RFC 2350 BMKG-CSIRT

1. Information Regarding Documents

This document contains a description of BMKG-CSIRT based on RFC 2350, namely basic information about BMKG-CSIRT, an explanation of its responsibilities, services provided, and how to contact BMKG-CSIRT.

1.1. Last Update Date

The document is version 1.6.2 of the document published on April 23, 2025.

1.2. Distribution List for Notification

None

1.3. Where this document can be found

This document is available at:
https://csirt.bmkg.go.id/rfc-id (Indonesia Version)
https://csirt.bmkg.go.id/rfc-en (English version)

1.4. Documents Authenticity

Both documents have been electronically signed by the Director of Communication Network Systems.

1.5. Document Identification

Dokumen memiliki atribut, yaitu :

Title	: RFC 2350 BMKG-CSIRT;
Version	: 1.6.2;
Publication Date	: April 23, 2025;
Expiration	: This document is valid until the latest document is published.

2. Data / Contact Information

2.1. Team Name

Meteorology, Climatology and Geophysics Agency -Computer Security Incident Response Team
Disingkat : BMKG-CSIRT.

2.2. Address

Jalan Angkasa I No. 2 Kemayoran, Jakarta Pusat, DKI Jakarta 10610

2.3. Time Zone

(GMT+07:00)

2.4. Telephone Number

08888196196

2.5. Fax Number

(021) 4241169

2.6. Other Telecommunications

Telegram (@bmkgcsirt)

2.7. Email Address (*E-mail*)

csirt[at]bmkg[dot]go[dot]id

2.8. Public Key and other Encryption Information/Data

Bits : 4096
ID : 0x99A17197F709F292
Key Fingerprint : 8F52 4299 29B7 A135 9E49 A2FE 99A1 7197 F709 F292

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

xsFNBGf/H54BEADJACBLEaWv2QYrr5iLNsvjznhWLmoV//+0zp/0zmNTCfm1nE4M
7ytaCf5l67TcS29ULOOSaBSkN2LRiCJ+87SU1XMLpDS0iG6HwPr320RCRMgUj7/
O
CY3Wjx1lpHcdDq2y8ASp55tsxyRVXLgx+uljBeM1P1PdAOwUgIQ7ZnaB/INp2CBI
AHR5TRm4TUalLJkahJzxi73esboeE7KJNElpEua2X6z6VNpvfMpHvdk/NMoaBkhf
W2tQiSvBBLsUQionGt9zaXXUWv7R3PlZURjCc8mhm1QJTc/
PpzK2wJxxySHCu2Aa
b6qc2K05oz6DXYjUxE1r6FspybNwWWAB0kcc9OCS4UDq7KbV6lCED5YWHy6qtc
Ln
kf8oU7Was/xhPGI1c0A5agEnWlRlahrePT/iQuE/pv+mJc71tzmqBNR9vnPcm4PP
l3IhA/3dzoka94HfAwO0WHnO89q/0q38gpbyq1wjjqo1RqmlxHM8DHXZ6qhRBlYZ
2fFm32QwCPxFxMNxpuIWNiP8L4HHK7wVQN58/2P2rFz2KR/
nONqYIG6OTu5+u9Pt
JG1j4fKURCgHjESDGhxpbtF3CZ0PoKe4THauJ+NqmXgUCusbaiBPmC2lLRhrQQ
5H
V0jNGlLZQyu2AzGi2hyVI45o8noPvBbpxjjziWsQUI04/TlAiG+ptjw5ywARAQAB
zR1CTUtHIENTSVJUIDxjc2lydEBibWtnLmdvLmlkPsLBjQQTAQgANxYhBI9SQpkp
t6E1nkmi/pmhcZf3CfKSBQJn/
x+gBQkA7U4AAhsDBAsJCAcFFQgJCgsFFgIDAQAA
CgkQmaFxl/cJ8pJeRQ/+NK+9eCHxfGRGJaBnq/VGWKhAiaIcEsWOSgYJhzDlg7jd
T86cJuWOo2guV/LCfOazNBZ0/GNTKBHZhqRcrXdPVeczdkbCCMmt3e2cEf/
Y+VGf
9q6N4V6JS6YzFn1cfVrDEAceXuWeRwqNOia8pyVUpfom7PGppslBPHSBqfT8qky
n
lw/JL2wfRc89pCZASG5w+uNhIAIWvojkmbUvg+z7adwNmRAT0nw9ZoMkuPtf1kut
XToytbjGgeMjOdyGVlOdVv5oknTPpPbpu7FJZze3hbh+WD0tr+C58jdCWonYXn70

