RFC 2350 UGM-CSIRT

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi CSIRT UGM berdasarkan RFC 2350, yang menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi CSIRT UGM.

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 17 Juli 2023.

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.ugm.ac.id/rfc2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen telah ditandatangani secara digital oleh Ketua CSIRT UGM sesuai dengan sub bab 2.10.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 UGM-CSIRT;
Versi : 1.1;
Tanggal Publikasi : 17 Juli 2023;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Incident Response Team Universitas Gadjah Mada
Disingkat : CSIRT UGM.

2.2. Alamat

DTI Universitas Gadjah Mada
Rumah Dinas E1 Bulaksumur, Sagan, Caturtunggal, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55281

2.3. Zona Waktu

Yogyakarta (GMT+07:00)

2.4. Nomor Telepon

(0274) 515660

2.5. Nomor Fax

(0274) 515664

2.6. Nomor Helpdesk (Whatsapp)

+62 811 2826 543

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

csirt@ugm.ac.id

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

Komunikasi melalui email dapat menggunakan PGP. Adapun public key CSIRT UGM adalah sebagai berikut:


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBGPr+KsBEADIp3BbKlwJG1iHp/AifLs4y96ms6wCdHIXfiV3lAJjF3TQzB8H
nh0GM8TYdWutuU5vG31ItvX7sB0acK9e81IwAxN0G6SHClcdpfMt4y6etm5/lIzL
OSRCBpHHU/FcDrLaOfTUqvMRFokZFR0Phg4Oq+RopeiDfzz8cEBU5npeKzyjl7ss
NihOHNbcfST8u9XPm9XBRvzzk8c8Rm3r2nh8zft1Nb7ezlEJV4FM6d/GDRmyGBUr
1Htf0HWbuk5ZycbjPruTdKfqWJZaQgh6CCKChEsm7Hn2lfe4vkccmP3c3tN/fteN
46a5Z/DZpI6MkzcA3w7Q4QLxcB1U7bV10sq2irj1UuOcv48Nv7r32NFaJbcTLE3+
WTYCx4AXmv1vpP+H/no/QyfW4o9yfU5qM/ybyvAsKog6ZGb7JPPgoUqnzsIJrMgX
aAdIqGCns+dEScaP8VV48DyjN+nh/SY9KQMkHwK0MzJ5Xb+4DieAfseIvvXePJxv
NWTIXCr82my267jGoapgKapbKcruXlRIgNVRk0xdX/vqo/RY3R0yVgA8XOp4spQx
GaRPmZxguatIuqut8XEG4pU70vAGCA5MAEL0sxoujEbkamQ4ojHMkQBh7m4W4EK8
GxX5yg6Ya9sLzuChbVHxShRaiv2k87v4MTBqH5hnWLn8BqaBXOSMYbwq/wARAQAB
tBtjc2lydC1yc2EgPGNzaXJ0QHVnbS5hYy5pZD6JAlcEEwEIAEEWIQRWxgWzuyk/
CGp/b63f3mFgIsnROQUCY+v4qwIbAwUJA8QmpQULCQgHAgIiAgYVCgkICwIEFgID
AQIeBwIXgAAKCRDf3mFgIsnROfPGD/9hzkPoR2aTbwckuwBKtrCgOUqd7+75+SIs
E1F+EWJOQJet1HLCktMmOlg7alv5YQSnN6wbT8hrFoc4mmsKpg0Z5oY6dwhIIOdf
VY4WlTB+er+KwcpbUEr+MWLc/Iga8eeIV3fIUXaQnXRSwZiSgSZ9mWjKPPbTFPLB
tJE5GT4k5RQAv5VjSD6d2d9J8mw1HnbHsoGe3j0Vmu5h8CcRvJ3e6/9ueKaupsCN
/ZRrMY50nt/cAlDb1uQJtiIpNKlyq4d/6Fsl64km+V2IyEkrbXMsH+HMTB9caweI
J49AeTi7pTBsmIiynB7nOhSagX1dTOFBE7rbgvTd5D8zR1y1CK/bA3Wbb7RdesTb
Y+fHMbvDYqLKj80CqFrW1sYXOKhZTz6Vjnrlfbgme JFiuwU/bngZrigjOnGuj3fK
3+PiYjb3jiG6YqAPUlPVkZTdKPlYwJY1sUKZo+jGRkU5Srzi2v6t9ubm2FHrAgov
LMkIS2Wk/cBDkMf6dRcVHJbRThfKsgg+E4tqaOTE9pTdyptQtdgg9di8AqQ3G5lq
ugFAdTTPy/k2pTn0J/HXTff9w5WHmSwCJPMUEAfWrVNGnXyXAtfoyXvLjo2LsvSD
10QXhZN0DFYKJ97uu030hKqEYSpz6H77LGD5rof0Nj0nk8476MjVyIK5vHoIrEtb
jHQrYxH0LLkCDQRj6/irARAAvSE7lcUFTaeKZfOoXUSBd6od/XNq8pKNBFMeysm2
hpNd3NRPvWfKRJnJD16plF5CnIThT60hJjNVLcU5ILgQaeps4MfdE2ywm8od0hE9
tGqUiU+1KxvYszoxbwonXBrsqeE84urLgsV9j/wgfOiI1gxPB5KpCDabplEDOZkz
Ek5Jvhx7Nnua9NbfWia7I/CUDu1xmGDY6woWCbZZz24loueFU1VMDJf4E/UkYh/B
uOQeUasm4Lqt9ZAqJxiHM4sDzHtR0oUmlepwiDgUEnLR6YZKSyNAv+dsouTJev05
43umJVr0Tkdsb4oe+X3A+Wcgx3Y8whIhZW/Pdknq/hAOBlg/tdjBEZ5yXdHiXDuc
+L++xrDuFiUBz6g2nteQPe3xvkUGl7e6shZCMJsl4TsrvGRnIwpQmXLeJUA73IvA
```

