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 1.6.3 of the document published on 16 July, 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	: July 16, 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 : 0xCEA24612B62A7F79
Key Fingerprint : 4294 7833 E4F7 E536 503A 8B25 CEA2 4612 B62A 7F79

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

xsFNBGhcu7wBEAClnbWXpbQ9fzOgkQdNFE9J4w9MFsr/4XxBk4Xe3dsiCdf7YvJ2
b9TgFVNC5AW5QJCw/9x9O5dYfrd4awSrtAH3zZZw1v9qllbcWtSaKmpzS3rAXX1R
Kx4vHvZ/rziafKwWNg9iiFmelfnEE4uKVUZiw2F55RpriGFAh4xmxLjWgS7YLLd/
YQzXNfWqUwXLnSPC11mMaZKvG9Dr38jdEmQ6lv4d5EJ0pK3tZwuXVN2Pz4+fe8
MO
gdmtHGwO1eklxZzUhvUPqMyui3q3nWNKE3Wz+nPG6j87okEs7k4Qc3Wk/V3MB9
3R
luWWYDWl7lR9jiq83eSJNDhjMXCy0rwWYwpYKdWvSO2uSitxxNfhCE93hTSbQiG
U
6KxKR2TJFXInNo/leuuvjD4qNK3lZ9O9dA0Q2K+nCF1/qxztrW/KiQc0d3kt6+7D
bCjvTB1ISr/5Kb68t7gQX80OKpG1gCqqWILYT8qEPjOWGd7PlRfBLo1GM/29J1a4
7cGoOFpUJrgD58yuaNzMHfOn4CrGONeyeyESplez1LsXvKK9SIW0McaPbk1/g3V
N
fWPsQ8i1vfc6YyXpvK4Tnw4QVa3bRz3rYv9f8hneYiia4uTzGa5aDsx8g0/HaRyd
5fMWYm7+K2PeRfxr55N8BrysB93y82i546ks3s3g0WxrR31brolzavEocwARAQAB
zR1ibWtnIGNzaXJ0IDxjc2lydEBibWtnLmdvLmlkPsLBjQQTAQgANxYhBEKUeDPk
9+U2UDqLJc6iRhK2Kn95BQJoXLu9BQkA7U4AAhsDBAsJCAcFFQgJCgsFFgIDA
QAA
CgkQzqJGErYqf3n4PA//Y7jmG9UT/JoWMv+yh5mjxiNS1QGt6Ksm0wkM+kV1e3T
W
WvPOcPRwM30osksynz/s60zxhF4k1/D5anFiR8EPArXONqvAKPNzy2FW6w3ilHbi
pIqEkYandjV6kkJg99uFcdwQxijrTpOiKgvO0pPpABLoSRU+9JXxI/1HlHl9zFx0
w3aUsL1oLAxRdAg8cEDb4R/QML494rN5+UE5icez8Viz5YWyW+dLxO0oeoBDMk
0a

y37beFHjOJWaKMpKTWOP6Z2+IIVuE5jy6cuHSRImAGtIeftuGmJA+3/y2BMKNm9Y
7R494oyvbWE9qvyr5NckS5tEoHnHya8qeOsYf0ZJWUl0WRdiadVusrDJ8yLXLdKuMU9VZ8BJNX4q7ZF1fAvvtuu+3zltZCyowq2pTlQEtD1FdbgcgAve+9PasHzFIKF6vOnYE44oOzlV+3mlsUJwVZgOtXayN9mT89kAtlJcFSEebX2QCN62Vv/Jx409RIdTpAQQ1um/ZUYwCVNkaZ4o3zWLoINSoOf9X6GZU42G6iERNsI7X+KDDOkPl4cTL8zo
LzhvRJyBMz6HrVC21pwz663Eo+2D5AOEwySvASlsPBhXDmavEjzW2pwJ0tKcGb9W
jI8lughOl+PEGm5SuITGWkqP/VMlqhL//ZfmNf5Lc0A9xkBRlVP2mWSdWD/dvLTOwU0EaFy7vQEQAMk0BiewPceZ4r9BXoq17vKkl4pvRipbOm4TdjnZz8DOstiAlCtidpwTIAS3tv9WptPwLF0O1IDh7bU5Af0iNoCwIqj+fU9hyyPf3exRZ6wPDw52z9ocC6QotIP723qrQqn0GLO4fIsvOcsZoN5PzKNeHG4DEDkPmvvWr6FwkaaHJMpcefa3
x7foV/AKiXxjxjtzHxpu7dry9cTobowqzEztDFMcf4cf+rytfMtZAbiqnBp2z7q3
9gEmRxerr9GNCmA80AaYfqYML7zBr8hLaINhdNlr8eJU7idzJgSIOOsVR8BBjYPqVg1YXcPRhHq9cvI+PQi5SFz81Gj/iBApJIIJMsx+66xmRY52dFZXzcVBwMDYAp9F3JZZt172Zt3U/mPdhJgJGwifEIvSO414opdASLsqjW83xF3mW5fxLmpDKUZ9GQIwwfKKLx39H8fcjNtVd7m7m4gnVqMPbyDvZfSaN2MXpyBHdPY9i6k6y2rfLy94Le2Oi4MGjRYyQaLYVZSeeOgCZQWhodrsfdPzSNjHV+NfoTjO/73KKEQeuyLLXoD23hK0
Qwosy82ocY3TICTefOql+vIADj/Tiyz7znRIRh9btIvkujJeKZy3e1TtsEBHr7FpLHT5OD6AAs7MDWaXgQ0qltcOV0MWuntcZd8lDnn/6emjgrerC+W7WxzrABEBAAHC
wXwEGAEIACYWIQRClHgz5PflNlA6iyXOokYStip/eQUCaFy7vgUJAO1OAAIbDAAK
CRDOokYStip/eeHhD/9SEKBGaVURd+6loXLiVGVJV6LzIYALi4ynj9yeF7RRuI9SsE26KbaKP4cOb5ir3TOrKz+omDzNxwQPaSDg69S8tHzzC6svPcgL5WlI6jK3YtlggLNi/6GdFu7Fz5d+vVVFtLfe4K/NYeglsTz7cnRFLK+FtNGZxC1Fw16IDTQL4CdGikyn9qJsE90OQ+mloo2HPlhGxXk8nMNozporBmOJ3aTi7jj5qozZZU9iQv0HpnN1uGZCnUC3ypn0ArtnY/e/6RJzUObBjc4/HcVt5XOG+IWvpw8fBY08Twqe3PpHJn/DCOTjSp3eE2DhvIFDqfSIi5vs28mhie5npyqOX0Ksdno/bcZ+ZBoEPCncSOx2qDwYFyfS97hdaU2CiPd0sudrvkNapjdA43MZ3jKpGhaukeTfUlt7e8GNuSBNzZbcM3RUuXVMPog8wEsK+oY/hGQrZaWQ0Md7/FhR+0anWB8jmrOftVUDkg3p/4l5Q5GMYO1s
dAqSWwmcHoX1CpyhufYN1C+zdWvWn8Cl88qCjhU5hG5SDvQjSJ1jR9+inl2y398A
HbAmy5LBjysMMwf6fTQ9CJhrazFpof3MVl9Li2HXAVHpBWtplDVKkb48qUNRwH3n
38nL0PXwH/Cg+MTX2WAtK4t9IgWqPNEzRVep9b/i3gTalZGr1zP2UppLbgvaJQ==
=luHe
-----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, July 16, 2025
Plt. Directorate of BMKG
Communication Network System

Irwan Slamet