RFC 2350
UNISAYogya-CSIRT

UNIVERSITAS ‘AISYIYAH YOGYAKARTA

Kampus Terpadu:
Jl. Siliwangi (Ring Road Barat) No. 63 Mlangi, Nogotirto, Gamping, Sleman, Yogyakarta. 55292 Telepon: (0274) 4469199 Fax.: (0274) 4469204
Email: info@unisayogya.ac.id

RFC 2350

UNISA Yogyakarta *Cyber Security Incident Response Team*

UNIVERSITAS ‘AISYIYAH YOGYAKARTA

2022

disusun oleh:

UNISAYogya-CSIRT

Badan Pengembangan Teknologi dan Sistem Informasi

Kampus Terpadu:
Jl. Siliwangi (Ring Road Barat) No. 63 Mlangi, Nogotirto, Gamping, Sleman, Yogyakarta. 55292 Telepon: (0274) 4469199 Fax.: (0274) 4469204
Email: csirt@unisayogya.ac.id

1 Informasi Mengenai Dokumen

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

1.1 Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 16 September 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.unisayogya.ac.id/rfc2350.pdf (versi Bahasa Indonesia)

1.4 Keaslian Dokumen

Dokumen telah ditanda tangani dengan sertifikat SSL milik UNISAYogya-CSIRT, untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 UNISAYogya-CSIRT;
Versi	: 1.0;
Tanggal Publikasi	: 16 September 2022;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan

2 Informasi Data/Kontak

2.1 Nama Tim

Universitas Aisyiyah Yogyakarta-*Cyber Security Incident Response Team*
Disingkat : UNISAYogya-CSIRT.

2.2 Alamat

Jl. Siliwangi (Ring Road Barat) No. 63 Mlangi, Nogotirto, Gamping, Sleman, Yogyakarta. 55292

2.3 Zona Waktu

Yogyakarta (GMT+07:00)

2.4 Nomor Telepon

+62 895-2940-5592
(24/7)

2.5 Nomor Fax

(0274) 4469204

2.6 Telekomunikasi Lain

-

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

csirt@unisayogya.ac.id

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

2.8.1 Ketentuan

a *Digital Signature* diutamakan menggunakan SSL dan apabila tidak bisa, maka menggunakan PGP

b Enkripsi pesan *email* menggunakan PGP

2.8.2 Kunci Publik

- ☐ Installer *dan* Downloader kunci publik di Windows https://csirt.unisayogya.ac.id/RootUNISAYogyaInstaller.bat
- ☐ Panduan Penggunaan dan Validasi *Digital Signature* https://csirt.unisayogya.ac.id/CaraValidasiDigitalSignature
- ☐ Panduan Pertukaran Pesan Terenkripsi https://csirt.unisayogya.ac.id/EmailDenganPGP

