RFC 2350 CSIRT UMM

1. Document Information

This document contains a description of CSIRT UMM based on RFC 2350 that includes the basic information of CSIRT UMM, explains the responsibilities, services provided, and how to contact CSIRT UMM.

1.1. Last Updated

The document version is 1.3 issued on March 29, 2022.

1.2. Notification of Distribution List

There is no distribution list for document updated notifications.

1.3. Document Location

This document is available at:
https://csirt.umm.ac.id/csirtummrfc2350.pdf (versi Bahasa Indonesia)
https://csirt.umm.ac.id/csirtummrfc2350-en.pdf (English Version)

1.4. Document of Authenticity

Both of the documents have been signed with PGP Key belonging to CSIRT UMM. Seethe details in subchapter 2.7.

1.5 Document Identification

Document has the attributes, i.e:

Title	: RFC 2350 CSIRT UMM;
Version	: 1.3;
Publication Date	: March 29, 2022;
Expired	: Valid until the latest document is published.

2. Data/Contact Information

2.1. Team Name

Computer Security Incident ResponseTeam System and Network Security Division of Muhammadiyah Malang University, abbreviated as CSIRT-UMM.

2.2. Address

ICT of Muhammadiyah Malang University St. Raya Tlogomas No. 246 Malang, East Java

2.3. Time Zone

Malang (GMT+07:00)

