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

1. Information About Documents

This document contains a description of Pertamina SHU-CSIRT's RFC 2350 based on RFC 2350. Among them is basic information about Pertamina SHU-CSIRT, responsibilities, services provided, and how to contact Pertamina SHU-CSIRT.

1.1. Date of Last Update

The document is a version 1.0 document published on March 1, 2024.

1.2. Distribution List for Notifications

There is no distribution list for notification regarding document updates.

1.3. Locations where this Document can be obtained

The latest version of this document can always be found and available at:
https://phe.pertamina.com/en/page/csirt-id (Indonesian version)
https://phe.pertamina.com/en/page/csirt-en (English version)

1.4. Document Authenticity

This document has been signed with Pertamina's PGP Key SHU-CSIRT. For more clarity, see Subchapter 2.8.

1.5 Document Identification

Documents have attributes, namely:

Heading	: RFC 2350 Pertamina SHU-CSIRT (Pertamina SHU CSIRT);
Version	: 1.1;
Publication Date	: March 1, 2024;
Expired	: June 21, 2035 or valid until the latest document is published.

2. Contact Information

2.1. Team Name

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

2.2. Address

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

2.3. Time Zone

Jakarta (GMT+07:00).

2.4. Telephone Number

+62 21 29547000

2.5. Fax Number

-

2.6. Other Telecommunication

-

2.7. E-mail Address

Please send an information security incident report to csirt.shupstream@pertamina.com

2.8. Public *Key* and Encryption Information

Pertamina SHU-CSIRT uses signing keys for operational purposes. Please encrypt sensitive emails with Pertamina SHU-CSIRT public key and send them to csirt.shupstream@pertamina.com.

Pertamina SHU-CSIRT PGP keys are:
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
UoNpgvwH2Zy7I4ZmoEPEf8Xw7EYPZd9o3XyhbgZ1Den54nQyKLjfYG8fLVy/tV3Z

osRJQm9L7rlaYJy531KTXa8BEJTGrP6GijTR3wwJmc51IIGJt1BleGPM7lY3AP+D
nSwEh0eyBpdfobHOjxu0z2SbwOXgg+oAwoaqCjmCsilmVd+Xb3q9KWKowUBy27Ib
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* is available at:
https://phe.pertamina.com/uploads/2025/10/287cf178-b9a2-46a3-bd42-293224ff92a7.txt

2.9. Team Members

The Chairman/Coordinator of Pertamina SHU-CSIRT is the Sr. Manager IT Operation of Pertamina Subholding Upstream. Included in the team are all Information Technology functions within Pertamina's Upstream Business Group (Subholding Upstream Group) both at the Head Office and Regionally, Subsidiaries and Affiliates as stated in the Pertamina SHU-CSIRT Warrant document.

2.10. Other Information/Data

Further information about Pertamina SHU-CSIRT can be found at:
https://phe.pertamina.com/en/page/csirt-id (Indonesian version)
https://phe.pertamina.com/en/page/csirt-en (English version)

2.11. Notes on Pertamina SHU-CSIRT Contact

The chosen method to contact the Pertamina SHU-CSIRT Order is via e-mail. For reports of incidents and information security-related issues, please contact directly via email to csirt.shupstream@pertamina.com

3. About Pertamina SHU-CSIRT

3.1. Vision

Pertamina's vision for SHU-CSIRT is to effectively respond/overcome cyber incidents within the Pertamina Upstream Business Group (SH Upstream Group), reduce the likelihood of successful attacks, and reduce the risk of damage caused in order to restore information system operations within the Pertamina Upstream Business Group (SH Upstream Group).

3.2. Mission

The mission of Pertamina SHU-CSIRT, namely:

a. Carry out the management of information system security and prevention of information system or cyber security incidents in accordance with the Information Security Guidelines which include risk management, monitoring systems, cyber security incident response and recovery systems;
b. Increasing the competence and capacity of cybersecurity countermeasures and recovery resources within Pertamina's Upstream Business Group (Subholding Upstream Group).
c. Communicating the importance of awareness of maintaining cyber security within the Pertamina Upstream Business Group (Subholding Upstream Group).
d. Providing services and support to certain constituents and related parties in terms of preventing, handling, and/or responding to information/cyber system security incidents that occur within the Pertamina Upstream Business Group (Subholding Upstream Group).

3.3. Constituent

Pertamina SHU-CSIRT **constituents** include all stakeholders including workers, working partners of the board of directors within the Pertamina Upstream Business Group (Subholding Upstream Group) both at the PHE Head Office and at the Regional Head Office, Zone, Site, Field, Work Area, Subsidiary (AP) and Affiliates consisting of:

1. Main Stakeholder/Shareholder : PT Pertamina (Persero)
2. BOD/BOC PT Pertamina Hulu Energi & Subholding Upstream Group
3. Workers & Partners in the Upstream Subholding Group
4. Function of Information Technology, Directorate of Human Resources & Business Support, Pertamina Hulu Energi
5. Regional Information Technology Functions/Subsidiaries/Affiliates related to the CSIRT Subholding Upstream Group organization.
6. PT Pertamina Hulu Energi as Lead Subholding Upstream Group
7. Subsidiaries of Subholding Upstream Group:
   a. PT Pertamina Hulu Rokan (Regional 1)
   b. PT Pertamina EP (Regional 2)
   c. Pertamina Hulu Indonesia (Region 3)
   d. Pertamina EP Cepu (Region 4)
   e. Pertamina International EP (Region 5)
8. Affiliated Entities of Upstream Group Subholding:
   a. PT Pertamina Drilling Services Indonesia (PDSI)
   b. PT Badak NGL
   c. PT Elnusa Tbk
9. The State Cyber & Cryptography Agency, the Ministry of SOEs, SKK Migas, and IDSIRTII/CC as the National CSIRT of Indonesia.