a PGP

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

xsDNBGMa3soBDAC/h6B4FD3AR50a6/ALbLqd10tXLWd9SQ2XkTe4kuDGjL+MUJoc
9ERcr2dNZ9UVjeSIjUVZwdGfawxuhMpFlfQF5Z27jVSrNfWJv4Q4lFShYY8CQ+w4
XGh44B3qygFdUxEwwD86DcBBAqQyN9vqpkF3ynu/X0vyle36tqwXZVZinNM5UtuU
mB8U7wHmc8ijbZtMqaxUi8RHu1lKdcSTyrGYpPbrOWvDA/YCaGLx6jjZFcMjc+tG
xWezMW1RbwwyeHtjWqJMRvx2Tgygjh9RiijAV30/SNtU69go3zebGryqpFyB6Mwu
r5nRrBBiij7d3ALvcHo1og0RjH8Wve9VY71eJp83YhV28+5yXHUuLWJCrJAZK2H7
yrPEYTJSnpJP7X4TYutqcjfiFqd9nvOF+EWZgeudUhwSgwT9vQJnNG88PgNr2IJR
YdOiQbIa7Gos5rS16UmXpODoeaRHYh0kHuqhsMQ4/5arsSOcw9wEhuJ3sQebhwKY
hbaCJmDr4h8+gUkAEQEAAc0pVU5JU0FZb2d5YS1DU0lSVCA8Y3NpcnRAdW5pc2F5
b2d5YS5hYy5pZD7CwQ0EEwEIADcWIQQD0sLfkwCWDtAm6v5S7Ka8jwaikQUCYxre
zAUJEswDAAIbAwQLCQgHBRUICQoLBRYCAwEAAAoJEFLspryPBqKRh30L/REfR1OE
UGjobr2zBcxl2qUOGULKI5fukShSp8RvTiJpStCq+6MwglOTNkeU17JK3PFUZSVS
5gydMOJoTNkFhRU7o19cIU9kYWWixgrS/tFHe8o1cDc2xaaO6X768XbQpiR0lY+T
QXWdpuVB7+279JXgq+ODpqjCRYZ8j+4a2nTj5po54AtGA5CPLdnpt4c7+8NHNybq
dlYtwvc+rk78zbBocknKQhygoMFMAgvWdbSde8FDaL1xJ0A6JcFys5/Q96x7Zw8g
9YdwqqHMZkE6XWnmxRxzeIL6KqCUU2zaNihy8vGJMqm3dicQITvUapTZmRHwis4Z
ldXFey2VNaYOuXwkt/3G/QfjrotPrYVX+Bx2jWRRHntUwaUetENFlrh6/0TSFgVY
G4wdLCaqLQRnqyrbv8ciWADSGzq3DR3Y3mI7W/eK1NdCLUt/S10/o8SjdEdPmcVU
xJmsMJUJqehzcHZPJ0AeJy2BzfZd6PHwUvsmXX0XMWKRhY+pjryB7fVZp87AzQRj
Gt7MAQwAqBHpX4nGWKt5hvsx/2RexQ7kNflkVM+R7PXYqwsWtWAywuvPcLUWnmcY
Lw2/oT2XBgdcEovYYbR1Ckxz1wLj6bpup1C72UyyRO8ZOL6whYU83WyRVl8NELka
jV54SPolTZJ7UPI7JYBCt8omp6KaHilED/qGjU2wie3BsgptFAUY3aXQurFpn8Ms

amRrfeCqjmZI7KMS4ohIIydsZgOWo6SJeudHYnhK6DXfqTupRZN5Ycr6kVCVbqkO
HpWF6SpDJyguclOakVb04mb9cK02N5kIRxv2D3O6B46Ws6vTk1JUZ0Kyrcles+d0
tOXEjvNfs4UwHkgUcFr58g//dNfUgMxzPgmOG3MKrJebZo3nvhBVqwdi0nDH7Gxr
CC+Tpase0N13/KWbkgxZVflTkSkh3NFbzEFfNq9ZFsyXo6qhFMPOQwXa9xj8CY8H
VgKFccXY1tp8Mou9agy5jQltW57las3klsHXk21nw4v8fh/85S1UKcu5AQR9MMsY
SQPrmJuRABEBAAHCwPwEGAEIACYWIQQD0sLfkwCWDtAm6v5S7Ka8jwaikQUCYxre
1AUJEswDAAIbDAAKCRBS7Ka8jwaikaQ7C/9S1SAb0PDaL9t8tfh2CIqSrg8omBfO
byxglm2cXAym8pkfWTgWTLUJuBdHlhzCTRHpU3l5aFaBrLxY4A/0UapDbKuipIca
qgVu44xkQwB4/ejbUEjuaVKyTLyLY5OFK/F0gVhcQVMkqGzDcQlInaxO/bJ/x5KX
NOBguDKrY18c3RkPsunbt9TeY5fLd9CivkmrcVma/wrWy8ImsxkU/KibBziEIGGn
Bltj3aEXjskk6i0YVMnaOwueOsAo1ZsS0NXUQLJCmfyHbkI4gTtXC/8a74YXNmNr
4wvw6l2paFIIv9BhARfjC3z0lgG1IT8LP+6bRbqA6YB5XoxBldh9LrSScJURf/4E
jyHctZpGFWqpiRo6onkUytRk5IDLFiy56+ORjuyrX7+QHr+47gRHnv6Gw6N/b6AW
NswTJpACE61wIM3NUtcc+6ljMb9i/fPWhjRBp4xHGEQK3o6uB2gc0yZFNx4foQME
EEPnLsR0K8fS4EKefTZMRRvVKCqNpBGh3DQ=
=6PgP

