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 1.6.1 of the document published on February 26, 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/file (Indonesian Version)

1.4. Documents Authenticity

Both documents have been signed with the BMKG-CSIRT PGP Key. For more details can be seen in Sub chapter 2.8.

1.5. Document Identification

Documents have attributes, namely:

Title	: RFC 2350 BMKG-CSIRT;
Version	: 1.6.1;
Publication Date	: February 26, 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

Abbreviated: BMKG-CSIRT.

2.2. Address

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

2.3. Time Zone Jakarta

(GMT+07:00)

2.4. Telephone Number

08888196196

2.5. Fax Number

(021) 4241169

2.6. Other Telecommunications

WhatsApp BMKG-CSIRT (CSIRT Service Catalog)

Telegram BMKG-CSIRT (CSIRT Service Catalog)

2.7. Email Address (*E-mail*)

csirt[at]bmkg.go.id

2.8. Public Key (*Public Key*) and other Encrypted Information/Data

Bits	:	4096
ID	:	0xD77CB11C188D27C3
Key Fingerprint	:	BF93 8B46 46D2 23B5 C733 42F2 D77C B11C 188D 27C3

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

xsDNBGe+eVsBDADhUrj8Y0SNoXpIk+v5Z2G5L/db8k76QStBqQmTkjsQcPdcRmIH
MGWKGGYom49NvDr3vkUxtP/Wbg9igj7uHGcE+89v/JyjimBChcWz9oHEYSifDowo
ZP77XXtSvQjAUJLyHK7pxCzuVsAESWAlG/bR3KnizGAcxjj7WHt2rpxODZCZtTIf
eO58l9jSLddlTGtjk8EfzGNop26vemqaHajMmGPs4d8QTPAVluyPHaZWIwQo1UQZ
xRIIyHPbNnWCgUMPBVo7De4wDGm3+WWyM/YS93PXYzUFG1RfvldysGqAxBVH9sZd
7MBet/AfxbhyjigVXSzYeYWPRlrSFvmjHzXk/HHnOTZrLDrAPvoViEmRYnpXW1kv
sh16uKE/mfgjSO+8oDXn1KpXLJKL4RG7hzlFQktIBIdOq582lE/gDcvCVii9Hlgi
xUNtOcnJK+tBNLxb2cwFjZjADpuxslRLCn7519HOEZCG+aasMBQtM2KFwz9hSEM3
qg5Nna2LfCQzhoUAEQEAAc0dY3NpcnQgYm1rZyA8Y3NpcnRAYm1rZy5nby5pZD7C
wQ0EEwEIADcWIQS/k4tGRtIjtcczQvLXfLEcGI0nwwUCZ755XAUJAJ40AAIbAwQL
CQgHBRUICQoLBRYCAwEAAAoJENd8sRwYjSfD8bEMAKbzcf+hlWMVyGBC
```

j8NPrh8W

ryrKudChQzOh9ADPedAgrYVxJKT/vkrGANen/DNSsG2SmPLrTqgUQ0xOaOmXMdnD

dySiyjU9kx89hrul95FPLj+gmbYIMh1MwACghRMo9ynAbOfRbs8P0VxfcRy61FRD

7Km9FPS5OQsl9S6HzqGUflxZ/c/n2fIEQ/sgHm3J3t+VbFy7XUNDgdyZCL6PSBQF

PyunY6+xa4DRDefoJuolUEV6uBT48fS+hVzAEYYIL2LqUv/eZ9unOUm0yKPeHp7R

LAKiONTT0T67QZGrX3fHMG41Wji64Ro6m7FKZQVj33IChBfs+L/sKLvMPPJpXeDH

nlPtGC890hjsGm86ynMLOy3U4TGr3caDI42iUekmopg/ZOp0bhk023u6oVdNfFMA

evyoJEk15k5jC+jJA+hlfMNlJntShVmT4hsHu9VNqgebrk44dN8Tu39HqMA0zA64

YWi6LJ9ebY//WmVsAON0MuxQhYjj5jItRH96kcTKK87AzQRnvnlcAQwAxAlIqVAG

cOTfpWL3JMswpH3amSCFD1UnycarNraaNLZis21YerYg9eDmi0BD0CSuewVHV/Rv

ZJnwEZnG74IEcq481cc32J+kxGKTWfZwh7B0NLW1hdb9b8vcY+rdCTpEffmw+xX6

HxNiZQkUx1ffrQylmLGi9BVNbd0XI1DztiXIt8FQ9vbTt0/06Q3Cwjh+aNKVjCe+

yUYj9H5Ai/HbeHVAhu2susXZnWhVqB9+iaxgumggv0pisGfDway9MtAjMzXAtEwT

ZTjC0YTbeLiGU4mdjePuskNV+8/FV6GHqxxYfFi1Gt9Pk2F8PFyfGIwC+tgXEBPW

wgVndxd6tGQcY1Ey+tXnVMkpoARqTJOs4/o8rVQNRvhpuIXcAG54hdRMrtYlWO2b

a8hAK1XIxWJSDukVKzx+7exNx6rbCLPUwrKT3WMRCdW+ni+4NlGA/eLitV5zq0ry

68abD45F66+YMJcsPi3meDxjTMbLOM2eLlmiiq6kwL1QVHrrKG/dxexZABEBAAHC

wPwEGAEIACYWIQS/k4tGRtIjtcczQvLXfLEcGI0nwwUCZ755XQUJAJ40AAIbDAAK

CRDXfLEcGI0nw56/DADKuhc+PkIUeTOQ2UtH86bFK2jI01gZf71pw07dtoCJvJY6

ldiFVxWveysSU9KzyV0Q5K25ulsMeCN9JHyMiAVVKezN73HkXDqCcR+LKR6gjMuU

RZKzepQNBvUKKb/AIN9xpjeNVWgGO7bq8c0EPSOXHUT9tkvpfhltzUc1DTryeXq4

ArfX6TLyJvI+arB5Yv5Vf0rN5XI/Pdfsc5AcHOvkMOn5dD2VB0jNynCJFwLNElt6

WgKufL70JNr1WHU1yT7OrPYisb/V0AKd1wzy2CP8RlUzVPVzLCslEn675n84ROjD

NLBSPi/C8SPg979fnYiizu4g4iOHrbpN7PDv6LRr8CMmhVBW1iL5/AF3w6IYynM7

