RFC 2350 CSIRT UMM

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi CSIRT UMM berdasarkan RFC 2350, yaitu informasi dasar mengenai CSIRT UMM, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi CSIRT UMM.

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.3 yang diterbitkan pada tanggal 29 Maret 2022.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt.umm.ac.id/csirtummrfc2350.pdf (versi Bahasa Indonesia)
https://csirt.umm.ac.id/csirtummrfc2350-en.pdf (English Version)

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP *Key* milik CSIRT UMM. Untuk lebih jelas dapat dilihat pada Subbab 2.7.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 CSIRT UMM;
Versi : 1.3;
Tanggal Publikasi : 29 Maret 2022;
Kedaluwarsa : Valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Incident
Response Team Divisi Sistem dan
Keamanan Jaringan Universitas
Muhammadiyah Malang disingkat
dengan CSIRT-UMM.

2.2. Alamat

ICT Universitas Muhammadiyah Malang jalan raya Tlogomas No. 246 Malang, Jawa Timur

2.3. Zona Waktu

Malang (GMT+07:00)

2.4. Nomor Telepon

(0341)464318

2.5. Nomor Fax

(021)7401727

2.6. Alamat Surat Elektronik (*E-mail*)

csirt@umm.ac.id

2.7. Kunci Publik (*Public Key*) dan Informasi/Data Enkripsi lain

-----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
oz3IjaOi7IUz6md6AHKZpup0tJIsiu19POq0jP69TQL/nk2vXgmC++3UsWXxihej
PBPMAcJME4hD/66YJc7boT/NnUpusig7zc3FiEDOuTkiou751tsaAbCTie5W9q1e
AXDU7409/D78/8BtgHWog1ic6Js3ClsNFDbhfIlV6HXPABEBAAGJAjYEGAEIACAW
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-----

File PGP *key* ini tersedia pada :
https://keys.openpgp.org/vks/v1/by-fingerprint/73B2AB2814C95A0D32F89811EE4A1FFD818F06AC

2.8. Anggota Tim

Ketua CSIRT-UMM adalah Kepala Divisi Sistem dan Keamanan Jaringan dengan anggota tim adalah seluruh staf Bidang Substansi Sistem Informasi dan Komunikasi (INFOKOM) dari satuan kerja di unit UMM.

2.9. Informasi/Data lain

Tidak ada.

2.10. Catatan-catatan pada Kontak CSIRT UMM

Metode yang disarankan untuk menghubungi CSIRT UMM adalah melalui e-mail pada alamat csirt@umm.ac.id atau melalui nomor telepon (0341)464318 ke CSIRT UMM yang siaga selama 24/7.

3. Mengenai CSIRT UMM

3.1. Visi

Visi CSIRT UMM terwujudnya ketahanan siber pada sektor Pendidikan yang handal dan profesional.

3.2. Misi

Misi dari CSIRT UMM, yaitu :

1. Mengkoordinasikan dan mengkolaborasikan layanan keamanan siber pada sektor pendidikan baik internal dan eksternal
2. Mengidentifikasi kerentanan keamanan secara menyeluruh
3. Meningkatkan respon aspek keamanan kepada seluruh Satuan Unit Kerja UMM
4. Meningkatkan mutu layanan TIK Pendidikan dari ancaman siber.

3.3. Konstituen

Konstituen CSIRT UMM meliputi seluruh satuan unit kerja UMM

3.4. Sponsorship dan/atau Afiliasi

Sponsorship dan/atau Afiliasi CSIRT UMM INFOKOM UMM sehingga seluruh pembiayaan bersumber dari anggaran instansi UMM.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/*Level* Dukungan

4.1. Jenis-jenis insiden dan tingkat/level Dukungan CSIRT UMM memiliki otoritas untuk menangani insiden yaitu:

a. Web Defacement;
b. DDoS;
c. Malware;
d. Phishing;
e. Pembajakan akun
f. Akses Ilegal
g. Spam

Dukungan yang diberikan oleh CSIRT UMM kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

CSIRT UMM akan melakukan kerja sama dan berbagi informasi dengan CSIRT dari Kementerian dan atau Lembaga lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh CSIRT UMM akan dirahasiakan..