3.4. Sponsorship and/or Affiliation

Pertamina SHU-CSIRT funding is sourced from the budget of PT. Pertamina Hulu Energi (PHE).

3.5. Authority

Pertamina SHU-CSIRT responded and carried out technical handling of cybersecurity incidents that occurred within Pertamina's Upstream Business Group (Subholding Upstream Group).

4. Policies

4.1. Types of Incidents and Support Levels/Levels

Pertamina SHU-CSIRT is authorized to handle any type of cybersecurity incident that occurs or threatens our constituents (see section 3.3 Constituents) and cyber strategic interests, which require cross-organizational coordination, especially at the corporate level. We will take any necessary precautions and are committed to keeping our constituents informed of any potential vulnerabilities. Particular attention will be paid to issues which directly affects critical infrastructure.

4.2. Cooperation, Interaction and Disclosure of Information/Data

Pertamina SHU-CSIRT will collaborate with other organizations in the field of cybersecurity and Internet infrastructure. Such involvement often requires the exchange of data or information regarding incidents and problems. However, Pertamina SHU-CSIRT is committed to protecting the privacy of its constituents and therefore (under normal circumstances) only conveys limited and anonymous information to other parties, unless some contractual agreements apply, such as Non-Disclosure Agreement (NDA) or Statement of Confidentiality.

4.3. Communication and Authentication

For ordinary communication, which does not contain sensitive information, Pertamina's SHU-CSIRT will use conventional methods such as unencrypted e-mail. For secure communication, PGP encrypted email or phone will be used. If it is necessary to authenticate someone before communicating, this can be done either through an existing peer of trust or even a face-to-face meeting if necessary.

5. Services

5.1. Main Services

The main services of Pertamina SHU-CSIRT are:

5.1.1. Giving Warnings Related to Cybersecurity

This service is a technical service for IT infrastructure security monitoring, IT infrastructure security and providing computer security device support for constituents when needed to prevent cyber incidents.

5.1.2. Cyber Incident Handling

This service is a technical service related to handling incidents that occur in constituents which includes coordination, analysis, technical recommendations, and on-site assistance, so that an incident is immediately remediated and does not recur.

5.2. Additional Services

Additional services from Pertamina SHU-CSIRT are:

5.2.1. Handling Electronic System Vulnerabilities

This service includes coordination, analysis, and technical recommendations in the context of strengthening security (hardening) in the constituents of Pertamina SHU-CSIRT.

5.2.2. Notification of Potential Threat Observations

Analyze the information obtained from monitoring to identify potential threats that can have an impact on the company. This analysis involves an in-depth understanding of the nature of the threat, attack techniques, and groups of attackers that may be involved, as well as notifying relevant parties within the company including providing recommendations to mitigate risks.

5.2.3. Cyber Attack Detection

Analyze data to detect attacks on electronic systems or suspicious activity against electronic systems or violations of information security policies/guidelines.

5.2.4. Cybersecurity Risk Analysis

Identify and assess cybersecurity risks and recommend follow-ups to address those risks.

5.2.5. Consultation on Readiness to Handle Cyber Incident

Providing insights, understanding, and ways that need to be implemented in order to help handle cyber incidents.

5.2.6. Building Awareness and Concern for Cyber Security

This service is in the form of regularly delivering information to constituents about information technology security so that awareness and concern for these security issues can increase.

6. Incident Reporting

Cybersecurity incident reports can be sent to csirt.shupstream@pertamina.com by attaching at least:

1. If from outside the Company:
   a. Photo/scan of ID card.
   b. Evidence of the incident in the form of photos or screenshots or log files found.
   c. If contacted, they are willing to provide data related to the need to resolve the incident.
   d. Or in accordance with other applicable provisions.
2. If from within the Company:
   a. The Company's *e-mail* address.
   b. Evidence of the incident in the form of photos or screenshots or log files found

7. *Disclaimer*

All handling depends on the availability of Pertamina SHU-CSIRT's tools to respond to incident reporting during working hours (07.00 WIB – 16.00 WIB), however, the time for resolving cyber incidents varies according to the situational conditions of the incident faced. Any precautions that will be taken in the preparation of information, including warnings and notifications, Pertamina SHU-CSIRT assumes that it will not be responsible for errors,

omissions, or damages resulting from the use of the information contained therein. This information should be used only as already mentioned.

PERTAMINA

CSIRT SH UPSTREAM

Ditandatangani menggunakan sertifikat elektronik dari BSrE