```
l38BOV5TNljQe0zVEnOkl9h2GYfaYEIKTdj8cIzmswQxzpiGegkVhwy4yjMJVfn0
0AA7xzsbwZIsrOtn07/2iP3p8JfYhPFLOuYBzaPQXmLkLz/TkHN5Fu16/ik3BYTH
Yjvlx1dGcLzhD8gi884=
=/Cqo
-----END PGP PUBLIC KEY BLOCK-----
```

File PGP *key* ini tersedia pada :
https://csirt.bmkg.go.id/storage/public-key/Publik-Key-BMKG-CSIRT.ascTeam

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 BMKG-CSIRT Contact

The recommended method to contacting BMKG-CSIRT is via *e-mail* at the address csirt[at]bmkg.go.id or by telephone number 08888196196, on

Monday-Thursday, 07.00 - 21.00

WIB Friday, 07.00 - 21.00 WIB

Saturday, 09.00 - 16.00 WIB

3. Regarding Gov-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

BMKG-CSIRT constituents include:

a. Autonomous System Number
b. ICT service users at BMKG

3.4. Sponsorship and/or Affiliation

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

3.5. Authority

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. Policy – Incident Types and Levels / of Support Policy

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. Phishing.

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 share information with CSIRT and other organizations in the scope of cybersecurity. other organizations within the scope of cybersecurity. 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 normal communication to BMKG-CSIRT, you can use the email address of without data encryption (conventional email) and the sibatik.bmkg.go.id application. However, for communications containing sensitive/restricted/confidential information, you can use official email with public key encryption. through 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, then the vulnerability report cannot be handled;

b. The vulnerability handling service in question may also be a follow-up on 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 artifact handling in the context of recovery of affected electronic systems or investigation support. affected electronic systems or 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

BMKG-CSIRT builds *People, Process, Technology* to support building awareness of sustainable information security.

1. Organizing cybersecurity workshops forconstituents;
2. Organizing Cybersecurity Incident Drill Test activities to constituents;
3. Organizing security socialization to 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.