RFC 2350 BSN-CSIRT

1. Information on Documents

This document contains a description of the BSN-CSIRT based on RFC 2350, which provides basic information about the BSN-CSIRT, describing its responsibilities, services provided, and how to contact the BSN-CSIRT.

1.1. Last Update Date

This is version 2.0 of the document and was published on 12 August 2024.

1.2. Distribution List for Notification

There is no distribution list for notification of document updates.

1.3. Location where this Document can be obtained

This document is available on:

a. RFC 2350 document in Indonesian

https://csirt.bsn.go.id/assets/rfc2350/RFC2350---BSN.pdf

b. RFC 2350 document in English

https://csirt.bsn.go.id/assets/rfc2350/rfc2350-en.pdf

1.4. Document Authenticity

The document is digitally signed using a PGP Key. For more information, please refer to point 2.8.

1.5 Document Identification

This document has the following attributes:

Title   : RFC 2350 BSN-CSIRT;

Version   : 2.0;

Published date   : 12 August 2024;

Expiry Date   : The document is valid until the latest document is published

2. Data/Contact Information

2.1. Team

Badan Standardisasi Nasional – *Computer Security Incident Response Team* which abbreviated BSN-CSIRT.

2.2. Address

Jl. Kuningan Barat Raya No. 01A, Kuningan, Mampang Prapatan, Jakarta Selatan, DKI Jakarta

2.3. Time Zone

Jakarta (GMT+07:00)

2.4. Phone Number

Not available

2.5. Fax Number

Not available

2.6. Other Telecommunications

Not available

2.7. E-Mail address

bsn.csirt[at]bsn.go.id

2.8. Public Key and other Encryption Information

```
Bits : 4096
Key Fingerprint : 624B090111548871AA49969DFAD07B49C0111D10
Key ID : C0111D10
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBGBp3rgBEADcxzRXb1DkEahEVlibeq1vEmZZXGjuUE8Yr+qzAnllRe4Bqg50
J05z9PXaDZDjL1ke7G89rnTiLoGZvb+FIwAj1/QQb8SjEbXG15QM7s/h9Fy0F7Xf
3n8mM9qphKBOJlkduT7rduLH3JoQwFbZLavgle0uzl0HigEzg7w9xYALIm/tX4al
B4ux2s3/exeCymEo00b97veXvrNKh/6zNlrpEP9sQJR3jOAfU8m0pV3wQmHOa8IF
cN5baQMZ2Xc1TskDlmhyJRr5cH8QKslyFVLqt2dlyTIKc89Z7EQ/UkxBtHyUB6Cu
Y46L7pWyfNjiDr1+8zPqtSXaUvHtn3OyuBgeu9o1Guvm+1HJna4DkBDlDi2Jj+eS
lQQgamBnfKt89EPTPzbQgzoCbIi4Fz5E+1bKyn+6Gnm9IIkxfJHnwKNbliZKzQQl
JWzWNKUEtJAfFDPVHFURoo3+J1h2Nnh5UkomQPkJYyyd8Ssl8+9XTgkoVA3OGk/D
Gb5Ol113wjcNm/Pr4ZZTQItZdGDHOHnH4EdwAoOeqBl6SdpERVWc1ks9F0psHM7R
jkkZnFn/3sPDmcl34+7lb2pKGT3n52qd+X8iAxtTpoCOTJVWRRl3cHPh0DTgdami
WIDLjHVA6YhTtJBMa+uNlJUEoxPLzTQfcndRI4k0Q8J1GCeB9WrIJ/eaLwARAQAB
```

