

RFC 2350 PLN BATAM-CSIRT

1. Information Regarding Documents

This document contains a description of PLN BATAM-CSIRT based on RFC 2350, namely basic information about PLN BATAM-CSIRT, explaining responsibilities, services provided, and ways to contact PLN BATAM-CSIRT.

1.1. Last *Update* Date

The document is a version 1.0 document issued on May 5, 2023

1.2. Distribution List for Notices

There is no distribution list for notifications regarding document updates.

1.3. Location Documents can be obtained

This document is available at :

<https://csirt.plnbatam.com/rfc2350.pdf> (Indonesian version)

1.4. Document Authenticity

Both documents have been signed with the PGP Key belonging to PLN BATAM. For more details can be seen in Sub-chapter 2.8.

1.5 Document Identification

The document has attributes, namely:

Title	: RFC 2350 PLN BATAM-CSIRT; : 1.0;
Version	: 1.0;
Publication Date	: 2 May 2023;
Expired	: This document is valid until the latest document is published.

2. Data/Contact Information

2.1. Team Name

PLN BATAM-Cyber Security Incident Response Team (CSIRT)

Abbreviated: PLN BATAM-CSIRT.

2.2. Address

PT PLN Batam
Jl. Engku Putri No. 3
Batam Center
Batam – Riau Archipelago

2.3. Time Zone

Jakarta (GMT+07:00)

2.4. Phone number

0778 - 451415

2.5. Fax Number

There isn't any

2.6. Other Telecommunications

Mobile Phone: (+62) 821 3339 0808

2.7. Email Address (E-mail)

csirt[at]plnbatam.com

2.8. Public Key and other Encryption Information/Data

Bits : 4096
ID : D4CFA233

Key Fingerprint : 97A1 17D8 B3C8 5B10 C2CE 1A73 B03B F7AA D4CF A233

PGP Public Key Block For example:

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

```
xsFNBGRQ27sBEADGLSkdppp1/zBrRZzNB5LnJSKKcw+uZ9ToWXPfRGD8OfibLCt
fCX2+hJvOLA4TdZBjpl2uu2al+M4Oe2JsQ4Dyp4rrAyIWdM4wZXT x4xENxuNRlba
WoutDqRA5P9GtsY5PKafa0stn7iZWVtfra62NBQBks7HFNSc5hJsaFUZFBfsg+qr
JuiXbRakKX0GB+ppcaBwHQuHMopN249GplyinU5gcbinmK9UF4ugHywQbcBARxq8
OqllBFV4k4cnNjaVus+eY9F0y9PJxkPwbT+toEODYaLztFvXe9DHvZVI3aUs/08q4
QQaretRCsHfgtuzbLjKVtu0Ysnh3yTXjL6ZHuxJp7eNuQP7TQDU8vd2i8li+8zC7
7ctp72BWvTxJZPHsyxvLwMpawJ6K7eauVZe/YzB/hzTGDQgbnhSMx7W4kN4kU9V0
iMR9JW80s/9Q /mLeVTVebqGMYl0CwbaU4rfRd8CiCVpq7zShZ2WpQnwnk8P0z1Cm
deKWolKn8+AF9AjGuyhi0TYwYiWJMG3xmDGlpRmnPLVSSoxn0OG1R7Hib/DPqf3z
rF8mW37INSntSi5Dm01Zulvo35XzN/KeHHRW R1rodwK+P0Tzor/llgGJFckD+p0/
kc9G3OWRDP9FpK6K0svB3RBIGzwM59jwdmclAiY3xU3Ugzt5yhZhRerkAwARAQAB
zStQTE4gQmF0YW0gLSBDU0lSVCBUZWVtIDxjc2lydEBwbG5iYXRhb S5jb20+wsGU
BBMBCAA+FiEEI6EX2LPIWxDCzhpzsDv3qtTPojMFAmRQ27sCGwMFCQeGH1UFCwkl
BwlIGFQoJCAsCBBYCAwECHgECF4AACgkQsDv3qtTPojOvQg/+MNWReYkM+8y5ENEa
77QXzjh1TlxC9KGLpDRbUj2Sf2fR5JOVo8yKQ3se0Rg0IZVp31aaX0RT0ZyFGgS
AlhBXRyJAwjsO9JLw9Wejy1TJccaNr2kGYSfldGNyYkKHI3g8h9wdW4hrqf6v+ln
C1WeR/fPQR0/NRiqwxFP+jJDK58nQqXWhG1pH7KRKsN+W61aXCMPHGOUkmCIOB+7
W4yap2NPrq49Y/ijz9HN51QUZnlRYo9isTPe4uv4K+bcR9xyQa3JLf0Wju3OnfZw
W7zj4lQM2J6EA8vCqc/HI9aN+VfDFoRGkOHZR6torTUQTRRTlc+agcSku4Rqoy5p
dbyTZixrketqJMbHTv+23cZNxYLHjyrZe6UJcJVUj13LdHEnt9m1dMDZRhQxdB2P
O5Kcfa/JxRUtRCHVwJ+AJe5wYvgb8GSSCV7vVXN/xhDpzde9QbPYtLbFK3+7Glu7
8PMPwEuIDK5U3Cv1B7wyQp28qgdN9vfH32HBoflBPIJZgQBdxFVLIrV7jOZ+wXha
dLKZMXfDqvwFchVpBPfC/TUzMdjsiY31PDdtWGteL4eE4FujnNnU4OYr7qNHDvdv
c90aJB0 cUBEdtF5aMVRrRyyGQHD2fgdMq3EVygNB00/QlyZl7olAhMmghkddDI4q
SZDSWcS29eogd1MOS8xIG/r/JsXOWU0EZFDbuwEQANix1X+q3lITB7q8Fg6zGjvL
WoRbeK6u7b9sQGuiH5M6v2J3ggQUvtX9GyeKLZmn1Vv0X0WvjH9XOdBoC/Pq1tU/
5dnzucDPvJkvB+WxCX985SmGrH23zOw5YbTSMcJGYQ+cOxHKHzQ8ZJBnPremOTi0
NykfZK8a5HDGiubx2yiHvUFBdwQqj2lzj5KSt3PvOkbxysV/boh73qHknE0yGBja
sydAuWTfks63xj4RC+oqAjWki3T82SiJvcfzkeJynYrHVR2qew3gv1kP/3lg0F8Y
Rk40tZhYhaxXfV+Y0nJkvDx/1ju6bd26QkENc9cuyGZf+golxd4XASYlx9KNz+
```

