RFC 2350
CYBER SECURITY INCIDENT RESPONSE TEAM (CSIRT)
PERTAMINA SUBHOLDING UPSTREAM (PERTAMINA SHU-CSIRT)

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi RFC 2350 Pertamina SHU-CSIRT berdasarkan RFC 2350. Diantaranya berisi informasi dasar mengenai Pertamina SHU-CSIRT, tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi Pertamina SHU-CSIRT.

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 1 Maret 2024.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Versi terbaru dari dokumen ini selalu dapat ditemukan dan tersedia di:
https://phe.pertamina.com/en/page/csirt-id (versi Bahasa Indonesia)
https://phe.pertamina.com/en/page/csirt-en (versi Bahasa Inggris)

1.4. Keaslian Dokumen

Dokumen ini telah ditanda tangani dengan PGP Key milik Pertamina SHU-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 Pertamina SHU-CSIRT (Pertamina SHU CSIRT);
Versi	: 1.1;
Tanggal Publikasi	: 1 Maret 2024;
Kedaluwarsa	: 21 Juni 2035 ataupun valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Pertamina Subholding Upstream - Computer Security Incident Response Team.
Disingkat : Pertamina SHU-CSIRT.

2.2. Alamat

PHE Tower
Jl. TB Simatupang Kav. 99
Jakarta Selatan 12520.

2.3. Zona Waktu

Jakarta (GMT+07:00).

2.4. Nomor Telepon

+62 21 29547000

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

-

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

Mohon kirimkan laporan insiden keamanan informasi ke csirt.shupstream@pertamina.com

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

Pertamina SHU-CSIRT menggunakan kunci penandatanganan untuk tujuan operasional. Harap enkripsi email sensitif dengan kunci publik Pertamina SHU-CSIRT dan kirim ke csirt.shupstream@pertamina.com

Kunci PGP Pertamina SHU-CSIRT adalah:
Bits : 4,096
ID : 0x4AE0218C
Key Fingerprint : 209920745FD989C4B58D39680F64A2234AE0218C

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQGNBGZ1I/8BDADPwAOgCwG+MZk8+NA15svcQD1eQjfyO9AF4lAj1SvGSZRNnKp7
oMd3WOZXDGQDVrQajuOkYqyY9iQtzmWxAwDW/xPM6E5MCKOlrnAbEtu2DqJl1E11
woflC2meHJpIoi4xF7QdAB6ke9TbNv/QTrAjmxY5/AbzN3WRGc2ZzsS9rNwORBME
wCx7c6HgPNpKAQYVwXpOWBDCtrOOGGvG2pX5Ocb9/JZy7DPOWklVBY4d6Y67Ppml
ddAs61iNXiVvmOhAsqlcIfF7s7P4Q5ZeW2EvPGAUPDm6JT8q+H//BAoKekKcepJN
S/aU8L5pJb8k4JnUIwGylPqJzNI9hlLmH235AG+IOyW3+yB951sc2qjZA25xf522
HWBGlLxxOFu/B400whZM8pqILcxS9cZnqSfAWptS5F/vr+tAyp2L27RxUydgcLK1
taaKqDcQbKvDnN547D3Rp5cItK4233hXu/7nWjQBe/mywEB3gXdokWy515fWriRY
V2SyfnqdvFkh7z8AEQEAAbREQ1NJUlQgUGVydGFtaW5hIFN1YmhvbGRpbmcgVXBz
dHJlYW0gPGNzaXJ0LnNodXBzdHJlYW1AcGVydGFtaW5hLmNvbT6JAdcEEwEIAEEW
IQQgmSB0X9mJxLWNOWgPZKIjSuAhjAUCZnUj/wIbAwUJFK++UQULCQgHAgIiAgYV
CgkICwIEFgIDAQIeBwIXgAAKCRAPZKIjSuAhjOc0DACjrYyqoyqbr01l3Fg/H6ry
Q6w0GaNnVvZUaYixRbMa9MfzZdtImp6Ic1GR0surDn14evv3D6c3G/Pmv1cbVeeX
uYcVc5yrxi7vgDWiTJ0vvduthh65wvkjPbXXqytxbLau8S0ZNz13/7E/JUgPMEsc
NWRSmr7/Od6LH3rEZCqCOet3kNVR7hPpOMOJeB/ecmL1NpGx50RR7c2runHmKo6x
2F1Xez1bmgGmy+6/kXvitNxbWlLoAlcG0qJgYIKRJQfzD2pVsua0EAaljMQzrZvL
2gPo0bJUN7vrhC8pGbA5lrjBLtZ+eGa+FK99dbnyhkokGeBJNY4bxOs7PJ9pjzYh
ngivV9hPnqLtQPb2hpmbR9ctklpYEbekAKrcfDbsZZJHPNX8AKPHG8f3LHYt90TW
1ZaXhIxgQz4FQr8IVQNCy69b+p3KEOQiAIL0k8orp+VTOPSlhcD9j/NhyJSLTH9O
fbtmkInt66ndJhDRnCipn9HVITn+Ol5DL85KSXccCBi5Ag0EZnUj/wEQAM8A1VPZ
gRXI64BOj1o6kM1eeAjp7khSeCrlj4ANiUAPnnzuIYmVBMjv8Yq18TilSKEFCh2k
5mQQl9tTk8hc6NqqadYa8t2KgIUqX1U7u2BW8pHeI0OU6Jf/sTXG5BYB2o2xehZb
33Z1zQJxHY5XI3O26eL6K/R5vCMWEcjqMXvjFUBG2JdOG3YQxNkO9+NZLzozEEEA
0OJB4NNb/9vAi3DW1BqvIoKz6u/dBLHOP7k43WsykwnPoQ1n82HJXJjCDMD1k+FS
PN0wqk3zgPzwAVNZ1PHZYbt0Z3+oytsi9dhkzj0ufeDs1cWS0YbCKv7UCy8xsa+W
jG0xEfRi3c3SbjHToq6OKf6Sj68SAcfhJxA6KNldn1gGaYyDVqqoJfUjlFx1/r3c