qgUk4PB8TS+MHSKtXR/SSYmY8d+fc8NIsT9lxg82SuV1kAa2W+oJw7gRd8JRKEtt
lp+2UHIrFo7i0xJjBNw7K91meJ/RfqervR1iSk29RQqGUNMXIoRLd4Nm54MlmH0W
J/DlFDZDnEJw6lAooqp3mXo+ZNYlGvW+5oQIeEIWDHgquMj/7dJTZq5YyU0y7OOi
0zjeZ3VwfH8dGZ0fnKUATKCI5FCZ472HJV19VG5O1jxezaM4xBqTdD9073YgePu
E
P7Rlj5a6zJgpUJwbb7EP4xjoL/XSGxSFR9RbSy6gfE2S9Jz0xpcJdIwr6KAN++dK
MpLTMv34o926TPWmy54lji5hyBF9VgSP+UrULYXgXD55cOB7zoMixTn1zrr5DBzO
wU0EZ/8foAEQAMb1X4E8wDTZ2aDomNyKTyY3xvLEq9KE8n3O/0g0tieG87E9/
mKb
JHi1L3nVyDWfSy/3lzZwW0M4QsHyGOsIwDwk4FePUNgVkFwi/
EBNQaWj3jHfSGhR
CbGGHJSy1X8UUS6CBqr2EREdh4xmGCL3Ynzeeyoe+F8ttn6noxWrdRTN/
geoZmgM
PaIWy5ezJhYBZxgDRMwUg7CWX1Kf6t69JRvf3RXL6bkRNPxjA06z3+/5qgaSiSnu
1ArsfoNkWEuRwaoHDyv/8gYHiMYWrHcpSFZbbWqRJsn/
ypifSb6ENDAUqR2SNak7
DAHs9drGGm0dvynZWZY+gGL322z2ZkyP71jOXW78DyBj00nwRLevvcxPzvgJReG7
P7zt7xQ+3JC6S0RaT/
W3CQLEKbzaJCnH3gE6xcFZVOxSimf1Hta2chgdB0HLU2MZ
Bk5B9E5C2BWeipGHJPtfwzsG0cjpXJcYlg7jW4wAdtfvZo8HZRwuh2euIMV9OnLl
1SdYkuXBAFD9BGYxzbQwSTPT9bzaD3eo3vYujs7kV2lDIYVhks4M0JPRmeHxmw
vA
CK1WVKzKI+Heb7S61qYDUJcocXp2Bzk03HkESYaWeZe+/cLHkdsw8YKd/
JBLvrCl
ciLgMgPawZJAN3dc2zeZ1i3FEJoiSP+p9xTXX5zOXvPW9whsF38DFv0HABEBAA
HC
wXwEGAEIACYWIQSPUkKZKbehNZ5Jov6ZoXGX9wnykgUCZ/
8foQUJAO1OAAIbDAAK
CRCZoXGX9wnykpB/D/4nKHh1Sw1WqC+X92aVMi9LwOJx2xRcPx97tDl/
mTkkUOAA
L2R1vDInMcphUVe51zhu0kONRbz7UlZ88nH5L2x5zL0oO6uYFuvmxyXB5vC8ncw
X
OCShth/a5vnucb9BCJChYzEzsIVprfxqMxOoAlvTOTxG4EIOs5aShVhBlzEUP8kp
ju7iq08FT2EXRBIS1CPa0luNJNE/FG2XRtwQ2wn9pu6wg0G5UgarE2kEtuZH9dGE
feAxbpst383mUZKSmViUY7RIwHW2lOGCxnMBbQz1TQUEqDjxRZgLZtK9WrNjBe
qK
ke1/VfMUkZRhzGB06bKFQshrumS1DBliLnPzXLntLAARTut8lhGhhyqbW65kRLgp
/NhoPOqBMkoTVv6XS5Ky23b/Kj2lUxLgldITVeYOoXueCNOUlDmxLwsmIBcQoccj
Ie9RCELEe3NCLQiWyA8aj7ubNBdjOpjm92KVKvfT8b/dvsgdsnv9PHZswVmjSba7
x8q4BjgudmEaYS9iANYio3T8WBinwcMTeR3XsoGUVYzZBrYuiIu+2xFZ4Vtz/yR8
xvDErha7gXMjyBEnl0V9t/IJBEFIOmk2MI3dpv4wGwN6XvqlubfX2DgjdV+f/R1T
BBe8wNXAqCZemc+fV67F9MdzkkDZY/iWCHC8GdqOjEjGi/
lUOPJQBENmtMpFWg==
=RkbN
-----END PGP PUBLIC KEY BLOCK-----

These PGP key files are available in :
https://csirt.bmkg.go.id /pgp

2.9. Members

The person in charge of BMKG-CSIRT is the Deputy for Meteorological, Climatological, and Geophysical Infrastructure. The Chairperson is the Director of the Communication Network System, while the Secretary is the Coordinator of the Information Security Division. The members consist of specialized functional experts within the Directorate of the Communication Network System.

