

RFC 2350 UMMETRO-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 11 Agustus 2023.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk informasi pemberitahuan RFC 2350.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada:

<https://csirt.ummetro.ac.id/rfc2350-csirt-ummetro.pdf> (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGPKey milik UMMETRO-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 UMMETRO-CSIRT;

Versi : 1.0;

Tanggal Publikasi : 11 Agustus 2023;

Kedaluwarsa : valid hingga dipublikasikanya dokumen terbaru.

2. Informasi Data/Kontak

2.1. Nama Tim

Tim Tangap Insiden Siber (TTIS)/CSIRT Universitas Muhammadiyah Metro
Disingkat : UMMETRO-CSIRT.

2.2. Alamat

Kampus 1 Universitas Muhammadiyah Metro
Jl. Ki Hajar Dewantara No.116, Iringmulyo
Kec. Metro Tim
Kota Metro
Lampung 34381

2.3. Zona Waktu

Kota Metro (GMT+07:00)

2.4. Nomor Telepon

0725-42445

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

Tidak ada.

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

csirt@ummetro.ac.id

2.8. Kunci Publik (*PublicKey*) dan Informasi/Data Enkripsi lain

ID : 0x1E53BA595869AEA6

KeyFingerprint : 040151952F126BD6EFEDE6641E53BA595869AEA6

Blok PGP Public Key :

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

```
xsDNBGTWAdYBDACYFj+7skYAgSfl3B/WD3llCzi5abhLCJsHRptmUI/4yo98Zxrl
ck7f/7D8ddzTzjgyC5yURyVfmbOm2wpsQdeaf5yiw1ZxB0C7Bz8tlvQTIIs+vQRmz
YgSwPK4cUE8I338g+8XxWeb8ioQ0Sze4+4CJB0cKe7AZJD0/NoclYrjFf3UMm0+
O
bD6dURVVaT0K8CISOQgJ1w++LBn24AAv772Hd9o59DLmFTNevKLLPjH/+zwrf+i
A
mwA06cl6fc7/CooT6qA5YnFPLY3HMeovuqJytqO8WcjlHy2Fi5B9gcYfHDIf+rco
YMcjrDqsNz2RSCqel6wWolfcMysmsreiahChfVyfLmlLasui/+dFI4i2DmkfqTx4
1s5SPc0UXVL5tJCbq1x/E8ZKxbC7yu0zQHx361q8Qaon2klUBrANBAosnmWAwC
7I
Teg9SRLWCy3ceMFclSx4elmLo9pvNruedwp3G4U0zMcGtTRYxCcH6MP4VT8Qjvj
u
2A3DIJtjNg4xb0AEQEAAc0jVU1NRVRSy1DU0ISVCA8Y3NpcnRAdW1tZXRyby
5h
Yy5pZD7CwQ0EEwEIADcWlQQEAVGVLxJr1u/t5mQeU7pZWGmupgUCZNYB1wU
JBaOa
gAlbAwQLCQgHBRUICQoLBRYCAwEAAoJEB5TullYaa6melgL/0ivOuyIcm07Bd2
G
F8bTEXwno65j3UaeYfOAqDKnkqjWUDcSq9WJcb+xolkoOfjDk2x0Nt3MeE3WauY
X
gF3nu6DK+49DErJT57s9UIHFk9mxRibGo8nyLWI9Hv5BddlrS3PqDSfZos7WhJ5Y
ijq2a8kzr0x7USmtRoPBZStWeoCS6ojVeTMrp3MePJK305739VZf9NEO0nM3nLY8
DAtsvwTde4UK8QvS19rJWGO+sLbtNai/5Mkvw3p8oQM/x+sybQWle3FJuwdeIS4o
LYdsfEgR3+naWI8dLYclyFKFPzErwqbuzyEHvQl3Ppk7SMvs6J8IEBncAL5j+iXr
crWu+pzJ3y7e1gJmE6fggc069YlXDkIlSr35s8GDxsLgCK2dHJMqDdbFJqS65I0w
fvmRA21Pj3RXC8aWO9HljopdvqJbpMPW8o4AQrdLpFkhUkCARCcx2tps3FPnl862
JM/ujS1fEfaZ9KQTN8iVnYPTXdh2mARv2/0HZX24s3O2jZjID57AzQRk1gHYAQwA
1lqoRw/hcrh/xvNsRPvd0LTLVT/r7fd2v/XZi4UpZZjL8/+7gyZEbPXYD9QCsYtv
DZ3iQz+9qSac3bzyxHOZ+0LAzJQy5qKGD2NfhCNGQlhYeT6/Q0G5N9u52tKZuc
G3voidgV2udsoluE3mzrzrvkhXbfYB9GK23ljEylr8HbYdXo9Bj1RbLm/CWj5+
09Hq0UmMA94rydq4lkcSzOdd4dlthNqG7VNc8gx3wcq0xeZBsQR6EOtwRveKZVm
A
```

```
urGmGdWxHbB5dfmczg2MJL8zcuL2271ZDikBkKMOUKfm5Zxujg9fbKJzZoRM99b
K
gX+JScyi3GfJ2m2y/VrQIYFbcNt17kiuVDApzQffknAsmQGO4hE27GPVYJfNktTV
6RP2IAqjIA6eHH3Yjl+u1muqdKnILWnu35xdrWsudvKq1CST5gw0S57pOXaAPjl
CtXCZBGauU6XeeFt/vZKKWIHnxuzvT3p1eiGyGTAj8LIT/lmohQ/DR//V9B9wBJX
ABEBAAHCwPwEGAEIACYWIIQQEAVGVLxJr1u/t5mQeU7pZWGmupgUCZNYB2
QUJBaOa
gAlbDAAKCRaE7pZWGmupkGRC/9P8P8rghW31TJA9RlcX8vvq1qd9u7y9k542+
AA
WTusVxtzLptv/+FaQ23frMwoU6mbRBwSs75sSe/pylW4RXkbYkUd4ETn0RjgNGA
J
ouOi8ZVIQ1dnZk3WXQr8vlkEFza8V9481T5qd+gB4GREgyHF7WAZGohvUc6hC8z
K
ypPGzraltextfiJs14I4+Nq0daolyYwammL9eIEN9SX2xuCDURZ6olamsJEYI402a
AS3pVVxMFNO5CYt4FzuzZowHgVXu+H8jAp/xDSuH7uQu5wAvc8gsPzG/sX4inka
N
JdmHN5JYURZ3tvhvLXbt6f7hBtWwMDphlzXHkwSqDZmcetWun7DrZvFHpGZ9Ug
sd
NNp5QTyjW7KoqvVTsgqMhK6+l36z+MWJE/zJP7wwHaFqtGOcNccFg3J8usWYTE
Ak
NOQwFMqzZuggQ5wbGqAsm64HsYZz3JHWQqVbJjEs/Bv1ZTusoCvyKcRLbTbh16
q3
y7fIMJiGZO4UbDZ1bhVTucukfRE=
=M7v6
-----END PGP PUBLIC KEY BLOCK-----
```

