RFC 2350 PGE-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 27 Agustus 2024

1.2. Daftar Distribusi untuk Pemberitahuan

Pembaharuan dokumen RFC 2350 akan diinformasikan kepada pihak – pihak berikut:

- General Manager
- Human Capital and Services Manager
- Seluruh konstituen PT PGE

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://pge.id/csirt/

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 PGE-CSIRT
Versi	: 1.0
Tanggal Publikasi	: 27 Agustus 2024
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan

2. Informasi Data/Kontak

2.1. Nama Tim

PT Pema Global Energi Computer Security incident Response Team
Disingkat : PGE-CSIRT

2.2. Alamat

Kantor Pusat

PT Pema Global Energi
Jl. Jend Sudirman No 59 Geuceu Inem, Banda Aceh
Aceh 23243, Indonesia
Telp (0645) 8089000 Ext 3333

Kantor Lapangan
PT Pema Global Energi
Aceh Production Operations
Point A, Nibong 24385 Telp (0645) 8011801 Ext 3333

Zona Waktu
Banda Aceh (GMT+07:00)

2.3. Nomor Telepon

(0651) 808 9000 Ext 3333
(0645) 8911801 Ext 3333

2.4. Nomor Fax

Tidak ada

2.5. Telekomunikasi Lain

Tidak ada

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

csirt@pge.id

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

Bits : 4096
ID : 3A20B7DDB26DDA69
Key Fingerprint : 9FFE577F8CBC6BE940A6C4C33A20B7DDB26DDA69

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

mQINBGafYGsBEADTKJ1z13T6QmkP8PhkS9ssJ/SCXwrNwWRltk60FxqFACa5T
G1o
nnzLqBWEeIkOEObgxBLrpTfo9XeCTiJgL6urAXuRJ+uxz+bbSiyddgzaI8gQLZhz
nRNfHZmJ5KnKd/O14zdoWEVT3jtuxqcPtzr7/mecQgoEsKiYrhhRPLJvfcqWtfxE
buHCPfHYtbpTcp2cBC7NmtvJi9a3wXxJRHXawmPAvSO5KM9LxP0p3Kek6U+LfT
XH
LdvSZCj+zUINnbOWo1lzdJZDubzY9237cR0mQ8tB0Ida93DLc13wRc/qY5eyM38I
6opokEIGhUeU9DOQmHUoDI96vIhEisS166lbSM4snm6HBTCS8rx76jO1EX8xNTkf
GERLoffT9dhKdTonBQVOohVfChg89uAoKUEjK4IAKHeh8xkuBrRdgaojeHjVamoW
TSpTxQvU2FXx2N5jkDikpdEghBZvNFj1wHVYGNQ1u8NJZnBNAmV970dwlAT4LN
Zl
EUNkaXH7r8CE5/S5w+jW2ue8vyo/ElhPdjWAJENxV49hWuKmnP1zAKmW66mX6
DYz
PXXqJ8go4DhpbU6El5CVc4kY5UHJgkYZzP5r2WV3G4rfGSCXABe9iUjm7dw0yKu
4

