RFC 2350 CSIRT-TGI

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 12 Nopember 2026.

1.2. Daftar Distribusi untuk Pemberitahuan

Internal.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://www.tgi.co.id/csirt/rfc2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen telah ditanda tangani oleh pihak yang berwenang di CSIRT-TGI menggunakan tanda tangan elektronik.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 CSIRT-TGI;
Versi : 1.0;
Tanggal Publikasi : 12 Nopember 2026;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Insident Response Team Transportasi Gas Indonesia
Disingkat : CSIRT-TGI.

2.2. Alamat

JB Tower, Lantai 21, Jl. Kebon Sirih Raya No. 48-50, Jakarta 10110, Indonesia.

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

+62 21-5085-2000

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

-

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

csirt[at]tgi [dot]co [dot]id

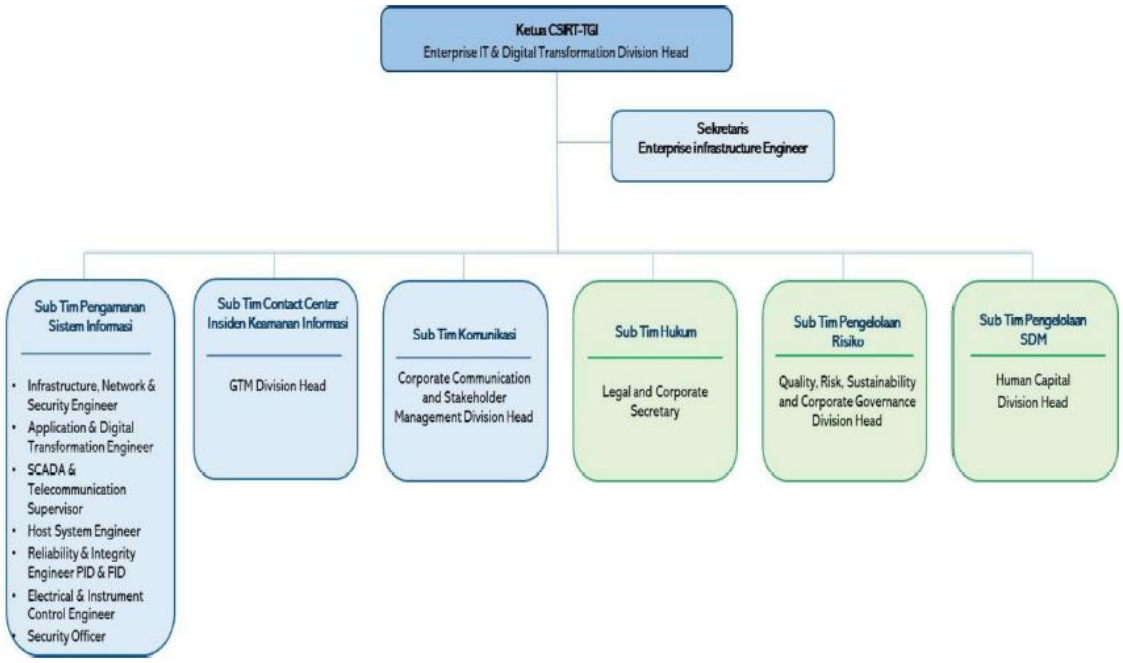
2.8. Kunci Publik (*Public Key*) dan Informasi/Data Enkripsi lain

Bits : -
ID : -
Key Fingerprint : -

File PGP *key* ini tersedia pada :

2.9. Anggota Tim

Anggota Tim CSIRT-TGI tertuang dalam struktur organisasi seperti pada gambar di bawah ini.



2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak CSIRT-TGI

Metode yang disarankan untuk menghubungi CSIRT-TGI adalah melalui *e-mail* pada alamat csirt@tgi.co.id atau melalui nomor telepon +62 21-5085-2000 ke CSIRT-TGI pada hari kerja jam 07.30 - 16.00 atau siaga selama 24/7.