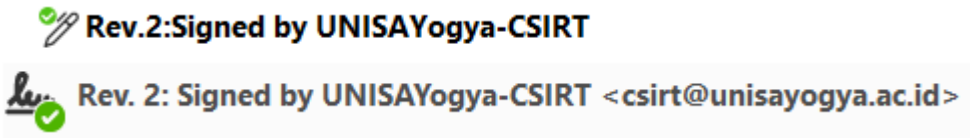
-----END PGP PUBLIC KEY BLOCK-----

Sidik Jari : 03D2 C2DF 9300 960E D026 EAFE 52EC A6BC 8F06 A291

File PGP key ini tersedia pada :

☐ Kunci Publik
https://csirt.unisayogya.ac.id/UNISAYogya.asc

b SSL untuk Digital Signature



-----BEGIN CERTIFICATE-----
MIIGQzCCBCugAwIBAgIJAPXvR2ipR+xnMA0GCSqGSIb3DQEBCwUAMIG2MQswCQYD
VQQGEwJJRDETMBEGA1UECAwKWW9neWFrYXJ0YTETMBEGA1UEBwwKWW9neWFrY
XJ0
YTEpMCcGA1UECgwgVW5pdmVyc2l0YXMgJ0Fpc3lpeWFoIFlvZ3lha2FydGExGTAX
BgNVBAsMEFVOSVNBIFlvZ3lha2FydGExETAPBgNVBAMMCFVOSVNBIFlrMSQwIgYJ
KoZIhvcNAQkBFhVpbmZvQHVuaXNheW9neWEuYWMuaWQwIBcNMjEwOTI3MTY1NDUw
WhgPMjA3MTA5MTUxNjU0NTBaMIG2MQswCQYDVQQGEwJJRDETMBEGA1UECAwKWW
9n
eWFrYXJ0YTETMBEGA1UEBwwKWW9neWFrYXJ0YTEpMCcGA1UECgwgVW5pdmVyc2l0
YXMgJ0Fpc3lpeWFoIFlvZ3lha2FydGExGTAXBgNVBAsMEFVOSVNBIFlvZ3lha2Fy
dGExETAPBgNVBAMMCFVOSVNBIFlrMSQwIgYJKoZIhvcNAQkBFhVpbmZvQHVuaXNh
eW9neWEuYWMuaWQwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCsKyLz
Hf2lOysNPeIvKxIsOCE1/5Fs3zPfce4BWjKsFkKdgtcorTav+PqbRzzqHxcsWoBE
ObkaYQBYETo+t6jKJKHfVtSlvQuvhuqjNOKboiPfxje0OVbVsLRgq0KPwci8/dBi
ros77F7bQu3kUThBhjfWJhulGwmYgjTFeUbdosh1INDelUWKNL4m1WErxvDjno8M
tWSeNZFCg8/9PC3Ic0rGwQhVbXprlAslkJmc821ith4KWNrW30sxOd8aOLmCuOFS
Ix1jFXF3HO4VWgGI6jjvR1aImXmjGJ3LuZiRj/sVy4QbrwHsuMbfL2Q/Jo1IFVaq
jfioovjrPi7o9brQ/IbytpCoxvJNYUgzcVv0K6BKYp+MeO7gmH1kLHpSWIyEn0vW

