RFC 2350 TTIS-PU

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi Tim Tanggap Insiden Siber Kementerian Pekerjaan Umum (TTIS-PU) berdasarkan RFC 2350, yaitu informasi dasar mengenai TTIS-PU, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi TTIS-PU.

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 1 Juni 2025

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt.pu.go.id/RFC2350

1.4. Keaslian Dokumen

Dokumen telah ditandatangani dengan secara elektronik menggunakan sertifikat yang dikeluarkan oleh BSSN.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 TTIS-PU
Versi	: 1.0
Tanggal Publikasi	: 1 Juni 2025
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Tim Tanggap Insiden Siber Kementerian Pekerjaan Umum (TTIS-PU)
Disingkat : TTIS-PU.

2.2. Alamat

Kementerian Pekerjaan Umum
Gedung Pusdatin
Jalan Pattimura 20
Kebayoran Baru, Jakarta Selatan
DKI Jakarta, Indonesia 12110

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 7232366

2.5. Nomor Fax

Tidak ada

2.6. Telekomunikasi Lain

(+62) 81119500600 WhatsApp Center Pusdatin

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

batin20[at]pu[.]go[.]id

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

Bits : 256
ID : 78CA 638F DFF6 72BA
Key Fingerprint : B119AB2E7BBCFC2ABFDDDDC378CA638FDFF672BA

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

mDMEZNnHcRYJKwYBBAHaRw8BAQdAxpM8fsoafcAapG6kly+qF3sUj1Gk4Khxzhwk
xdPtnSy0H1BVUFItQ1NJUlQyMCA8YmF0aW4yMEBwdS5nby5pZD6ImQQTFgoAQRYh
BLEZqy57vPwqv93dw3jKY4/f9nK6BQJk2cdxAhsDBQkJaJHfBQsJCAcCAiICBhUK
CQgLAgQWAgMBAh4HAheAAAoJEHjKY4/f9nK6olYA/jxv65FCkQztSsqeV/UJtzHd
MmUlhgkcF3jOnW1AHPfzAP0cCsA0T4SFJbD57jyKMoiCBoAUDGTYjTakPl9eLXJk
Bbg4BGTZx3ESCisGAQQBl1UBBQEBB0CBmAx8KyAtR9wJU8T6Oy/oi4xa8XF0Tayn
AoWXZp2cSAMBCAeIfgQYFgoAJhYhBLEZqy57vPwqv93dw3jKY4/f9nK6BQJk2cdx
AhsMBQkJaJHfAAoJEHjKY4/f9nK6gyYBAOf8XRkvADFqHDrKWw0Y9harjQQCfXFK
/DeDC0WotRMBAPwKRcVxcQ+oeOseyIxzkbR5FKJNfdoe42Wa+6BT1+aaAg==
=vPLq
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirt.pu.go.id/storage/asc/pgp_public_pu.asc

2.9. Anggota Tim

Ketua TTIS-PU adalah Kepala Pusat Data dan Teknologi Informasi. Yang termasuk anggota tim adalah personil yang tercantum pada SK Sekretaris Jenderal Kementerian Pekerjaan Umum tentang Pembentukan Tim Tanggap Insiden Siber Kementerian Pekerjaan Umum.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak TTIS-PU

Metode yang disarankan untuk menghubungi TTIS-PU adalah melalui *e-mail* pada alamat batin20@pu.go.id atau melalui nomor telepon +62 811 1950 0600 WA Center

Pusdatin siaga selama 24/7.

3. Mengenai TTIS-PU

3.1. Visi

Visi TTIS-PU adalah terwujudnya tata kelola keamanan teknologi informasi di lingkungan Kementerian Pekerjaaan Umum sesuai dengan prinsip utama keamanan informasi, menjamin ketersediaan (*availability*), keutuhan (*integrity*) dan kerahasiaan (*confidentiality*) informasi.

3.2. Misi

Misi dari TTIS-PU, yaitu :

a. Mendorong kegiatan pengamanan informasi di pusat dan daerah dan pencegahan insiden keamanan informasi.
b. Melakukan pengujian / security assessment pada aplikasi, baik yang sudah berjalan maupun dalam pengembangan.
c. Memastikan keamanan jaringan dan lalu lintas data, baik di pusat dan daerah.
d. Membangun kesadaran tentang keamanan informasi (end user education & security awareness).