```
IJDTd3CgBHv9xOB+HMU+c53tAWBOnOCA1F8MY6dym4QyrjLRPuHWociSO+HBKfhF
7FBSdeiC0f0EzAKL+DjXZNNbsKoM4AGwB4hQ+Ae5ye7V5JsHXbFWHoswKtLCVMzD
G4qOexxtTRQr1lZxlEwJcqWmrNKS0H9/JBY10gi6uvpCJowg7DqhB9ThhSjFk13F
6wdI0tFYJRdD1C/R2QSj1wrvXJr69N/RpKdOMwmDNStCJX8AwBofo5IU9n+hn1hQ
0REAEQEAAYkCPAQYAQgAJhYhBFbGBbO7KT8Ian9vrd/eYWAiydE5BQJj6/irAhsM
BQkDxCalAAoJEN/eYWAiydE5+VQP/jeeKRvUsYXSX8fZXUWdt08UY2U65MCCW3rf
lph985hqSTG/6NTmNGn75CyfBrDPzGq02ZFKZgi5lvvEhufniJ4CBEh0jwJ62vh1
epAXRQUWXZZWK3+91VGBFOmwvqGrkcNm1cBD5ehdXQ5YritOi0r75ZnDBbIRHeSz
sD3naArWheUm+7/FXzQvtWSYlUqc5XHZzRyOPPS6k++aiJ3ipXZLB0Ngl3oO4EJd
pnVfj7GleXp/Q3fjlQIWZAkCmEJZQZMjgkA2dKSXMzDa6d8x+Vs514rN0Qaxw/O6
10oEgfi9xZEWelzreRcJzBdsaYFZqcNRYLiCinqnMKtcUHF+AJVRP2DXBd70hDej
oI1z9MKgmYYxygAfssm2Xh1CWLkf3qiCWErTj5LzKwjZ9wx9c6MT4aTWYPpaKBbb
aRGkNk3e7gzcBJzyRJ2v0ktbqCtsrnVoQZdwtlqrxQpNiarSOyJTYaTC08w4jrli
jmNIVSyqFdB/rB1D8ZIBIcCFQszVeF7DBE0uZWjSqDF6nh26oyUV/yy3Os0SFf7A
ZXlxATsQKLujukVjPw1/9CL0SFgqyzwin3WE7pnNgi/w7qyV77MLQfI3oMxNRYgT
dy/+c5FfG0hfyL1w0IGO2eyap0GR6uSCQ0pFaS+3kbSCfzk9+zrBJnrDvmu/mt4V
RMq4APJi
=HoP1
-----END PGP PUBLIC KEY BLOCK-----
```


File PGP key ini tersedia pada :
http://csirt.ugm.ac.id/keys/publickey.asc

2.9. Informasi/Data lain

Tidak ada.

2.10. Anggota Tim

Ketua CSIRT UGM adalah Direktur DTI dan anggota tim CSIRT UGM adalah semua staf di Sub Direktorat Infrastruktur dan Keamanan beserta perwakilan semua Sub Direktorat di DTI UGM.

2.11. Catatan-catatan pada Kontak UGM-CSIRT

Metode yang disarankan untuk menghubungi CSIRT UGM adalah melalui e-mail pada alamat csirt@ugm.ac.id atau melalui helpdesk WA di nomer +628112826543. Dapat juga menghubungi melalui nomor telepon +62 (274) 515660 bagian data center pada hari kerja jam 07.30 - 16.30 WIB.

3. Mengenai UGM-CSIRT

3.1. Visi

Terwujudnya ketahanan siber yang handal di lingkungan Universitas Gadjah Mada

3.2. Misi

Misi dari UGM-CSIRT, yaitu :

a. Mengkoordinasikan dan mengkolaborasikan layanan keamanan siber di Universitas Gadjah Mada baik dengan pihak internal maupun eksternal;
b. Mendorong kegiatan pengamanan informasi dan pencegahan insiden keamanan informasi;
c. Membangun kesadaran keamanan siber pada sumber daya manusia di lingkungan Universitas Gadjah Mada.

3.3. Konstituen

Konstituen CSIRT UGM yaitu semua unit kerja di lingkungan Universitas Gadjah Mada.

3.4. Sponsorship dan/atau Afiliasi