ZrmicJwLcSpxj/KLDKo3tT6HW2cfhnpeBjCElMKT3Yq2lZEojUGzWMIxrQARAQAB
tBhQR0UgQ1NJUlQgPGNzaXJ0QHBnZS5pZD6JAlcEEwEIAEEWIQSf/ld/jLxr6UC
m
xMM6ILfdsm3aaQUCZp9gawIbLwUJBaNy5QULCQgHAgIiAgYVCgkICwIEFgIDAQI
e
BwIXgAAKCRA6ILfdsm3aac6QEACJaubt8BYP9DSGKz87pP4UOlbw+8fB3RMSEzd
9
IKXuDosOOrD95O05hO+/qDqhNSJRRc/GWP2VEd3XMbIkz10CFzRc8U6CbdqewSi
9
3BXKxyLElrVrCDqHvJCMo8olajTIDsGyUwCqekiZVTQ1Fe7g9D54I2YqBUqh5X8U
f5hzFuFblP+JEHgk8K/pBg1vy29JmyK4CSYcXS8BNCuTnH5bDQvvhV79IVdI74Sm
aM2LY0ftgXN4J/yBXkrMHH5de3aHCtnzIaHIe4zSyivmzVKJEr1zuHZ8+2TbBijT
eYPajfS9kPmOnww4cXZ+cEKLvgbG9pp/jojaeQGF9ucbBrrn92q0Svsnf5S3oohj
Lq1zMyLWC4xt7LK+ccPrFpY3BkbllPS1sEPYej671jw85WuYfLNthFSwRyOcP8wI
cx6dzw/ieA23eeqRf5+6VrS6Da1pAkYqATEuutHruQBim0iWKYWFLvamea3foNB7
9GIlZ5BCMH3FpvdBErOyi+2FoUVLsMA+H86ek7x7EsHK3OyO1RTdUWgBSPcVJ
c//
F5p46oFTDO7eI7qPSBvREa24jV1SULueLYxy2wx1Ntt6ve5YvNXn9EwYpnxWHGJ
J
qAiTEK3eDLUzCK2282Cby9+DD/7xwWBoYRtKnTrYr8Tyl6kjVB187lNU95469lmb
Aq5d7w==
=iMEM
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://pge.id/csirt/

2.8. Anggota Tim

Ketua PGE-CSIRT adalah Zulfikar. Yang termasuk anggota tim adalah

- Zahril Manaf
- Feriza Rizki
- Silfiana
- Dea Hanindita
- M Rizki Wahyudi
- Riski Ramadana
- Teuku Fachrizal

2.9. Informasi/Data lain

Tidak ada

2.10. Catatan-catatan pada Kontak PGE-CSIRT

Metode yang disarankan untuk menghubungi PGE-CSIRT adalah melalui *e-mail* pada alamat csirt@pge.id atau melalui nomor telepon (0651) 808 9000 Ext 3333 dan (0645) 8011801 Ext 3333.

3. Mengenai PGE-CSIRT

3.1. Visi

Visi PGE-CSIRT adalah Membangun lingkungan PGE yang aman dari serangan siber yang mendukung pencapaian tujuan perusahaan.

3.2. Misi

Misi dari PGE-CSIRT yaitu :

Sebagai tim yang mengkoordinasikan sistem keamanan siber, yang mengoperasikan sistem mitigasi, manajemen krisis, pencegahan, penanggulangan serta pemulihan terhadap insiden keamanan siber pada lingkunagan PT Pema Global Energi. (PT PGE).
Membentuk tim yang handal dalam rangka penanggulangan dan pemulihan insiden siber di PT PGE
Menciptakan kemampuan dan kapasitas sumber daya penanggulangan dan pemulihan insiden siber di PT PGE.

3.3. Konstituen

Konstituen PGE-CSIRT meliputi : Unit kerja Head Office Banda Aceh dan Area Aceh Production Operation (APO)

3.4. Sponsorship dan/atau Afiliasi

Pendanaan PGE-CSIRT bersumber dari PGE HCS ICT

3.5. Otoritas

PGE-CSIRT memiliki kewenangan untuk melakukan penanganan insiden keamanan komputer di semua wilayah kerja PT PGE, termasuk tapi tidak terbatas:
• Mengambil langkah-langkah yang diperlukan untuk mengisolasi insiden seperti mematikan server, mengisolasi jaringan, menyita PC/Laptop yang dicurigai menjadi jalan masuk serangan, membatasi akses, dll.
• Mengambil langkah-langkah yang diperlukan untuk melakukan mitigasi insiden seperti memformat storage, melakukan konfigurasi ulang perangkat keras, melakukan pembersihan malware, merestore data, mencabut akses, dll.
• Bekerja sama dengan berbagai pihak dalam penanggulangan dan pemulihan insiden seperti bekerja sama dengan pihak ketiga penyedia layanan perangkat keras dan perangkat lunak, konsultan keamanan, BSSN, dll.
• Melakukan investigasi dan forensik insiden.
• Memberi laporan tentang insiden kepada pihak-pihak terkait termasuk yang diatur didalam peraturan pemerintah yang berlaku seperti pelaporan kepada Indonesia National CSIRT. Pelaporan insiden akan mengikuti proses pelaporan dalam penanganan emergensi dan krisis.