3.3. Konstituen

Mencakup semua Unit Organisasi dan Unit Kerja/Balai di lingkungan Kementerian Pekerjaan Umum

3.4. Sponsorship dan/atau Afiliasi

Pendanaan TTIS-PU bersumber dari Pusat Data dan Teknologi Informasi (Pusdatin) Kementerian Pekerjaan Umum.

3.5. Otoritas

TTIS-PU memiliki kewenangan secara administratif dengan konstituennya dalam penanganan gangguan keamanan informasi.

4. Kebijakan – Kebijakan

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

TTIS-PU melayani penanganan insiden siber dengan jenis berikut :

a. *Web Defacement;*
b. DDOS;
c. Malware;
d. Phishing;

Dukungan penuh diberikan oleh TTIS-PU kepada konstituen dapat bervariasi dan bergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Otentikasi

Komunikasi dapat dilakukan melalui alamat email dan telepon.

5. Layanan

5.1. Layanan Utama (reactive services)

Layanan utama dari TTIS-PU yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber (*alert and warning*)

Memberikan laporan dan informasi ke konstituen yang berada di lingkungan Kementerian Pekerjaan Umum terkait insiden yang terjadi serta ancaman dan/atau serangan siber. Pemberian peringatan ini berdasarkan skala insiden yakni, tingkat keparahan dan/atau kerentanan yang ditemukan. Penanganan insiden ini dilakukan dengan beberapa tahapan. Tahapan ini meliputi Identifikasi, Investigasi, penghapusan dan pemulihan.

5.1.2. Penanganan Insiden Siber (*incident handling*)

Menerima laporan dan informasi dari konstituen dan/atau insiden siber yang terjadi di lingkungan Kementerian Pekerjaan Umum . Menganalisa insiden siber yang terjadi serta menindaklanjuti hasil analisa insiden siber.

5.1.3. Penanganan Celah Keamanan (*vulnerability handling*)

Penanganan celah keamanan ini dengan cara mendeteksi dan menganalisa celah keamanan dengan *tools. Tools* ini secara default akan memberikan informasi terkait celah keamanan. Setelah mendapatkan informasi maka akan dilakukan *containment* dan *eradication*.

5.2. Layanan Tambahan (*proactive dan security quality management services*)

Layanan tambahan dari TTIS-PU yaitu :

5.2.1. Asesment Kerentanan (*Vulnerability Assessment*) atau Pentest

Melakukan asesmen kerentanan (VA) dan pentest secara periodik terhadap semua aplikasi. Hasil audit keamanan (VA) dan pentest akan dilaporkan ke konstituen.

5.2.2. Sosialisasi Security Awarenes

Sosialisasi terkait security awarenes ke konstituen dengan cara Bimtek, workshop dan blasting informasi.

5.2.3. Dokumen Teknis

Secara berkala Tim Monitoring meninjau hasil monitoring dan menerbitkan dokumen teknis jika terjadi anomali, secara berkala. Hasil dokumen ini dikirimkan ke konstituen untuk ditindak lanjuti.

5.2.4. Analisis Risiko Keamanan Siber

Ancaman kejahatan siber dan insiden siber mempunyai dampak yang berbeda beda terhadap target. Dampak ini harus di dibuatkan profil untuk

dianalisis dan menghasilkan identifikasi risiko, juga memberikan rekomendasi kontrol keamanan yang sesuai dengan risiko yang akan diturunkan. Kontrol keamanan yang direkomendasikan pada analisis risiko, selanjutnya akan dinilai kembali dari aspek efektivitas dan efisiensi dalam menurunkan setiap risiko, pada proses mitigasi risiko, sehingga proses ini akan memberikan dasar yang kuat dalam menentukan rencana keamanan informasi yang menyeluruh, efektif dan efisien.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke batin20@pu.go.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*

- TTIS-PU tidak bertanggung jawab atas kesalahan/kelalaian/kerusakan yang diakibatkan oleh penyalahgunaan informasi yang terkandung di dalam aset terdampak.
- TTIS-PU akan menjamin kerahasiaan pelapor aduan insiden siber.