iglLwyMbs1+UDSFxcaye+Ov3EUsmh1bVcWZzCU/hxqVlhh4GoxaDYSrh1tz00cPi
4VwklFJLTtruAJS8NRxKuRMfM9OMxOt23GWvYwh39wiX2KLhYZx1mYuHk8lvrBaL
wzSpxB74b3S4ryWDG83aoWSJffCcY9tGpV4VD1D1JCnr0SnCo8OXzY6xFZR4QRJD
7ok7K8OOUAtzffjU hvONjHvbKnUNvsLEzWYxzKNVLYeNfmkSQVT3v4anwmmT758U
MwGSW5J0taPa9Z72hiYDyedLMJ8kM+eUbujtkjAP0k//VrqHEbYCgyb2jW9lyDI
e+t4qAt9CRNhGfBn28bVABEBAAHCwXwEGAEIACYWIQsXoRfYs8hbEMLOGnOwO/eq
1M+iMwUCZFDbuwIbDAUJB4YfVQAKCRCwO/eq1M+iMybQD/9CWj1RzcvsEiZUqLH
aSycqKEmdgm0z4tjN6UDtlo4M6Q7hNyySIXy60N06vbf+w5IsKUCSOK3DFjPG1rQ
Zmfx1VmJHRaLfWn8zfSvZ/VSL098cvQBy8uESBdAR4We+IGSjm30IгнаML83DBtX
OLdjicighYTooyloC3WvnCJFwKGEkqxQFEQ1Ehue6h/5vZNEpR7YoyXq1lpEsuhlj
pDMgVBSz6BKAK2oYOMd9gdoqACMHqmxW4gWZar2Znb5mXaExsw9192ht5PGRX3G
yRfOZBMSDSJm9i/U 18Qj18aBzWNR2Znz5cFToQokgQcys7WW08yR56fjaEY3g5xv
BnheGHkmWn7c5POhaksITLUuT3i9kueERqIJyLdFGtbZegsMrJohsQa1rWiATqeV
D/6HJD4yFGE1CUWuhxyUaQ/d7pKRStVDCi1QuMuhD1gu2ypfxWdJJlgzhYIOzbBx
BBO68VcR+XT+GKn0YWNauV1UodOv7XEG7r6xoIO4lwsTapUR3wyfuPSeylpGZ/q
APVh/umlSc+auI/T8J8lqqiLKxfeZ4oMgo/z3QFU5w+j/X8TqbzDkdnnUjBCtnSz
JFUSzMiP8gmj61w2nP/N21m0Pr7hXDpeUFIJXEn6Jq9GSJQmsIN43B40Qyt5jQ4m
sQHhtznvVu7rG4u8rHC/X1tkqg==
=DPQ+
-----END PGP PUBLIC KEY BLOCK-----

