etika penggunaan teknologi).

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt.wantimpres[at]setneg.go.id dengan melampirkan sekurang-kurangnya:

a. Nama
b. Penjelasan dan langkah penemuan insiden
c. Bukti insiden berupa foto, *screenshoot* atau *file* yang ditemukan
d. Data pendukung lain yang dianggap perlu

7. *Disclaimer*

a. Kami menghargai partisipasi Anda dalam membantu menjaga keamanan sistem informasi Wantimpres.
b. Identitas pelapor akan dijaga kerahasiaannya oleh Wantimpres dan hanya dapat diungkap jika diwajibkan oleh hukum yang berlaku.
c. Kami tidak mentoleransi penyalahgunaan celah keamanan, uji penetrasi tanpa otorisasi, atau tindakan apa pun yang dapat merusak ketersediaan, kerahasiaan, dan integritas layanan atau data.
d. Wantimpres berhak mengambil langkah yang diperlukan untuk menjaga keamanan layanan sesuai peraturan perundang-undangan yang berlaku.
e. Wantimpres tidak memiliki program *bug bounty*, imbalan, kompensasi, atau bentuk penghargaan sejenis untuk pelaporan kerentanan.
f. Dengan mengirimkan laporan, pelapor menyatakan memahami dan menyetujui ketentuan di atas.

Jakarta, 13 Oktober 2025
Kepala Biro Data dan Informasi,

M. Arfan Sahib Sali Kando