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, CSIRT UMM dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon.

5. Layanan

5.1 Layanan Reaktif

Layanan reaktif dari CSIRT UMM merupakan layanan utama dan bersifat prioritas, yaitu:

5.1.1. Layanan pemberian peringatWan terkait dengan laporan insiden siber

Layanan ini dilaksanakan oleh CSIRT UMM berupa pemberian peringatan adanya insiden siber pada sistem elektronik dan informasi statistik yang dikelola oleh masing-masing satuan kerja UMM.

5.1.2. Layanan penanggulangan dan pemulihan Insiden

Layanan ini diberikan oleh CSIRT UMM berupa koordinasi, analisis, rekomendasi teknis, dan bantuan kunjungan ke lokasi dalam rangka penanggulangan dan pemulihan insiden siber. CSIRT UMM memberikan informasi statistik terkait layanan ini.

5.1.3. Layanan penanganan kerawanan

Layanan ini diberikan oleh CSIRT UMM berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (*hardening*), CSIRT UMM memberikan informasi statistik terkait layanan ini. Namun, layanan ini hanya berlaku apabila syarat-syarat berikut terpenuhi:

a. Pelapor atas kerawanan adalah pemilik sistem elektronik. Jika pelapor adalah bukan pemilik sistem, maka laporan kerawanannya tidak dapat ditangani;
b. Layanan penanganan kerawanan yang dimaksud dapat juga merupakan tindak lanjut atas kegiatan *Vulnerability Assessment*.

5.1.4. Layanan penanganan artefak

Layanan ini diberikan oleh CSIRT UMM berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdempak ataupun dukungan investigasi. CSIRT UMM memberikan informasi statistik terkait layanan ini

5.2. Layanan Proaktif

CSIRT UMM secara aktif membangun kapasitas sumber daya keamanan siber melalui kegiatan:

5.2.1. Pemberitahuan hasil pengamatan terkait dengan ancaman baru

Layanan ini diberikan oleh CSIRT UMM berupa hasil dari sistem deteksi dini sistem monitoring keamanan. CSIRT UMM memberikan informasi statistik terkait layanan ini.

5.2.2. Layanan security assessment

Layanan ini diberikan oleh CSIRT UMM berupa identifikasi kerentanan dan penilaian risiko atas kerentanan yang ditemukan. CSIRT UMM memberikan informasi statistik terkait layanan ini.

5.2.3. Layanan security audit

Layanan ini diberikan oleh CSIRT UMM berupa penilaian keamanan informasi. CSIRT UMM memberikan informasi statistik terkait layanan ini.

5.2.4. Layanan Manajemen

Kualitas Keamanan CSIRT UMM meningkatkan kualitas keamanan melalui kegiatan:

a. Konsultasi terkait kesiapan penanggulangan dan pemulihan Insiden
b. Layanan ini diberikan oleh CSIRT UMM berupa pemberian rekomendasi teknis berdasarkan hasil analisis terkait penanggulangan dan pemulihan insiden
c. Pembangunan kesadaran dan kepedulian terhadap keamanan siber
d. Dalam layanan ini CSIRT UMM mendokumentasikan dan mempublikasikan berbagai kegiatan yang dilakukan dalam rangka pembangunan kesadaran dan kepedulian terhadap keamanan siber
e. Pembinaan terkait kesiapan penanggulangan dan pemulihan insiden
f. CSIRT UMM menyiapkan program pembinaan dalam rangka pendukung penanggulangan dan pemulihan insiden

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@umm.ac.id dengan melampirkan sekurang-kurangnya :

a. Foto/*scan* kartu identitas
b. Bukti insiden berupa foto atau *screenshot* atau *log file* yang ditemukan
c. Atau sesuai dengan ketentuan lain yang berlaku

7. Disclaimer

terkait penanganan jenis malware tergantung dari ketersediaan *tools* yang dimiliki.