This PGP key file is available at:

<https://csirt.plnbatam.com/publickey.asc>

2.9. Team Member

Team members consist of the Head of the CSIRT and several support teams that have been formed based on Decree Number 00013.K/DIRUT/2023 dated 28 April 2023

2.10. Other information/data

There isn't any

2.11. Notes on Contact PLN BATAM-CSIRT

The recommended method for contacting PLN BATAM-CSIRT is by *e-mail* at csirt@plnbatam.com or by telephone number (+62) 821 3339 0808 Every day for 24 hours (24/7)

3. Regarding PLN BATAM-CSIRT

3.1. Vision

The vision of PLN BATAM-CSIRT is the realization of cyber security/resilience within PT PLN Batam

3.2. Mission

- Coordinating, preventing and mitigating information security within PLN Batam internally and coordinating with other incident agencies in Indonesia,
- Building cooperation in the context of incident response and recovery cybersecurity within PLN Batam,
- Increase awareness of the importance of information security for human resources within PLN Batam.

3.3. Constituents

PLN BATAM-CSIRT constituents include:

- a. PLN Batam CSIRT constituents include users of electronic systems in the environment PLN Batam
- b. All customers who use electronic systems within PLN Batam

3.4. Sponsorship and/or Affiliation

PLN BATAM-CSIRT funding comes from PLN Batam Budget

3.5. Authority

PLN BATAM-CSIRT has the authority to deal with cybersecurity incidents against assets managed by PLN Batam. In carrying out prevention and recovery PLN Batam-CSIRT coordinates with constituents, BSSN or other parties for incidents that cannot be handled.

4. Policies – Policies

4.1. Incident Types and Levels of Support

PLN BATAM-CSIRT serves the handling of various cyber incidents that occur or threaten constituents, including but not limited to:

- a. *Web Defacement*
- b. *DDOS*
- c. *Malware*
- d. *Phishing*

Support provided by PLN BATAM-CSIRT to constituents may vary depending on the type and impact of the incident

4.2. Cooperation, Interaction and Disclosure of Information/data

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

4.3. Communication and Authentication

For ordinary communication, PLN BATAM-CSIRT can use e-mail and telephone addresses.

5. Service

5.1. Main Services

The main services from PLN BATAM-CSIRT are:

5.1.1. Giving Warning Regarding Cyber Security

This service is carried out in the form of giving warnings of cyber incidents to owners of electronic systems and statistical information related to services.

5.1.2. Cyber Incident Handling

This service is provided in the form of coordination, analysis, technical recommendations, and *on-site* assistance in the context of handling and recovering from cyber incidents.

5.2. Additional Services

Additional services from PLN BATAM-CSIRT namely:

5.2.1. Security Awareness and Concern Services

This service is in the form of *awareness* dissemination related to cyber security to related parties to increase user/people's understanding of the importance of cyber security and protection of data and information security.

5.2.2. Security Assessment Service

This service is in the form of vulnerability identification and risk assessment of the vulnerabilities found in the system. After that it will be reported to the owner of the system for handling.

5.2.3. Handling Electronic System Vulnerabilities

This service is provided in the form of coordination, analysis, and technical recommendations in order to strengthen security (*hardening*) of IT services. This service only applies if the following conditions are met:

- a. Reporters of vulnerabilities are owners of electronic systems. If the reporter is not the owner of the system, then his/her vulnerability report cannot be handled;
- b. Vulnerability handling services in question can also be follow-up on *Vulnerability Assessment activities*.

6. Incident Reporting

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

- a. Identity number can be a passport, driver's license, student card
- b. Incident evidence in the form of photos or *screenshots* or *log files* found
- c. Or in accordance with other applicable provisions

7. Disclaimer

PLN BATAM-CSIRT responds to incident reporting 1x24 hours. However, the time for solving cyber incidents varies according to situational conditions incident encountered.