tB9CU04gQ1NJUlQgPGJzbi5jc2lydEBic24uZ28uaWQ+iQJOBBMBCAA4FiEEYksJ
ARFUiHGqSZad+tB7ScARHRAFAmBp3rgCGwMFCwkIBwIGFQoJCAsCBBYCAwECHgEC
F4AACgkQ+tB7ScARHRA5pw/7BLJr3G2sY+ZVJBqm4YABDgHfNSgQSGPml0OHuIOY
BX2mzkFM1v8rrFdD72KWIH2BPpGdLfz+51M08nngf3NVlexseSy1Aq2jNVMMr/gR
Sqj5/sbF6cnb8b6QJBYRM925Tavrt+woJNLsZu+G4NL8rNFIhuaSwHidUX8JIdWG
B+PebRKj1moMN8ViX0tRIJBd2A3zhUVP+HoCo9eSS535jvRHZPxQWR3EqY5S5HnM
Wd0iNqGHUTxqgpHB/J7VrLejRP7l4b+VCDRCim8hM4J7Vldw6Gos73K7j7ZI77vR
BtpyKGBNPNsR+vM1bIvXttJQq7aeFUzBQTEgdn+pcGsyt42jqwTX/15tQkPLIyPO
563usH/PZLQEpQW5w39XdyivPftYUu03Nkve82W/UGWfUU+JiBVCqUFfr+f5yMUO
AC8Nun/Pg3M7pzspPcYffZ8MVaFLBTwqgnqS8h7KzumOYVCRuIysjH6zXQjvmK5h
05Ohh/nAQk+JmEAW5A+1uEHEiVhtgS7KA24GpMiZqu+3AuYhbaEhv7UH3qV02DAQ
GTqVI3BCKaF2cIzDKquXFrkaXWH9CJ/0kkFQzOsOZbWugMtKCq1LYLlBnD+OY9n5
+LJMtcRVbDJYMXaKuMIDM4mRQ3w2mwcwkz8frxP3HwSH2anf1NsQfXCYshj7dZM1
hqe5Ag0EYGneuAEQALVwZo1g9khICf4Segogh0lm/RFX9mE9X+MRtG81EnLHEPqw
ujPHSLHBo/evnJkTYUcsu3b+chevqRCFVZNaeo2dmWe7K2z9WgUvwH/4aZxw7uVk
CdZp0DStRQT7shi4x5mmBjlEz6eoYjUbJeRj0tr7v0IZdhucLMzcTnN5+YFS37dC
IvCYBImgKfceu6oNg595768B8nhDhP8xJYEikP74xhrBn7OuKhCY5OM3phv0wQ+S
O6RlSgrKpvAfBtjQNdWMx6veYhPQ9yfJjhkef8jW529uu/LqVxOUk24prwOXrC3j
m9++Be9b51bG+2iaqytbFlcq2Gis1QXYQd7G2QZfHJvzG3WpDFZV1JcTTH6Gxo6r
5e0A+vUHTUv3Zd8vNeEhC2kPcGx89Y1yt3/u2/eCbc5AF2oW1c1uRRWTe1Bx1nOE
oL9yOy76WIiiiFX7RAegAAywh9r9d+nOGJWPUlULP8lAyZlhYunouhGUAE+LPJXR
KvaqFBSKMcclzXAU69ylGQTc4XoXtrQQHHpW6yjC//FG5txLjAMc4cJVzfiLdl/1
9N6mNPdid/oUnve2etMbh+IPmJcHEOtm7zm1GbB5Bi2yjfCczmjlQn0GGGKywHSC
qidn01LAIcxrGEQ3vg2lmItxkDdAuCTCphS864k5OGdYvocM5JrCbyw6xt9/ABEB
AAGJAjYEGAEIACAWIQRiSwkBEVSIcapJlp360HtJwBEdEAUCYGneuAIbDAAKCRD6
0HtJwBEdEAigD/wLKVRmLHGdQarHiUouNBm5+pvTNQtGzdl1q8gDl+ZODpZh7ttb
E7yKFia3fRht1hm/NSf4hcQ8wSwcCWGcuKsNTa+aCS/N+3fNBblI/JCu4vTBbtoH
00MZnCM3vXvg5ujpygtHDNQlxqFeL1dY2pLyvzoR+4PDshOs9FJZEIk8bRoZesqJ
nbfqzpm+8iJKsuHmioiLZJSeTqDseO/9IhZEgXE4vq8d+IytyqeWgWllrygkPrvG
SRn/vcuSuO6YggsZvHxl9Wnns1c5s6fj8tqk+EugJjADqlk4+iRRJiFrFRIT31YT
KH5WuS9/7nbP4AHPfpWiyoecrePp/G7eGLTvgc0WtzZQxHdkqm9GAHeJZ2ADcJ2F
iA3GbjJRDl6B55Nq59nu7raPqphHPg1gik1Es9tBINWbTVJbjRcND68GQTCbZkJ6
W+851+j1iU52Yv/59W323A5y/rF5zWaiTNNgjiIRuK3wLTWmVO/6vfHefT5a0lhO
eOfvlpAFMEXZixNZWjUsYOav8iSJ/xzmCs5cEGM7GxsJjBP9zGKFvnBm77aUoHEJ
Cv82WA8fpdPcDV3qO4HRZ8Gsz3Tn3X9+Y/VuxVsktctonfeosM7IiiiRISftiDrmt
p5Lequ1DkpMfrDolFurb4I8pCRfsPC7NK4mnIvrHu1jqQCske5Awk5Y0eg==

```
=qqXG
-----END PGP PUBLIC KEY BLOCK-----
```