2.10. Other Information/Data

Information on operating hours refers to the BMKG Directorate of the Communication Network System service catalog.

2.11. Notes on CSIRT Name Contact

The recommended method to contact BMKG-CSIRT is via e-mail at csirt[at]bmkg[dot]go[dot]id or via telephone number 08888196196 which is on standby 24/7.

3. Regarding BMKG-CSIRT

3.1. Vision

The vision of BMKG-CSIRT is to increase experience in improving cybersecurity

in line with the vision and mission of BMKG

3.2. Mission

The mission of BMKG-CSIRT, namely:

a. Provide technology services aimed at establishing resilience and cyber reliability that support the objectives of BMKG-CSIRT's business processes cyber resilience and reliability that support the BMKG-CSIRT's business process objectives
b. To provide cyber education and awareness to employees and other parties with the aim of increasing cyber resilience.
c. Minimizing the impact of cyber incidents
d. providing information on vulnerability findings, potential attacks and information on threats or other cyber intelligence. threat or other cyber intelligence with the aim of establishing a cyber resilience ecosystem. Cyber resilience ecosystem.

3.3. Constituents

Constituents of Name-CSIRT are Users of ICT services at BMKG

3.4. Sponsorship and/or Affiliation

BMKG-CSIRT funding comes from the APBN (DIPA BMKG)

3.5. Authority

The authority of BMKG-CSIRT includes:

a. Implement cyber awareness programs with other CSIRTs
b. supervise the operation of information systems in fulfillment of cyber resilience and reliability that supports business process objectives

4. Policies

4.1. Types of incidents and levels of support

BMKG-CSIRT handles the following types of cyber incidents:

a. *Web Defacement*
b. Malware
c. DDOS
d. Phising

The support provided by BMKG-CSIRT to constituents may vary depending on the type and impact of the incident. (in accordance with the SLA in the service catalog BMKG Directorate of the Communication Network System)

4.2. Cooperation, Interaction and Disclosure of Information / Data

BMKG-CSIRT cooperates and shares information with CSIRT and other organizations in the scope of cyber security. All information received by BMKG-CSIRT will be kept confidential. In the implementation of cooperation, it is mandatory to include a Non-Disclosure Agreement form.

4.3. Communication and Authentication

For regular communication to BMKG-CSIRT, you can use the official email address without data encryption (conventional email). However, for communication containing sensitive/restricted/confidential information, you can use the official email with public key encryption using PGP.

5. Services

5.1. Main Services

The main services of BMKG-CSIRT are:

5.1.1. Provision of Cyber Security Warnings

This service is carried out in the form of warnings of cyber threats to owners / operators of electronic systems and monitoring information related to ICT services.

5.1.2. Cyber Incidents Handling

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

5.1.3. Electronic System Vulnerability Handling (Vulnerability Handling)

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

a. The reporter of the vulnerability is the owner of the electronic system. If the reporter is not the owner of the system, the vulnerability report cannot be handled;
b. The vulnerability management services referred to can also be a follow-up to vulnerability assessment activities.

5.2. Additional Services

Additional services from BMKG-CSIRT are :

5.2.1. Digital Artifacts Handling

This service is provided in the form of handling artifacts in order to restore affected electronic systems or provide investigation support.

5.2.2. Notification of Observation Results Related to New Threats

This service is provided in the form of results from the BSSN honeynet early detection system, BMKG CSIRT provides statistical information related to this service.

5.2.3. Cyber Security Risk Analysis

This service is in the form of vulnerability documentation and information security risk assessment in accordance with the ISO/IEC 27001 standard.

5.2.4. Consultation on Incident Response and Recovery Readiness

This service is provided by BMKG-CSIRT in the form of technical recommendations based on the results of analysis related to incident mitigation and recovery.

5.2.5. Building Awareness and Concern for Cyber Security

BMKGCSIRT builds People, Process, Technology to support building awareness of sustainable information security.

a. Organizing cybersecurity workshop activities for constituents;
b. Organizing Cybersecurity Incident Drill Test activities for constituents;
c. Organizing security socialization for constituents;

6. Incident Reporting

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

a. Full Name, NIP, Position, cell phone number, official email

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

7. *Disclaimer*

None.

Jakarta, April 23, 2025
Plt. Director of BMKG Communication Network System

Irwan Slamet