File PGP key ini tersedia pada :

<https://csirt.ummetro.ac.id/publickey-csirt-ummetro.asc>

2.9. Anggota Tim

Ketua UMMETRO-CSIRT adalah Kepala Unit Pelaksana Teknis Pusat Teknologi Informasi dan Komunikasi Universitas Muhammadiyah Metro. Yang termasuk anggota tim adalah seluruh staff baik dosen dan karyawan Universitas Muhammadiyah Metro, serta personel tambahan dengan kompetensi yang diakui secara nasional dan/atau internasional.

2.10. Informasi/Data lain

Tidak Ada.

2.11. Catatan-catatan pada Kontak UMMETRO-CSIRT

Metode yang disarankan untuk menghubungi UMMETRO-CSIRT adalah melalui e-mail pada alamat [csirt\[at\]ummetro\[dot\]ac\[dot\]id](mailto:csirt[at]ummetro[dot]ac[dot]id) (csirt@ummetro.ac.id) atau melalui nomor telepon 0725-42445 pada hari Senin hingga Jumat dan jam kerja Universitas Muhammadiyah Metro pukul 08:00 hingga 15:00 WIB.

3. Mengenai Gov-CSIRT

3.1. Visi

Visi UMMETRO-CSIRT (Universitas Muhammadiyah Metro Cyber Security Incident Response Team) atau Tim Tanggap Insiden Siber adalah menciptakan lingkungan

siber yang aman, tahan terhadap ancaman, dan responsif terhadap insiden, dengan tujuan melindungi aset digital, data sensitif, dan reputasi organisasi. Visi ini bertujuan untuk menjadi garda terdepan dalam menghadapi tantangan insiden siber dengan profesionalisme, kecepatan, dan ketepatan.

3.2. Misi

Misi dari UMMETRO-CSIRT, yaitu :

- a. Tanggap Cepat: Memberikan respons cepat dan terkoordinasi terhadap insiden siber untuk meminimalkan dampak negatifnya.
- b. Deteksi Dini: Mengembangkan mekanisme deteksi dini yang kuat untuk mengidentifikasi ancaman siber sebelum mereka berkembang menjadi insiden besar.
- c. Kolaborasi: Berkolaborasi dengan departemen internal dan eksternal untuk berbagi informasi dan pengetahuan tentang ancaman siber.
- d. Pendidikan Keamanan: Memberikan pelatihan dan kesadaran kepada karyawan agar dapat mengenali dan menghindari ancaman siber.
- e. Analisis Mendalam: Melakukan analisis terperinci terhadap insiden untuk memahami sumber masalah dan mencegah insiden serupa di masa depan.