3. Mengenai CSIRT-TGI

3.1. Visi

Visi CSIRT-TGI adalah menjadi tim tanggap insiden siber yang andal dalam melindungi sistem teknologi informasi dan teknologi operasional PT Transportasi Gas Indonesia untuk menjamin keamanan, keandalan, dan keberlangsungan operasi transmisi gas.

3.2. Misi

Misi dari CSIRT-TGI, yaitu :

a. Melindungi aset informasi, sistem IT, dan sistem OT/SCADA dari ancaman siber melalui pemantauan, pengendalian, dan penanganan insiden yang berkesinambungan.
b. Meningkatkan kesiapsiagaan organisasi terhadap ancaman siber melalui pengembangan prosedur, simulasi, pelatihan, dan program peningkatan kesadaran keamanan informasi.
c. Membangun koordinasi yang efektif dengan unit kerja internal, pihak eksternal dan pihak terkait lainnya dalam penanganan insiden siber.

3.3. Konstituen

Konstituen CSIRT-TGI meliputi Seluruh pengguna pengguna sistem elektronik di lingkungan PT. Transportasi Gas Indonesia baik internal yang meliputi seluruh direktorat dan juga eksternal yang terdampak oleh layanan TIK perusahaan.

3.4. Sponsorship dan/atau Afiliasi

CSIRT-TGI merupakan bagian dari PT. Transportasi Gas Indonesia sehingga seluruh pendanaan CSIRT-TGI bersumber dari anggaran yang ada di PT. Transportasi Gas Indonesia

3.5. Otoritas

CSIRT-TGI memiliki kewenangan secara administratif dengan konsituennya dalam penanganan insiden siber.

4. Kebijakan – Kebijakan

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

CSIRT-TGI melayani penanganan berbagai insiden siber yang terjadi atau mengancam konstituennya, termasuk tapi tidak terbatas pada :

a. Web Defacement;

b. DDOS;
c. Malware;
d. Phishing;

Dukungan yang diberikan oleh CSIRT-TGI kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, CSIRT-TGI dapat menggunakan alamat e-mail dan telepon.

5. Layanan

5.1. Layanan Utama

Layanan utama dari CSIRT-TGI yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik terkait layanan.

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 CSIRT-TGI yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan yang bertujuan untuk mengidentifikasi, menganalisis, mengoordinasikan, dan memantau penyelesaian kerawanan pada sistem elektronik yang digunakan PT. Transportasi Gas Indonesia.

5.2.2. Penanganan Artefak Digital

Layanan ini berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi dengan memberikan informasi statistik terkait layanan di lingkungan PT. Transportasi Gas Indonesia.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan pemberitahuan hasil pengamatan potensi ancaman yang dimiliki CSIRT-TGI yang ditujukan kepada seluruh user dan pihak eksternal yang ada kaitannya dengan PT. Transportasi Gas Indonesia sebagai pengguna layanan teknologi informasi.

5.2.4. Pendeteksian Serangan

Layanan pendeteksian serangan melalui monitoring pusat operasi keamanan siber yang dimiliki PT. Transportasi Gas Indonesia.

5.2.5. Penanganan Insiden Siber

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

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

5.2.6. Analisis Risiko Keamanan Siber

Layanan analisis risiko keamanan siber dilakukan oleh CSIRT-TGI menggunakan berbagai sumber data yang dimiliki oleh CSIRT-TGI.

5.2.7. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan yang memberikan pendampingan, rekomendasi, dan asistensi kepada konstituen di lingkungan PT Transportasi Gas Indonesia dalam meningkatkan kemampuan organisasi untuk mendeteksi, merespons, memulihkan, dan mengelola insiden siber secara efektif dan terkoordinasi.

5.2.8. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Pembangunan Security Awareness bertujuan agar semua konstituen memahami pentingnya keamanan informasi dan tanggung jawab mereka terkait keamanan informasi.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@tgi.co.id dengan melampirkan sekurang-kurangnya :

a. Identitas berupa Nomor Induk Pegawai (NIP), dan Jabatan
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan

7. Disclaimer

Ruang lingkup layanan CSIRT-TGI sesuai dengan konstituen yang ada.