VuVf1+38NV51lXoSf2qmOdA+7RStmKTCNhUP7nU+lHHX3UO9EMrEB5xoLqJlk0F4
UoNpgvwH2Zy7l4ZmoEPEf8Xw7EYPZd9o3XyhbgZ1Den54nQyKLjfYG8fLVy/tV3Z
osRJQm9L7rlaYJy531KTXa8BEJTGrP6GijTR3wwJmc51IIGJt1BleGPM7lY3AP+D
nSwEh0eyBpdfobHOjxu0z2SbwOXgg+oAwoaqCjmCsilmVd+Xb3q9KWKowUBy27lb
7F103Z545SW9gRjNjBBs24jWqWDlMnhh8DvlABEBAAGJAbwEGAEIACYWIQQgmSB0
X9mJxLWNOWgPZKIjSuAhjAUCZnUj/wIbDAUJFK++UQAKCRAPZKIjSuAhjB13DADO
yBxRVtuGTZHRDaVUUWzZX3+jzXeQcdFSWZwHkqLUKc9zU19vcLUuIY4ywDZeTa5E
MU2kQFkd2glJz4dRIxU4HBLKMFj2p6kjrzvN7wh1YdilMyF2ulsxxGPw0GhGXDfi
eseBYhKeCJye7yTqS4AE4zkajOs41mlfETpXqRl0dpztyP3HShpyjNXEX3GY6m81
bBGAa0+Suer2HMX4+BmxYwX8jG6dcv449C/kCbw8M0wjQ3UwUst6q9WMVKksceix
NOHlxLe+xMkyYtKz5GMHKZ8eLIlpq9Ld8VTgbCyVEdqPwiTkAnLtRmka0va9rst8
azF3DYcC0zRT7yYrnLzT5NLNTh3HabZ0YcNnbLX2OBG8N1wN0emil7674p04YqeJ
eJPJU4agCjB9XB905jBxF9QbGOsMNZdAwNOAvpRBx2/+rg/BxhBxVbK+H62BLhHu
sDefpbTxjydxDvj9mwuNp8FlTVGbKGLNznX799bo+d7+jJj4grTlJN52P0yAp8c=
=qaUF
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://phe.pertamina.com/uploads/2025/10/287cf178-b9a2-46a3-bd42-293224ff92a7.txt

2.9. Anggota Tim

Ketua/Koordinator Pertamina SHU-CSIRT adalah Pejabat Sr. Manager IT Operation Pertamina Subholding Upstream. Yang termasuk anggota tim adalah seluruh fungsi Information Technology di lingkungan Group Bisnis Hulu Pertamina (Subholding Upstream Group) baik di Kantor Pusat maupun di Regional, Anak Perusahaan dan Afiliasi yang tertuang dalam dokumen Surat Perintah Pertamina SHU-CSIRT.