3.3. Konstituen

Konstituen UMMETRO-CSIRT meliputi seluruh unit kerja dalam lingkungan Universitas Muhammadiyah Metro.

3.4. Sponsorship dan/atau Afiliasi

Seluruh pendanaan UMMETRO-CSIRT bersumber dari anggaran Universitas Muhammadiyah Metro.

3.5. Otoritas

- a. Investigasi Insiden: Menganalisis dan menyelidiki insiden keamanan siber untuk mengidentifikasi penyebab, dampak, dan metode serangan.
- b. Koordinasi Respons: Mengoordinasikan upaya respons insiden dengan berbagai tim internal dan eksternal yang terlibat.
- c. Penanganan Darurat: Mengambil tindakan darurat untuk menghentikan insiden yang sedang berlangsung dan melindungi sistem serta data.
- d. Komunikasi Eksternal: Berkomunikasi dengan pihak eksternal seperti media, pihak berwenang, dan mitra bisnis terkait insiden yang terjadi.
- e. Rekomendasi Keamanan: Merumuskan rekomendasi untuk meningkatkan keamanan dan mencegah insiden serupa di masa depan.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

- a. Web Defacement;
- b. Distributed Denial of Service (DDOS);
- c. Malware;
- d. Pembajakan akun;
- e. Akses ilegal;

f. Spamming.

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

UMMETRO-CSIRT akan melakukan kerja sama dan berbagi informasi dengan CSIRT dari kementerian dan/atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh UMMETRO-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, UMmetro-CSIRT dapat menggunakan alamat email tanpa enkripsi data (email konvensional) dan telepon. Namun, untuk komunikasi yang mengandung informasi sensitif, terbatas, atau rahasia, UMmetro-CSIRT akan menggunakan enkripsi PGP pada email (sesuai dengan subbab 2.8).

5. Layanan

5.1. Layanan Utama

Layanan utama dari UMMETRO-CSIRT yaitu:

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh UMMETRO-CSIRT untuk memberikan informasi dan peringatan akan adanya insiden siber kepada pemilik atau pengguna sistem elektronik dan informasi statistik yang dikelola oleh satuan-satuan kerja dalam Universitas Muhammadiyah Metro.

5.1.2. Penanganan Insiden Siber

Layanan ini diberikan oleh UMMETRO-CSIRT berupa koordinasi, analisis, dan rekomendasi teknis, serta bantuan on-site dalam rangka penanggulangan dan pemulihan insiden siber.

5.2. Layanan Tambahan

Layanan tambahan dari UMMETRO-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini diberikan oleh UMMETRO-CSIRT berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (hardening). Layanan ini hanya berlaku apabila memenuhi syarat-syarat berikut:

- 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.

5.2.2. Penanganan Artefak Digital

Layanan ini diberikan oleh UMMETRO-CSIRT berupa penanganan artefak digital dalam rangka pemulihan sistem elektronik terdampak atau dukungan investigasi atas insiden siber.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini diberikan oleh UMMETRO-CSIRT berupa informasi statistik hasil deteksi dini sistem monitoring keamanan siber atau informasi dari tim CSIRT kementerian atau organisasi lain yang perlu diwaspadai oleh para pengguna sistem elektronik.

5.2.4. Pendeteksian Serangan

Layanan ini diberikan oleh UMMETRO-CSIRT berupa informasi statistik hasil pendeteksian dan monitoring keamanan siber.

5.2.5. Analisis Risiko Keamanan Siber

Layanan ini diberikan oleh UMMETRO-CSIRT berupa laporan hasil analisis dan identifikasi kerentanan serta penilaian risiko terhadap kerentanan yang ditemukan.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan ini diberikan oleh UMMETRO-CSIRT berupa pemberian rekomendasi teknis berdasarkan hasil analisis atas risiko kerentanan yang ditemukan terkait penanggulangan dan pemulihan akibat insiden keamanan digital.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini diberikan oleh UMMETRO-CSIRT berupa informasi dan publikasi berbagai kegiatan yang dilakukan untuk membangun kesadaran dan kepedulian terhadap keamanan siber.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke [csirt\[at\]ummetro\[dot\]ac\[id\]](mailto:csirt[at]ummetro[dot]ac[id]) (csirt@ummetro.ac.id) dengan melampirkan setidaknya::

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

7. Disclaimer

UMMETRO-CSIRT bertujuan untuk membantu proses penanganan insiden keamanan siber di lingkungan Universitas Muhammadiyah Metro. Namun, kami perlu menegaskan bahwa dalam kasus insiden di luar kemampuan kami, kami akan melakukan koordinasi dengan layanan dan pihak eksternal seperti CSIRT nasional dan lainnya. Layanan kami bukanlah pengganti dari dukungan eksternal yang mungkin diperlukan dalam situasi tertentu di lingkungan Universitas Muhammadiyah Metro.