XNmIVuxLKI+PdW8AdkmWgXbAtzIEbWZ5CvpAAdrcTQ5ZSAR/vlYJu3IFQwuwF3N5
7bkomPRaW/YO5V9BbQ6wKcCoeOUMGXDYYb35VZlpW2XSDam9dTYa+5nv5Jo00zgA
ckewSDnuxbUyDrKAjZSye7BJCRYLMsljHQM/ZgmyAkrxE1+c3SyCUsnWh7Pm5nw8
+VcEhiv2NsHad+XQyjuFOS/3+5y+ah5094GWE9xyaLERujICnFOC9/tDrPQjAMwY
7u22+s4WdJliE4h57Wvpqwan3bY7URo3w0SSpwIDAQABo1AwTjAdBgNVHQ4EFgQU
BKNQX3INzLPr9hOpfJchbUwhd2MwHwYDVR0jBBgwFoAUBKNQX3INzLPr9hOpfJch
bUwhd2MwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAJtl3IRYZtzw0
+ec9ivX+ur9JrLiTdCx7sJD3rfCfdfH5IVXaOEllFu5wfBnxB16MwL6QE8b19Ok6
zBUrJr9FWKYiCYAJI/iCj8Wx8iHJtkd1vYaqefYHoMZ31ICAYH+r0SMRqbVpylGW
u6XLXysyimW51z5F3n1mBek9YllvPQxti9fdO/eedkd4QlsQnsaKsd8IasihWBtB
rkcOnGUTL+ac6h2LVQgkex7Ex9EZZX2Dn9v7GrhobwNku3iD00E5o/HqdjavBVPk
cNS9V3NEXhm8By+Ho7EGM+84TNncqXKVJCKo0DZGr+FnR0fAUzHc96RlQIGwqV+w
n7r9M4wQVVpM/rDvFvUaoYoHUznxBZd9bNd0VuMyjzjMl7tYp4m7tMKakDnbnmwm
JZWbWl8zdB8yA0psjPKDgs37zHOQOaduqCWLJn0jRLTCowsdFtcJ2DLK+e+ajeMk
H54qpZ/BmSn3LtnOvwFkWEWIgfbb2NyTiN2ZHXQftanrOvJWyaRbqHtGXFtAvDpB
PtkCBsutG35s9RCoYeb0PHLBsvKUg/VABdECCqmCBRB/IYw8GU+kzVJkCCO3oCRS
5tixTQoViFquY1IGdUcR11SOiWvqcTvLdM1i6KJ6E9hV1wqvj5nnWNMSBgsvxYNJ
YF1WXvgTpUCnTwuvvjGs86KgGlinXCc=
-----END CERTIFICATE-----

File SSL *Certificate Authority* ini tersedia pada:

- ☐ *Certificate Authority*
  https://csirt.unisayogya.ac.id/rootCAUNISAYogya.cer
- ☐ *Revocation List*
  https://csirt.unisayogya.ac.id/rootCAUNISAYogya.crl.pem
- ☐ Adobe Reader FDF
  https://csirt.unisayogya.ac.id/CertExchangeUNISAYogyakarta.fdf

2.9 Struktur

2.9.1 Tim

a Ketua (Koordinator PTSI Eksternal dan Jaringan)
Ikhwan Hawariyanta, S.T.

b Anggota
Arizona Firdonsyah, S.Kom., M.Kom.
Nurul Latifah, S.Kom.

2.9.2 Narahubung

Nurul Latifah, S.Kom.

2.10 Informasi/Data lain

-

2.11 Catatan-catatan pada Kontak UNISAYogya-CSIRT

Metode yang disarankan untuk menghubungi UNISAYogya-CSIRT adalah melalui *e-mail* pada alamat csirt@unisayogya.ac.id atau melalui nomor telepon +62 895-2940-5592 ke UNISAYogya-CSIRT pada hari kerja jam 08.00 – 15.00 WIB atau siaga selama 24/7.

3 Mengenai UNISAYogya-CSIRT

3.1 Visi

Visi UNISAYogya-CSIRT adalah terwujudnya keamanan siber pada pengelolaan Teknologi Informasi dan Komunikasi di Universitas Aisyiyah Yogyakarta

3.2 Misi

Misi dari UNISAYogya-CSIRT, yaitu :

a Membangun, mengoordinasikan, mengolaborasikan dan mengoperasionalkan pencegahan, penanggulangan dan pemulihan terhadap insiden keamanan siber di lingkungan Universitas Aisyiyah Yogyakarta;
b Membangun kerjasama dalam rangka pengamanan siber terhadap layanan TI di lingkungan Universitas Aisyiyah Yogyakarta.
c Meningkatkan kapasitas sumber daya manusia terhadap ancaman keamanan siber pada aspek pencegahan, penanggulangan dan pemulihan insiden keamanan siber di lingkungan Universitas Aisyiyah Yogyakarta.