2.10. Informasi/Data lain

Informasi lebih lanjut mengenai Pertamina SHU-CSIRT dapat dilihat di:
https://phe.pertamina.com/en/page/csirt-id (versi Bahasa Indonesia)
https://phe.pertamina.com/en/page/csirt-id (versi Bahasa Inggris)

2.11. Catatan-catatan pada Kontak Pertamina SHU-CSIRT

Metode yang dipilih untuk menghubungi Perintah Pertamina SHU-CSIRT adalah melalui e-mail. Untuk laporan insiden dan masalah terkait keamanan informasi, silakan langsung menghubungi melalui email ke csirt.shupstream@pertamina.com

3. Mengenai Pertamina SHU-CSIRT

3.1. Visi

Visi Pertamina SHU-CSIRT adalah untuk merespon/mengatasi insiden siber di lingkungan Group Bisnis Hulu Pertamina (Subholding Upstream Group) secara efektif, mengurangi kemungkinan keberhasilan serangan serta menurunkan risiko dampak kerusakan yang ditimbulkan guna memulihkan operasional sistem informasi di lingkungan Group Bisnis Hulu Pertamina (Subholding Upstream Group).

3.2. Misi

Misi dari Pertamina SHU-CSIRT, yaitu :

a. Melaksanakan pengelolaan pengamanan sistem informasi dan pencegahan insiden keamanan sistem informasi atau siber sesuai dengan Pedoman keamanan informasi yang meliputi manajemen risiko, sistem monitoring, sistem penanggulangan dan pemulihan insiden keamanan siber;
b. Meningkatkan kompetensi dan kapasitas sumber daya penanggulangan dan pemulihan keamanan siber di lingkungan Group Bisnis Hulu Pertamina (Subholding Upstream Group).
c. Mengomunikasikan pentingnya kesadaran menjaga keamanan siber di lingkungan Group Bisnis Hulu Pertamina (Subholding Upstream Group).
d. Menyediakan layanan dan dukungan kepada konstituen tertentu dan pihak terkait dalam hal mencegah, menangani, dan/atau menanggapi insiden keamanan sistem informasi/siber yang terjadi di lingkungan Group Bisnis Hulu Pertamina (Subholding Upstream Group).

3.3. Konstituen

Konstituen **Pertamina SHU-CSIRT** meliputi seluruh stakeholder meliputi pekerja, mitra kerja direksi di lingkungan Group Bisnis Hulu Pertamina (Subholding Upstream Group) baik yang berada di Kantor Pusat PHE maupun di Kantor Pusat Regional, Zone, Site, Field, Wilayah Kerja, Anak Perusahaan (AP) dan Afiliasi yang terdiri dari:

1. Stakeholder/shareholder utama : PT Pertamina (Persero)
2. BOD/BOC PT Pertamina Hulu Energi & Subholding Upstream Group
3. Pekerja & Mitra Kerja di Lingkungan Subholding Upstream Group
4. Fungsi Information Technology, Direktorat SDM & Penunjang Bisnis, Pertamina Hulu Energi
5. Fungsi Information Technology Regional/Anak Perusahaan/Afiliasi yang terkait dengan organisasi CSIRT Subholding Upstream Group
6. PT Pertamina Hulu Energi sebagai *Lead* Subholding Upstream Group
7. Entitas Anak Perusahaan Subholding Upstream Group:
    a. PT Pertamina Hulu Rokan (Regional 1)
    b. PT Pertamina EP (Regional 2)
    c. Pertamina Hulu Indonesia (Regional 3)
    d. Pertamina EP Cepu (Regional 4)
    e. Pertamina Internasional EP (Regional 5)
8. Entitas Afiliasi Subholding Upstream Group:
    a. PT Pertamina Drilling Services Indonesia (PDSI)
    b. PT Badak NGL
    c. PT Elnusa Tbk
9. Badan Siber & Sandi Negara, Kementerian BUMN, SKK Migas, dan IDSIRTII/CC sebagai National CSIRT Indonesia.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan Pertamina SHU-CSIRT bersumber dari anggaran PT. Pertamina Hulu Energi (PHE).

3.5. Otoritas

Pertamina SHU-CSIRT merespon dan melaksanakan penanganan secara teknis terhadap insiden keamanan siber yang terjadi di lingkungan Group Bisnis Hulu Pertamina (Subholding Upstream Group).

