RFC 2350 UII-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 21 Juni 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://bsi.uii.ac.id/doc-cybersecurity/rfc2350 (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Kedua dokumen telah ditandatangani dengan PGP *Key* milik UII-CSIRT. Untuk lebih jelas dapat dilihat pada Sub bab 2.6.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 UII-CSIRT;
Versi : 1.1;
Tanggal Publikasi : 21 Juni 2023;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Universitas Islam Indonesia Computer Security Incident Response Team
Disingkat : UII-CSIRT.

2.2. Alamat

Rektorat UII Gedung GBPH Prabuningrat (Lantai 4) Kampus Terpadu Universitas Islam Indonesia Jl. Kaliurang km. 14,5 Sleman Yogyakarta 55584

2.3. Zona Waktu

Yogyakarta (GMT+07:00)

2.4. Nomor Telepon

+62 274 898444 Ekstensi 1414/1415

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

abuse@uii.ac.id (untuk laporan insiden/pengaduan)

soc@uii.ac.id (administrasi dan respon)

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

Bits : 3072
ID : 0xCBEA9C2025228154
Key Fingerprint :6A8F 269A 4D5E 1196 A3CE A387 891B 948B 0B3A 857F

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

xsDNBGSZEagBDADpQ6xSTTXxm7SHI+lRXnE1QZwLOo1GtSv503JmLftB59Fxbgnk
kIs2EBqN9GrcTpArzb1bAPpG/L1my2yAs4QXM+p7rv3FbyOVK7hlf3Tb/ThBUtcs
TEjRAEJA09ANin6eGeXBmoqlTthsbcEL1TqgceFzl5O9zFyJKAyVkQI8BJ+dMixv
DRhjc49W+xXfRdmCOh6uPA3LhLxpN5ly2Qh3hLVflep33506XGZQ8QofPtgdmM8w
iPk5mnGVMg6AnBVIro0BXifPHLfwXw+Xy1qfYZeSMDyr0P255qb7c14E17y3fy2Q
ho+dzZ3XO4KGIBHfj0RbFh8h0r3syhQ1j2oLBWQbnrme+i9dv+xrkDefLtKWL+3f
bfoWlXkZ9DaY4YKpSF500goXe9HmbN7GCwLvZYZvQtYKf9keSzik3NonAbl0BHpv
522CtWEWlblVzLG9l5yKt7x+ao6HOqCpulH1lzyuA/eEkDkxnxpz82g5qtEJpxNi
B7a0amDSXhApTwkAEQEAAc0Xc29jIHVpaSA8c29jQHVpaS5hYy5pZD7CwQ0EEwEI
ADcWIQRqjyaaTV4RlqPOo4eJG5SLCzqFfwUCZJkRqQUJAeEzgAIbAwQLCQgHBRUI
CQoLBRYCAwEAAAoJEIkblIsLOoV/XokL/2CAST1ASVhiqiqkcQVAK2dYY+5SrEvJ
YHptMFQ83TaPSN5L2yQaKRFDDGwdIzEZZPn2h4gbXQ5qOj8mbdpDUSClVppF2fAP
jcWv+5AJ1enJ5EhM++xRwA+3+biUF8JZMWV6EKFtmea37fPejsjREx5WEKheHfgl
jIIKgBZCp9JgXzo5lHXQpp8xUtaO8j1z2Tim8X0cYvPplHBc/QaiO3T9KsJGBWTc
kZV48yXm8Cq4XNsou0hSoD7uaAXlm/B1VQb/jScFTURbocfnx7Zv5ZGHcq1IiYFx
6OWTAlIJVFsLOaaDee48z2idyOuZSpmYF7kXztEESQ3QqF40vK2gXCdaX3g3nwK5
U/E2Cyv347xjgPvuk2y/6Np+Smreb3rICsuW/fRbcGHpENop09eONtvNkqVhyjOg
nmdTzlHIcUDPQzpd1y4wTGkLS/AEj8ivDa7wUMUvYN56i0JzN53OP6WuSxdQ8q0w
kXj+PqYi+0p2/Qd3L7kL0QNlrxA5XztGwM7AzQRkmRGpAQwAsjy/31wVEBFl37lm
dZ7YY8416R0RCoe7P3MbRE7ciU6PBOrpQRIJvs2GBAYF6jD8Kf8IR5d2TXJxTl+H
Ul4sSkimg4NXluG7lRV/tpFV5QF0pRtn5gj0cjuDt/H44E3XrXe5QcM/e6N2Nn9N
5VJ0V+km4tS5Nkk15bSuWZPNc9B1hztw8XXgH2VxOeXkRVh1qaSrcXTfMmY0SU/l
AxZFj6/HPjQi4MlP5qeRP04GV0mjlOyF7dS/WTcQ0LMcuTQHYFDPM5t0rOyoMWbN
diMxlq2aBvkAmeGQ4lOzXA3ZWufNhKlI8Zlo7BfN2WVeXVpaqZxijWhFzAF6WpAz
ihZ2atwUVKUqjBTw1qDw10I6xgHSCUbR9zpMS+vRy49yRtYZ3PTYy5NHrGAb1DXU
GhyRBG1FU+v8QsByOFBbG1ok8LTv2V1mqkb8mzlty5fxFzgRTZvFs6rlnkNdnHeE
/KwdB1Zf3mngb4Z2Fv+RwU7CmiXPEkbPWkCc/GsG/9l661RzABEBAAHCwPwEGAEI
ACYWIQRqjyaaTV4RlqPOo4eJG5SLCzqFfwUCZJkRqgUJAeEzgAIbDAAKCRCJG5SL
CzqFf8pFDACy50wnLnqxXaY5YaXNyx+TAtLyCUhmYl3JEGYjODvhgar09sXyy54H
lzW7XRL+4kyxzknifXha7wgseY4kyFdCYslG+c2R6l33F4aZKa4Z6qRing/EytCJ
P3kFi+l78Ep+y6XDBD/oalFb+mXOXa/Hxa2drK7eid5bvSHo7pB4oVUId1i/VO2R
tXgn9sfpXK6jvajdedwAyDeR1ZcS9lOtL9cFhRoVvOzcJhH5uv1wSG5jVzZeIiK+
/ri1rMcIUDE6XpQ0jyVbxEM7n5H+iMivL909up3s8iHnzncMS5n4YG2wLx3L0lB3
4Riw0nRFeNasKhtMTYcUGzgHc/LFhw3Qho6UwWVHJqU7+dN9M+U2rhOUbNJAvb2V
m5EO4YGQCy8TJeFbcE0hKcrf9Zl+NBzbxut29rEQm8la6gBjzw0M5gykGLyTCy0U
SWDEQe5b2r386pACrlUz6lyI5S44M3PC+qgWbWGtXP+9469IC7TkgIuicvUhdhrJ
emXdwSxjvW8=
=WXwu
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://bsi.uii.ac.id/doc-cybersecurity/publickey