3.3 Konstituen

Konstituen UNISAYogya-CSIRT yaitu pengguna layanan TI di lingkungan Universitas Aisyiyah Yogyakarta.

3.4 Sponsorship dan/atau Afiliasi

Pendanaan UNISAYogya-CSIRT bersumber dari Universitas Aisyiyah Yogyakarta

3.5 Otoritas

UNISAYogya-CSIRT memiliki kewenangan dengan konstituennya dalam penanganan gangguan keamanan siber, mitigasi, investigasi dan analisis dampak insiden dilingkungan Universitas Aisyiyah Yogyakarta. UNISAYogya-CSIRT dapat berkoordinasi serta bekerjasama dengan pihak lain yang mempunyai kompetensi untuk insiden yang tidak dapat ditangani, seperti BSSN dan/atau IT *Security* dan/atau Ahli *Security* lainnya.

4 Kebijakan – Kebijakan

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

UNISAYogya-CSIRT melayani penanganan insiden siber dengan jenis berikut :

a *Web Defacement*;
b *DDoS*;
c *Malware*;
d *Ransomware*;
e *Phising*;
f *SQL Injection*;
g Pembajakan Akun Media Sosial;
h Akses Ilegal;
i Spam.

Dukungan yang diberikan oleh UNISAYogya-CSIRT kepada konstituen dapat bervariasi tergantung pada jenis dan dampak insiden. Layanan penanganan insiden berdasarkan pada laporan konstituen.

4.2 Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3 Komunikasi dan Autentikasi

Untuk komunikasi biasa, UNISAYogya-CSIRT 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 UNISAYogya-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 satuan kerja di Universitas Aisyiyah Yogyakarta.

5.1.2 Penanganan Insiden Siber

Layanan ini berupa koordinasi, analisis, rekomendasi teknis, dan bantuan *on-site* dalam rangka penanggulangan dan penanganan insiden siber di Universitas Aisyiyah Yogyakarta.

5.2 Layanan Tambahan

Layanan tambahan dari UNISAYogya-CSIRT yaitu :

5.2.1 Penanganan Kerentanan Sistem Elektronik

Layanan ini diberikan berupa pemeriksaan kerentanan pada perangkat lunak maupun perangkat keras, serta melakukan proses verifikasi kerentanan yang mungkin dieksploitasi dengan tujuan menyusun rencana untuk memperbaiki kerentanan yang teridentifikasi. 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* dan *Stress Test.*

5.2.2 Penanganan Artefak Digital

Layanan ini berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi dengan memberikan informasi statistik terkait layanan di Universitas Aisyiyah Yogyakarta. Kegiatan ini berupa analisis teknikal yang dilakukan untuk mencari jejak digital berupa

objek atau dokumen yang diduga digunakan untuk melakukan tindakan yang tidak sah terhadap Sistem Elektronik.

5.2.3 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.

5.2.4 **Pendeteksian Serangan**

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

5.2.5 **Analisis Risiko Keamanan Siber**

Layanan ini berupa proses penilaian risiko keamanan siber, meliputi: identifikasi, analisis, dan evaluasi risiko, serta menetapkan opsi pengendalian terhadap risikonya. Teknik pengendalian risiko terdiri dari menghindar, transfer, mitigasi, dan risiko diterima.

5.2.6 Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan ini berupa kegiatan konseling yang dilakukan dengan tujuan memberikan wawasan, pemahaman, dan cara yang perlu dilaksanakan dalam rangka membantu penanganan insiden siber.

5.2.7 **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@unisayogya.ac.id dengan melampirkan sekurang-kurangnya :

a Foto/*scan* kartu identitas
b Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
c Nomor telepon pelapor
d Atau sesuai dengan ketentuan lain yang berlaku

7 Disclaimer

Penanganan insiden tergantung dari ketersediaan *tools* yang dimiliki oleh Universitas Aisyiyah Yogyakarta.

CSIRTUNISAYogya

2022.09.16 16:08:45+07'00'