2.4. Telephone Number

(0341)464318

2.5. Fax Number

(021)7401727

2.6. Email Address

csirt@umm.ac.id

2.7. Public Key and Other Data/Information Encryption

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

mQINBGIfLPIBEADfw77yHx9+8v+Zf2kHq9jMou06hYsW3uhHzFx/fSUyDerRr9XH
NXBGv82VLBJRkjJh+c4vRht459O9dH1hcvctSr4cLfvClLIG7Jd6aSk9T+PHmuya
yMQCxuOHHKvEJKwFnT17OKL0tLyVgZXxYbAXAj/PTdeseujNu3g3cHjbEPoecHmI
r6kgudZa+YJrmmFeWZ7b5uI64nvXwipk5mOprpKOzP3CflqeMGEA/5AjdD+HROSD
2UvR09U2yacJ1Yt51tTIsbXc6z0iU38YXXC7ynTPj2nxrBa3IPH5BIMCB5Wk5EHD
+CAu6oUt9mnRS8raK2cC1HIfiTencMV+OHKMRzK0Acr3uwR1eBMwrmOfNKqV0Gg7
8aNDY4tISjwpi5/K/xioaRBArkZ09mCIF4bzpSp0zxi5Hq1A6dt9YRKHh/Sft64e
jGM35X/A8Ll+7oQ/W4rhXyDpQCjGXo18fJCOxx6nkARWXkIYCfS94PPnegDxC4bi
oVt92IbGytnnySTRNDNLE2plmAaRX2fhZccsgnm+4aZyfZ0az4aX0zbs76fVnD1j
PNROT7BlILQp19+N4CSY/AODYAIktbTc2t9sP1UKJO2V0NSBTS3JkafgooEoo5ws
LURFp6gOqClFUyuKAu0DPAUEPQZEA83YxD80vtjEPWUw+l4jvZ6TXbtDGQARAQAB
tENDU0lSVCBVTU0gKEdQRyBFbmNyeXB0aW9uIGZvciBDU0lSVCBVTU0gUkZDLTIz
NTApIDxjc2lydEB1bW0uYWMuaWQ+iQJOBBMBCAA4FiEEc7KrKBTJWg0y+JgR7kof
/YGPBqwFAmIfLPICGwMFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQ7kof/YG P
Bqx9YRAAmgOlIX60lLAksVjS3fuea+km0xT8VS8onl0+cq4P5mY5bfoEFOA9G2fg
rb/N5MwZSg8ThToKrFZlvqQoi8bRyfZ+/TLOOO0mpM9Awv5URiAxtQxy9taCsTAn
Ja28ki4ZbBshMDGIKBWKBiqw3Agi8R43nQIwe/zZ6GidCpPRplufBlbOATipqCCL
Qf6ccgGdHsyuW0mMNst4ROO08JiJB3sIBH5Mg9kUySCvmyWbG8p65bLZRQkCvEgM
cAYDkRRHRrr8lZnYB+8JlEvfcZWAvhqcgVPmGts3RLq9g1Qn7pW7PUckVpyxlSGo
LU/r/omlKT49alVz6x1wlBQK8D/EvYM0tHrBVuBClPLB+z3+kuFG/CZ+0XcBr/Be
f1w8gXl0oCPwyjHxBzQQ+B+cYHlZLSVUrWIouuYOOXXSkk/CDqZXZJukycg3Q5nk
+QFApQPzxYONUYDiHCzUAluQIt/SrYtK4D1Kz26Q/bVOdMKCm2gQGhXXcWbW3xuc
htJ+WC/LX6WI/FsrworDCRCM9TGtA0mhmL4yurAnFtx5ssssw1scbboXIGpGk22r
BfhG3U55BRG68mbXeutxh91ZAfz57B5PjqGqmjBtXsbb7PFbkx8ZdixZqUwZfvJj
bPefOW9pccOeOCJkhR+gy9w8CLQUV+55yo2i2XbWT+m2dag2Bm+5Ag0EYh8s8gEQ
ALNFRO/JC5BLwFg4040AvP1CH1C10K+HHTRILoEFxiAX7XbQLec4ywlt0hyBW4ww
3Nwda1SWgO17eGEtLikJjA0JBod/u3L8A5HwzrFE11Odagu4hSUfqoxoBfQLC5JF
OfucsZ2ExCZbncgtyc1VIL9TcWgSBEAGx1TsSHtx6TiU39eIrXQdAdtpeDD1dvob
1hb8UTiINK+4vnBldpUatf0DF53PfEzMe1XsakkVp7cepnERiytPPdCOD7MIDaGj
14JLPSj/JYTsKHEWT9lFyyTwsqAESxwczsrXsKA3ocdb0D8cPisJYowDHv6QC1qL
fcQh4ORdmmSbhueXoseOmGTBEKYbb1YF6OzfIXz4UsbdLse6ib7dXZPO5Kw2/UzI
WLupmcrUmtbILagKm7kBZSp1SZ3loQydHbuJippx0QKNYHRur5I2XcxeOFohIddE
hBgDkDzWew3o19V2qyt04An1pyRuJJpSSSpr5QYaPg/9r1TrFEnypix/jxlr2L9s
oz3IjaOi7lUz6md6AHKZpup0tJIsiu19POq0jP69TQL/nk2vXgmC++3UsWXxihej
PBPMAcJME4hD/66YJc7boT/NnUpusig7zc3FiEDOuTkiou751tsaAbCTie5W9q1e
AXDU7409/D78/8BtgHWog1ic6Js3ClsNFDbhflIV6HXPABEBAAGJAjYEGAEIACAW
IQRzsqsoFMlaDTL4mBHuSh/9gY8GrAUCYh8s8gIbDAAKCRDuSh/9gY8GrNsBD/9S
dE9WBXW8eZXCktd3BZEnmsmpEPzv0ZsscPyzQJ7iaUFJbjoKxOjZjnrwCCnI41Oj
GKjiNlXejudzwNfxXswXEos+ujctk5jXqKyMFP276NmXooY77/BOdkjBRaHTStre
mSpCnkgDUczc8krNbFhKSFWxFBnfhv5NppA+wZytHsk7MPmVQlzaQzHbyMxFOBEp
YXf/AYsVbJ6DpI4W24VeO3MFyzpEDL6Yp4LktIzWiiXYbHtzohFj/FFr4tueDrrd
7GG5PT4CL9pXdSnyIFSC4D0Gqfw6bcCmLYiJHXrF8xKSSkpf/myWS4yKBbaBiDt8
69woC0a9jMO4gEUIHT/2W58pHMcfiE72jQY9s7xSdSLRLAbH83f2RYVxwC/M/gYb
9C+pkJ5xChHBDqpeHulGEXxvuk6Gm3c40hzaaRZloYfmE7t+bzqRSLruj5ITE2kQ
x5L1anWoPGJ8t+VZvBujoeEJ5S6wtIY7ooeimpsCK1V5M4NJdJGYWG2qf6YSoAiS
IiWg+3eNrHq3Ds/3uSEfeKJtf4ZuoXZ2H2dDzDBxUERL6xwIKIRCbfTmT8vaKPYn
cNbZZOY2geB8bYli87BhbzuGMnxbi21Qih7iJIyqaFBb6hTcQdW0LF1WqriZ7DNW
b2zkCJrYtKKgejllGtP+zaLSMpkvX/yKSw1iinR8kw==
=3YtM
-----END PGP PUBLIC KEY BLOCK-----

This File PGP Key is available at:
https://keys.openpgp.org/vks/v1/by-fingerprint/73B2AB2814C95A0D32F89811EE4A1FFD818F06AC

2.8. Team Member

CSIRT-UMM President is the Head of System and Network Security Division and the team members are all staff of the Information and Communication System Substances Division (INFOKOM) from the UMM Work Units.

