# RFC 2350 Bank Maybank Indonesia-CSIRT

## 1. Information about the Document

This document contains a description of Bank Maybank Indonesia-CSIRT based on RFC 2350, namely basic information about Bank Maybank Indonesia-CSIRT, explaining its responsibilities, the services it provides, and how to contact Bank Maybank Indonesia-CSIRT.

### 1.1. Last Update Date

This document is version 1.2, published on August 19, 2025.

### 1.2. Distribution List for Notification

Distribution of the RFC document is limited to internal use within Bank Maybank Indonesia via internal communication channels.

### 1.3. Location Where This Document Can be Obtained

This document is available at https://www.maybank.co.id/others/rfc-2350

### 1.4. Authenticity of the Document

This document has been signed by the head of Bank Maybank Indonesia-CSIRT.

### 1.5 Document Identification

The document has the following attributes:

Title : RFC 2350 Bank Maybank Indonesia-CSIRT;

Version : 1.2;

Publication Date : August 19, 2025;

Expiration : This document is valid until the latest document is published.

## 2. Data/Contact Information

### 2.1. Team Name

Maybank Indonesia Bank-Computer Security Incident Response Team

Abbreviation: Bank Maybank Indonesia-CSIRT.

### 2.2. Address

Sentral Senayan 3 Building, Jl. Asia Afrika No. 8, Senayan, RT.1/RW.3, Gelora,
South Jakarta, Central Jakarta City, Special Capital Region of Jakarta 10270.

### 2.3. Time Zone

Jakarta (GMT +07:00)

### 2.4. Phone

021-29228800

### 2.5. Fax

-

### 2.6. Other Telecommunications

-

### 2.7. Email Address

Primary e-mail address: csirt@maybank.co.id

### 2.8. Public Key and Other Encryption Information/Data

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

mQENBGfRe/ABCAC0MwprtpM7wlYApuWtz1/bELS2hV7lnklRZgZJHz4Hv/n5G7lS
T8JJ8cmWeQqeQqyZKKbM8rAr0nhyJvodBNQj7yeH5r7jR4lP2lsCk2DfvDtfYYdO
EF3X84cerVTqnEiVNn2HbYdeJLkFjCicguW1HYs/BcMyoZquyOZSk1yk00oCLHJm
VAbAtngcKzQUIZfOAG8wwyxCA0KJ9UEfUaUw/onGaUnQhNLanZmpCCmQpKQ
291Mr
mcqElRmghsKwiCcGibdSM0Yjtc0oq8uFLVDUq8KSXcH2ilb8f0Nj0t+Z8FtEp3Ek
L1j53vvgzMegLxV7p2mn9cAFSB2g8rHe6xqXABEBAAG0H0NTSVJUIE1CSSA8Q1NJ
UlRAbWF5YmFuay5jby5pZD6JAVcEEwEIAEEWIQQLsjRARMO1SzK7CDtVbH5rWYks
0wUCZ9F78AIbAwUJBaSE4AULCQgHAgIiAgYVCgkICwIEFgIDAQIeBwIXgAAKCRBV
bH5rWYks04KZB/9ZLiA115NXiM8aUnEzZ8yXhN5yVfr9kSrTWuRdyCxv25kAAh3y
2tkFh0toZ4T0p7ZflqBsgVUXTkwOBLYyyUxNgQYFIEGttfOcsC2CXQgX+r0GOKOb
nupl4Qj7ponupnBXFMmqdoBRUaBVfa2D6cXjAAXq4GdRrezHePHaQoFyJ1+HCU/
z
```

