RFC 2350 BPS-CSIRT

1. Document Information

This document contains a description of the BPS-CSIRT based on RFC 2350, which is basic information about the BPS-CSIRT, explaining responsibilities, services provided, and how to contact the BPS-CSIRT.

1.1. Last Update

The current version is 2.0 and issued on December 16, 2024.

1.2. Distribution List for Notifications

There is no distribution list for document update notifications.

1.3. Location Where This Document May Be Found

This document is available at
https://csirt.bps.go.id/assets/rfc2350/rfc2350-en.pdf

1.4. Document Authenticity

This document have been signed with BPS-CSIRT's PGP Key. For more details can be seen in Section 2.8.

1.5 Identifikasi Dokumen

Documents have attributes, that is:

Title	: RFC 2350 BPS-CSIRT;
Version	: 2.0;
Publication Date	: December 16, 2024;
Expired	: This document is valid until the latest document is published.

2. Contact Information

2.1. Team Name

Badan Pusat Statistik - Computer Security Incident Response Team
Shortname : BPS - CSIRT.

2.2. Address

Badan Pusat Statistik Republik Indonesia
Jl. Dr. Soetomo No 6-8
Sawah Besar, Jakarta 10710

2.3. Time Zone

Jakarta (GMT+07:00)

2.4. Telephone Number

(021) 3863735

2.5. Fax Number

-

2.6. Other Telecommunications

(021) 3841195, (021) 3842508, (021) 3810291 Ext 3320

2.7. Email

csirt@bps.go.id

2.8. Public Keys and Data Encryption

PGP key file is available at: https://csirt.bps.go.id/assets/bps-csirt.asc

2.9. Team Members

The head of BPS-CSIRT is the Director of the Statistical Information System. Team members include Functional Officers at the Directorate of Statistical Information Systems.

2.10. Other Informations

-

2.11. Points of Customer Contact

The recommended method for contacting BPS-CSIRT is via e-mail at the address csirt[at]bps[dot]go[dot]id or via telephone number (021) 3863735 on weekdays at 08.00 - 16.00.

3. About BPS-CSIRT

3.1. Vision

The vision of BPS-CSIRT is to realize information security management in supporting safe and reliable BPS IT services.

3.2. Mission

The missions of BPS-CSIRT are:

1. Implementing information security management on BPS IT services and information assets.
2. Increasing the capacity of information security resources in the aspects of prevention, response and recovery of information security incidents.
3. Building awareness of IT service users towards information security.

3.3. Constituency

The BPS-CSIRT constituents include all users of information technology services within the BPS.

3.4. Sponsorship and/or Affiliation

BPS-CSIRT is part of the Directorate of Statistical Information Systems so that all funding comes from the APBN.

3.5. Authority

BPS-CSIRT has the authority with its constituents in handling cyber security disturbances. BPS-CSIRT can coordinate and cooperate with other organizations for incidents that cannot be handled.

4. Policies

4.1. Type of Incidents and Level of Support

BPS-CSIRT serves the following types of cyber incident handling:

a. Web Defacement
b. DDoS
c. Virus/Malware
d. Phising
e. Spamming
f. Others

The support provided by BPS-CSIRT to constituents may vary depending on the type and impact of the incident. Incident handling services based on constituent reports.

4.2. Cooperations, Interaction and Dislocure of Information

BPS-CSIRT will collaborate and share information with CSIRT or other organizations in the scope of cyber security. All information received by BPS-CSIRT will be kept confidential.

4.3. Communications and Authentications

For normal communication, BPS-CSIRT can use email without data encryption (conventional email) and telephone. However, for communications containing sensitive/restricted/confidential information, you can use PGP encryption on email.

5. Services

5.1. Main Service

The main services of BPS-CSIRT are:

5.1.1. Cyber Security Notifications

Providing notifications of cyber incidents to owners of electronic systems and information related to services.

5.1.2. Cyber Incidents Handling

This service is in the form of coordination, analysis, technical recommendations, and on-site assistance in the context of cyber incident response and recovery.

5.2. Additional Services

The additional services of BPS-CSIRT are:

5.2.1. Handling Electronic System Vulnerabilities

This service is in the form of coordination, analysis, and technical recommendations regarding the findings of vulnerabilities in certain electronic systems in order to strengthen security (hardening).

5.2.2. Digital Artifact Handling

This service is in the form of handling artifacts in the context of recovering affected electronic systems or supporting investigations.

5.2.3. Notification of Observation Results of Potential Threats

This service is in the form of notification regarding the results of monitoring activities for potential threats to an information technology asset.

5.2.4. Attack Detection

This service is in the form of monitoring results of anomalous cyber activities in order to detect cyber attacks on information technology assets..

5.2.5. Cybersecurity Risk Analysis

This service is in the form of identification of vulnerabilities and risk assessment of vulnerabilities found. Furthermore, recommendations are given that can be done to reduce these risks.

5.2.6. Cybersecurity Awareness

Socialization and guidance to all employees within BPS, which aims to increase employee awareness and concern about cybersecurity.

6. Incident Report

Cybersecurity incident can be reported through the HALOSIS ticketing system at https://halosis.bps.go.id or via email csirt@bps.go.id by attaching an incident report document that at least contains a log file, timestamp, vulnerability findings, incident identification/analysis, reporter's name, and reporter's mobile phone number.

7. *Disclaimer*

- BPS-CSIRT only serves vulnerability analysis reports and security incidents that occur on official information technology assets.
- The scope of incident handling depends on the availability of tools owned by CSIRT-BPS.