2.9. Other Data/Information

Not Available.

2.10. Notes on CSIRT UMM Contact

The recommended method to contact UMM is via e-mail at csirt@umm.ac.id or via telephone(0341)464318 to CSIRT UMM which is available 24/7.

3. CSIRT UMM Apropos

3.1. Vision

A vision of CSIRT UMM is the realization of cyber resilience in the education sector that isreliable and professional.

3.2. Mission

The mission of CSIRT UMM, i.e:

1. Coordinating and collaborating on cybersecurity services in the education sectorboth internally and externally.
2. Identifying overall security vulnerability
3. Increasing the security aspect response to all UMM Work Units
4. Increasing the quality of Educational ICT services from cyber threats.

3.3. Constituent

CSIRT UMM constituents include all UMM Work Units.

3.4. Sponsorship/Affiliation

Sponsorship/affiliation of CSIRT UMM INFOKOM UMM to all funding comes fromthe UMM agency budget.

4. The Policies

4.1. The Kinds of Incident and Support Levels

The kinds of incident and support levels of CSIRT UMM has the authority to handle theincidents, as follows:

a. Web Defacement;
b. DDoS;
c. Malware;
d. Phishing;
e. Account Hijacking
f. Ilegal Access
g. Spam

The support provided by CSIRT UMM to the variate constituents depends on the kindand impact of the incident.

4.2. Cooperation, Interaction, and Disclosure of Information/data

CSIRT UMM will cooperate and share information with Other CSIRT from the Ministriesand Institutions in the scope of cyber security. All information received by CSIRT UMM will be kept confidential.

4.3. Communication and Authentication

In the interest of normal communication, CSIRT UMM requires an e-mail addresswithout data encryption (conventional e-mail) and telephone.

5. Services

5.1. Reactive Service

Reactive service by CSIRT UMM is main and priority service, specifically:

5.1.1. Alerting Services Related to Cyber Incident Reports

This service is implemented by CSIRT UMM in cyber incident warnings ofelectronic systems and statistical information managed by each UMM WorkUnit.

5.1.2. Incident Response and Recovery Service

This service is provided by CSIRT UMM in the coordination, analysis, technical recommendations, and assistance of on-site visits of overcoming and recovering cyber incidents. CSIRT UMM provides statistical information related to this service.

5.1.3 Vulnerability Services

This service is provided by CSIRT UMM in the coordination, analysis, and technical recommendations in order to strengthen the security (hardening), CSIRT UMM provides statistical information related to this service. However, this service is valid if the following conditions are fulfilled:

a. Reporters of the vulnerabilities are owners of electronic systems. If the complainant is not the owner of the system, then the vulnerability reportcannot be handled;
b. The vulnerability handling service also can be the follow-up of theVulnerability Assessment.

5.1.4 Artifact Handling Service

This service is provided by CSIRT UMM in handling the artifacts of recovering impacted electronic systems or supporting investigations. CSIRT UMMprovides statistical information regarding this service.

5.2. Proactive Service

CSIRT UMM builds the capacity of cyber security resources actively through the following activities:

5.2.1 The Observations of Notification Related to New Threats

This service is provided by CSIRT UMM in the results of the early detection system of the security monitoring system. CSIRT UMM provides statistical information related to this service.

5.2.2 Security Assessment Service

This service is provided by CSIRT UMM in the identification of vulnerabilities and risk assessment of the vulnerabilities found. CSIRT UMM provides statistical information related tothis service.

5.2.3 Security Audit Service

This service is provided by CSIRT UMM in the information of security assessment. CSIRTUMM provides statistical information related to this service.

5.2.4 Management Service

The Quality of CSIRT UMM Security improved through the following activities:

5.2.4.1 Consultation on the readiness and the incident recovery

5.2.4.2 This service is provided by CSIRT UMM in providing the recommendations of technicalanalysis based on the results of the analysis related to incident response and recovery

5.2.4.3 Building awareness and concern for cyber security

5.2.4.4 In this service, CSIRT UMM documents and publishes various activities carried out thebuilding awareness and concern for cyber security.

5.2.4.5 Construction of the related incident response and recovery readiness.

5.2.4.6 CSIRT UMM prepares a coaching program in the context of supporting incident responseand recovery.

6. Incident Reporting

Cybersecurity incident reports can be sent to csirt@umm.ac.id by attaching at least:

a. Photo/scan of ID card

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

c. According to other applicable provisions

7. Disclaimer

Regarding the malware handling types depending on the availability of the tools they have.