The PGP key file is available on:
https://csirt.bsn.go.id/assets/Publik-Key-Bantuan70-pub.asc

2.9. Team Members

The Head of BSN-CSIRT is the Head of Pusdatin, and the Members of BSN-CSIRT are personnel within the BSN organization.

2.10. Other Information

Not Available.

2.11. Notes on BSN-CSIRT Contacts

The recommended method for contacting BSN-CSIRT is via e-mail at bsn.csirt[at]bsn.go.id on working days (Monday - Friday) 07.30 - 16.00.

3. Regarding Gov-CSIRT

3.1. Vision

BSN-CSIRT Vision:

1. Establishing of a reliable information security system at BSN.

2. Establishing cybersecurity awareness among Human Resources within BSN.

3.2. Mission

To encourage information security activities and prevention of information security incidents, build cybersecurity awareness among human resources within BSN and conduct periodic evaluations of the reliability of information technology security within BSN.

3.3. The constituent

BSN-CSIRT constituency is limited to internal BSN

3.4. Sponsorship and/or Affiliation

BSN-CSIRT is part of BSN within Pusdatin, thus all funding is sourced from state budget sources in accordance with applicable regulations.

3.5. Authority

BSN Regulation No.10 of 2020 on the Organisation and Work Procedure of BSN states that BSN-CSIRT (Pusdatin) provides the function of preparing and implementing technical policies in the management of data, information systems, technology infrastructure and information security for standardisation and conformity assessment; and management of information and communication technology infrastructure, as well as information security.

4. Policies

4.1. Incident Types and Levels of Support

The BSN-CSIRT has the authority to handle various cybersecurity incidents that may affect or threaten its constituents:

a) Web defacement;
b) DDOS;
c) Malware;
d) Phising;

The assistance provided by the BSN-CSIRT to constituents may depend on the type, impact of the incident and the services utilised.

4.2. Co-operation, Interaction and Disclosure of Information/data

BSN-CSIRT will co-operate and share information with CSIRT or other organisations in the cybersecurity space.

All information received by BSN-CSIRT will be kept confidential.

4.3. Communication and Authentication

BSN-CSIRT regular communication allows using e-mail address without data encryption (conventional e-mail) and telephone.

5. Services

5.1. Incident Response

The BSN-CSIRT will assist constituents to mitigate and recover from cybersecurity incidents with the following aspects of cybersecurity incident management:

5.1.1. Incident Triage

    a. The validity of the incident and the informant.

    b. Assessing the impact and prioritisation of incidents

5.1.2. Coordination of Incidents

    a. Organising incident coordination with constituents

    b. Providing countermeasure recommendations based on BSB-CSIRT guidelines / SOPs to constituents

    c. Organising incident coordination with CSIRT or other relevant parties.

5.1.3. Incident Resolution

    a. Initiating an investigation and analysing the impact of the incident.

    b. Providing technical recommendations for incident handling.

5.2. Proactive Activities

BSN-CSIRT actively provides coordination and services to relevant stakeholders through activities:

a. Conducting awareness and training activities regarding information security;

b. Conducting risk analysis activities concerning Information Security;

c. Delivering internal audit or assessment services (security audit or assessment).

6. Incident Reporting

Cybersecurity incident reports can be submitted to bsn[dot]csirt[at]bsn[dot]go[dot]id by attaching at least:

a. Photo/scan of identity card

b. Document proof of the incident in the form of photos or screenshots or log files found

7. *Disclaimer*

Not Available.