CSIRT UGM merupakan bagian dari DTI UGM, sehingga pendanaan berasal dari RKAT UGM.

4. Kebijakan – Kebijakan

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

CSIRT UGM menangani insiden keamanan sebagai berikut:
a. Web Defacement;
b. Web Hacking
c. DDoS;
d. Malware;
e. Phising;
f. Pembajakan akun;
g. Akses ilegal
h. Spam

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

CSIRT UGM akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh CSIRT UGM akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, CSIRT UGM dapat menggunakan email tanpa enkripsi data (email konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada email.

5. Layanan

5.1. Layanan Utama

Layanan utama dari UGM-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik yang dikelola oleh masing-masing unit kerja di lingkungan Universitas Gadjah Mada.

5.1.2. Penanganan Insiden Siber

Layanan ini berupa koordinasi, analisis, rekomendasi teknis, dan bantuan on-site dalam rangka penanggulangan dan penanganan insiden keamanan siber di lingkungan Universitas Gadjah Mada.

5.2. Layanan Tambahan

Layanan tambahan dari UGM-CSIRT yaitu :

5.2.1. Penanganan Kerentanan Sistem Elektronik

Layanan ini diberikan berupa pemeriksaan kerentanan pada perangkat lunak maupun perangkat keras di lingkungan konstituen, serta melakukan proses verifikasi kerentanan yang mungkin dieksploitasi dengan tujuan menyusun rencana untuk memperbaiki kerentanan yang teridentifikasi.

5.2.2. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini berupa penyampaian informasi kepada konstituen terkait ancaman terhadap sistem elektronik yang dapat muncul akibat pengaruh dari perkembangan teknologi, politik, ekonomi, dan perkembangan lainnya.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini berupa kegiatan analisis data dalam rangka melakukan deteksi serangan terhadap Sistem Elektronik.

5.2.4. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini berupa kegiatan diseminasi di bidang keamanan siber kepada konstituen yang bertujuan untuk memberikan pemahaman tentang bahaya yang terdapat di ruang siber dan cara mengatasinya.

6. Pelaporan Insiden

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

a. Identitas pelapor
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan

7. *Disclaimer*

Penanganan insiden tergantung dari ketersediaan *tools* yang dimiliki oleh Universitas Gadjah Mada.