4. Kebijakan – Kebijakan

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

PGE CSIRT melayani penanganan insiden siber dengan jenis berikut :
a. Infeksi Malware.
b. Denial of Service.

c. Compromised Information.
d. Compromised Asset.
e. Peretasan Internal.
f. Peretasan External.
g. Surel (email)
h. Pelanggaran Kebijakan.
i. Aktivitas Ilegal.
j. Konsultas

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Kerjasama,interaksi dan pengungkapan informasi/data

4.3. Komunikasi dan Autentikasi

PGE-CSIRT akan melakukan kerja sama dengan semua pihak yang diperlukan dalam penanganan insiden keamanan komputer. Kerja sama tersebut dapat melibatkan pihak internal seperti Legal, HR, dan Relation team serta pihak external seperti BSSN, pihak ketiga penyedia perangkat keras dan lunak, konsultan keamanan, dll.

Dalam bekerja sama tersebut, PGE-CSIRT akan mengungkapkan data yang diperlukan untuk penanganan insiden seperti Log SIEM, Active Directory, Informasi tentang insiden, dll. Pengungkapan data dilakukan sebatas yang dibutuhkan dalam proses penanganan insiden.

PGE-CSIRT akan mengikuti semua ketentuan yang berlaku seperti kebijakan internal tentang data, dan semua peraturan yang berlaku. Pihak ketiga dan semua pihak diluar organisasi PGE-CSIRT akan diminta untuk menanda tangani “Non Disclosure Agreement (NDA)” sebelum mendapatkan berbagai data tersebut.

5. Layanan

5.1. Layanan Utama

Layanan utama dari PGE-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini melibatkan penyebarluasan informasi tentang serangan penyusup, kerentanan keamanan, virus komputer, atau hoax, dan memberikan saran tindakan jangka pendek untuk menangani masalah yang timbul

5.1.2. Penanganan Insiden Siber

Dalam berkomunikasi dan melakukan autentikasi, PGE CSIRT akan menggunakan standar komunikasi dan autentikasi yang telah ditetapkan oleh perusahaan (standar media, enkripsi, kebijakan password, dan lain-lain).

5.2. Layanan Tambahan

Layanan tambahan dari PGE-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan reaktif dirancang untuk merespon permintaan bantuan, laporan insiden dari konstituen PGE-CSIRT, dan segala ancaman atau serangan terhadap sistem PGE-CSIRT:

Menerima informasi dan laporan yang berkaitan dengan kerentanan pada perangkat keras dan lunak, menganalisis sifat, mekanisme, dan dampak dari kerentanan tersebut, serta merumuskan strategi tanggap untuk mendeteksi dan mengatasi kerentanan itu.

5.2.2. Penanganan Artefak Digital

Penanganan artefak digital Artefak adalah semua file atau objek yang ditemukan didalam sistem yang digunakan untuk melakukan serangan siber (misalnya virus komputer, worms, exploit script, dan toolkits).

Layanan ini melibatkan penerimaan informasi dan menduplikasi artefak, melakukan analisa sifat, cara kerja, versi dari artefak, fungsi artefak, dll, dan membuat rekomendasi untuk mendeteksi, menghilangkan, dan bertahan terhadap artefak tersebut

5.2.3. Pendeteksian Serangan

Melakukan analisa terhadap log Intrusion Detection System (IDS) dan log-lainnya dan memberikan respons terhadap event security yang memenuhi threshold tertentu

5.2.4. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Melakukan training keamanan dan membuat berbagai program untuk meningkatkan kesadaran dan kepedulian konstituen terhadap keamanan siber.Serta akan melakukan penanggulan dan pemulihan keamanan siber dengan berbagai aspek manajemen insiden keamanan siber.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@pge.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*

Tidak ada

Act General Manager
PT PEMA GLOBAL ENERGI

Wiendra Akhmad Faridsyah