```
hUwYhznSCmn5Wl2st4Z9J2ptONDvAY8KmLTj3tw/B4QVm3zZOmL9vn/ojsuhw6
QN
PZN1ni8xpjiuhs0WDFlHnMZ6OdleESyULXSKZRmZZVqM9MDutiAN4/xBUI7Z8cXT
E1VNg66hK53u59WmeA1qXBrfUeDgJoed6W30uQENBGfRe/ABCADNv6XlfFQd+e
dl
svo2M3Vvxl5fU52fmNsJuJW3vog2BoTVTjJeMyeUnVXjxLimxVSv+dVtC5FqD8Qf
lZEl2QRMZFQhKzafn7kWl9SXyMZ9hVm/4lVsE6WQSJvFPNY11GjfR57fTuK/a8x6
WEvjK9xBGWJJgvfqScNsBSo6nwA0xLKg49Wh4Jze5u1KCqJ8lKDU0CBnxQM0Eo
Q9
2JWzJbv+p8kiCH/oR7N0GnX3v+eLUC9DClxAH/oSxtHH12w4qewVfPStyzQsZtmi
V56hBbtcu+hBA0pXrbGWPQ1cujtl6ybT6HA6Y1QeyMzuNyEW/8Y0pGL78yLpt5ql
ql+fJqf5ABEBAAGJATwEGAEIACYWIQQLsjRARMO1SzK7CDtVbH5rWYks0wUCZ9F7
8AIbDAUJBaSE4AAKCRBVbH5rWYks01E4CAChruwXmyG0reyrpFRX6xRP5u7lN0M
/
XNkkxrEUYsBJ6LbDGytiraqd7fv0w17uEROxT9ohIuDMyv8CLdmoBQzwH4V6Mo5x
t0PwTlsAG2NzWkJM8qAMJSwIBpMoytS3nhGm1vHikzEmLGmVCZ1AwO5S6AM7Lh
5p
FrOASMq+wj6n10SmrSXeiixlFJNxGqdxBOb9wUK7cb4H37NyM9Yulmvv/sCx9zRv
qPciYEZZi+GeG2eR1KTCUGFcsgvOr01z3DRy8YALKC3X0GDafG9NA4y7pW9ul7tT
Msw99E4sEZgok+vjoQkuD+OhQr1k/W7dQPY0zxjxLW4PO1x2toxL/3v4
=L9+n
-----END PGP PUBLIC KEY BLOCK-----
```

### 2.9. Team Members

The chairperson/leader of Bank Maybank Indonesia-CSIRT is the Chief Information Security Officer (CISO), who is responsible for providing direction to all CSIRT stakeholders in collaboration with the Computer Security Incident Coordinator (CSIC), who is the head of the IT Security work unit. For the composition of CSIRT and CSIRT team members, please refer to Bank Maybank

Indonesia Board of Directors Regulation NO.PER.DIR.2025.005/DIR IT & DIGITAL concerning Information Technology Security Incident Management regarding the structure of the CSIRT.

### 2.10. Other Information/Data

None

### 2.11. Notes on Contacting Bank Maybank Indonesia-CSIRT

The recommended method for contacting Bank Maybank Indonesia-CSIRT is via email at csirt@maybank.co.id

## 3. About Bank Maybank Indonesia-CSIRT

### 3.1. Vision

The vision of Bank Maybank Indonesia-CSIRT is to achieve reliable and professional cybersecurity within the Bank Maybank Indonesia environment.

### 3.2. Mission

The mission of Bank Maybank Indonesia-CSIRT is:

a. To build the capacity and capabilities of cybersecurity resources.

b. Providing a security system that includes procedures and systems for prevention, mitigation, and recovery from cyber threats.

c. Providing incident response and/or incident recovery mechanisms carried out by the cyber incident response and recovery team.

### 3.3. Constituents

The constituents of Bank Maybank Indonesia-CSIRT include all work units within Bank Maybank Indonesia.

### 3.4. Sponsorship and/or Affiliation

Funding for Bank Maybank Indonesia-CSIRT comes from the company's budget.

### 3.5. Authority

Maybank Indonesia-CSIRT has the authority to respond to incidents, mitigate incidents, investigate and analyze the impact of incidents, and recover from cyber security incidents within the Maybank Indonesia organization.

## 4. Policies

### 4.1. Types of Incidents and Support Levels

The support provided by Bank Maybank Indonesia-CSIRT to constituents may vary depending on the type and impact of the incident, as described below but not limited to:

*a. Denial of Service (DOS) / Distributed Denial of Service (DDOS)*

*b. Malware*

*c. Phishing*

*d. Compromised Information*

*e. Unauthorized Activity*

*f. Compromised Assets*

### 4.2. Cooperation, Interaction, and Disclosure of Information/Data

Maybank Indonesia-CSIRT will cooperate and share information with CSIRT/TTIS teams or other organizations within the scope of cybersecurity. All information provided to and received by Maybank Indonesia-CSIRT must be kept confidential.

### 4.3. Communication and Authentication

For routine communication, Bank Maybank Indonesia-CSIRT may use unencrypted email addresses (conventional email) and telephone. However, for communication containing sensitive/restricted/confidential information, encryption may be used for email, data, or other communication channels.

## 5. Services

### 5.1. Main Services

The main services provided by Bank Maybank Indonesia-CSIRT are:

#### 5.1.1. Cybersecurity Alert Notification

This service is carried out by Bank Maybank Indonesia-CSIRT in the form of issuing warnings about cyber incidents to electronic system owners and providing related statistical information.

#### 5.1.2. Cyber Incident Handling

This service is carried out by Bank Maybank Indonesia-CSIRT in the form of coordination, analysis, and technical recommendations for the purpose of cyber incident response and recovery.

### 5.2. Additional Services

Additional services from Bank Maybank Indonesia-CSIRT include:

#### 5.2.1. Electronic System Vulnerability Management

Bank Maybank Indonesia-CSIRT conducts coordination, analysis, and/or technical recommendations on a periodic basis in order to strengthen information system security.

#### 5.2.2. Notification of Potential Threat Observation Results

This service is provided by Bank Maybank Indonesia-CSIRT in the form of periodic monitoring of Bank Maybank Indonesia's assets for potential cyber threats.

#### 5.2.3. Attack Detection

Analyzing data to detect attacks on electronic systems or suspicious activity on electronic systems or violations of cybersecurity policies.

#### 5.2.4. Cyber Security Risk Analysis

Identifying and assessing cybersecurity risks and recommending follow-up actions to address these risks.

#### 5.2.5. Consultation on Cyber Incident Response Preparedness

Providing insights, understanding, and necessary measures to assist in handling cyber incidents.

### 5.2.6. Building Awareness and Concern for Cybersecurity

Carrying out activities to increase the awareness and concern of information system users regarding system/cybersecurity through socialization/training for relevant constituents at Bank Mandiri Taspen.

## 6. Incident Reporting

Cyber security incident reports can be sent to csirt@maybank.co.id by attaching at least:

a. Photo/scan of identification card

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

c. Or in accordance with other applicable regulations

## *7. Disclaimer*

- All cyber incident handling depends on the availability of tools and related resources owned by Bank Maybank Indonesia-CSIRT.
- The time required to resolve a cyber incident varies depending on the circumstances surrounding the incident.