4. Kebijakan – Kebijakan

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

Pertamina SHU-CSIRT berwenang untuk menangani segala jenis insiden keamanan siber yang terjadi atau mengancam konstituen kami (lihat bagian 3.3 Konstituen) dan kepentingan strategis siber, yang memerlukan koordinasi lintas organisasi, terutama di tingkat korporasi. Kami akan memberlakukan tindakan pencegahan apa pun yang diperlukan dan berkomitmen untuk memberi informasi kepada konstituen kami tentang potensi kerentanan apa pun. Perhatian khusus akan diberikan pada isu-isu yang secara langsung mempengaruhi infrastruktur kritis.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Pertamina SHU-CSIRT akan bekerjasama dengan organisasi lain di bidang keamanan siber dan infrastruktur Internet. Keterlibatan tersebut sering membutuhkan pertukaran data atau informasi mengenai insiden dan masalah. Namun demikian Pertamina SHU-CSIRT berkomitmen untuk melindungi privasi para konstituennya dan oleh karena itu (dalam keadaan normal) hanya menyampaikan informasi terbatas dan anonim kepada pihak lain, kecuali beberapa perjanjian kontrak berlaku, misalnya Non Disclosure Agreement (NDA) atau Pernyataan Kerahasiaan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, yang tidak mengandung informasi sensitif, CIRT Pertamina akan menggunakan metode konvensional seperti e-mail yang tidak terenkripsi. Untuk komunikasi yang aman, email atau telepon terenkripsi PGP akan digunakan. Jika perlu untuk mengautentikasi seseorang sebelum berkomunikasi, ini dapat dilakukan baik melalui rekan kepercayaan yang ada atau bahkan pertemuan tatap muka jika perlu .

5. Layanan

5.1. Layanan Utama

Layanan utama dari Pertamina SHU-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini merupakan layanan teknis untuk *monitoring* keamanan infrastruktur TI, pengamanan infrastruktur TI dan menyediakan dukungan perangkat pengamanan komputer bagi konstituen apabila diperlukan guna mencegah terjadinya insiden siber.

5.1.2. Penanganan Insiden Siber

Layanan ini merupakan layanan teknis terkait penanganan insiden yang terjadi pada konstituen yang meliputi koordinasi, analisis, rekomendasi teknis, dan bantuan *on-site*, agar sebuah insiden segera diremediasi dan tidak terulang kembali.

5.2. Layanan Tambahan

Layanan tambahan dari Pertamina SHU-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini meliputi koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (*hardening*) dalam konstituen Pertamina SHU-CSIRT.

5.2.2. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Menganalisa informasi yang diperoleh dari pemantauan untuk mengidentifikasi ancaman potensial yang dapat berdampak pada perusahaan. Analisis ini melibatkan pemahaman mendalam tentang sifat ancaman, teknik penyerangan, dan kelompok penyerang yang mungkin terlibat, serta pemberitahuan kepada pihak terkait di dalam perusahaan termasuk memberikan rekomendasi untuk mengurangi risiko.

5.2.3. Pendeteksian Serangan

Menganalisa data untuk mendeteksi adanya serangan terhadap sistem elektronik ataupun aktivitas yang mencurigakan terhadap sistem elektronik atau pelanggaran terhadap kebijakan/pedoman keamanan informasi.

5.2.4. Analisis Risiko Keamanan Siber

Mengidentifikasi dan menilai risiko keamanan siber serta merekomendasikan tindak lanjut untuk menghadapi risiko tersebut.

5.2.5. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Memberikan wawasan, pemahaman, dan cara yang perlu dilaksanakan dalam rangka membantu penanganan insiden siber.

5.2.6. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini berupa penyampaian informasi kepada konstituen secara berkala tentang keamanan teknologi informasi sehingga kesadaran dan kepedulian terhadap isu keamanan tersebut dapat meningkat.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt.shupstream@pertamina.com dengan melampirkan sekurang-kurangnya:

1. Jika dari eksternal Perusahaan:
   a. Foto/*scan* kartu identitas.
   b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan.
   c. Apabila dihubungi bersedia memberikan data-data terkait kebutuhan penyelesaian insiden.
   d. Atau sesuai dengan ketentuan lain yang berlaku.
2. Jika dari internal Perusahaan:
   a. Alamat *e-mail* Perusahaan.
   b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan.

7. *Disclaimer*

Seluruh penanganan tergantung dari ketersediaan tools yang dimiliki Pertamina SHU-CSIRT memberikan respon terhadap pelaporan insiden pada jam kerja (07.00 WIB – 16.00 WIB) namun, terkait waktu penyelesaian insiden siber bervariasi sesuai dengan kondisi

situasional insiden yang dihadapi. Setiap tindakan pencegahan yang akan diambil dalam persiapan informasi, termasuk peringatan dan pemberitahuan, Pertamina SHU-CSIRT mengasumsikan tidak akan bertanggung jawab atas kesalahan, kelalaian atau kerusakan akibat penggunaan informasi yang terkandung di dalamnya. Informasi ini harus digunakan hanya seperti yang telah disebutkan.

PERTAMINA

CSIRT SH UPSTREAM

Ditandatangani menggunakan sertifikat elektronik dari BSrE