2.7. Anggota Tim

Anggota tim UII-CSIRT adalah sub Bidang Operasi dan sub Bidang Pengembangan dari satuan kerja Badan Sistem Informasi. Ketua UII-CSIRT adalah Agus Setiawan *Lead* dari *Security Operation Cente*r Badan Sistem Informasi Universitas Islam Indonesia.

2.8. Informasi/Data lain

Tidak ada.

2.9. Catatan-catatan pada Kontak UII-CSIRT

Metode yang disarankan untuk menghubungi UII-CSIRT adalah melalui *e-mail* pada alamat soc[at]uii[dot]ac[dot]id atau melalui nomor telepon BSI UII ke +62 274 898444 Ekstensi 1414/1415 pada hari kerja jam 08.00 - 16.00.

3. Mengenai UII-CSIRT

3.1. Visi

Visi UII-CSIRT adalah terwujudnya ketahanan siber pada sektor pendidikan yang handal dan profesional.

3.2. Misi

Misi dari UII-CSIRT, yaitu :

a. Mengkoordinasikan dan mengkolaborasikan layanan keamanan siber pada sektor pendidikan baik internal dan eksternal
b. Mengidentifikasi kerentanan keamanan secara menyeluruh
c. Meningkatkan respon aspek keamanan dilingkungan Universitas Islam Indonesia
d. meningkatkan resiliensi dibidang keamanan siber

.

3.3. Konstituen

Konstituen UII-CSIRT adalah seluruh civitas akademika Universitas Islam Indonesia

3.4. Sponsorship dan/atau Afiliasi

Pendanaan UII-CSIRT bersumber dari Anggaran Universitas Islam Indonesia.

3.5. Otoritas

Memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada lingkungan Universitas Islam Indonesia.

4. Kebijakan – Kebijakan

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

UII-CSIRT melayani penanganan insiden siber dengan jenis berikut :

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

serta dukungan terhadap konstituen tergantung dari kasus yang terjadi berkaitan dengan keamanan ruang siber.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

UII-CSIRT kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber dan informasi/data akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Menggunakan media email terenkripsi yang ditandatangani dengan PGP *Key* milik UII-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.6.

5. Layanan

5.1. Layanan Utama

Layanan utama dari UII-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

peringatan diberikan kepada seluruh stakeholder di lingkungan Universitas Islam Indonesia dengan memperhatikan tanggung jawab masing masing stakeholder yang ada di lingkungan Universitas Islam Indonesia

5.1.2. Penanganan Insiden Siber

layanan penanganan insiden siber yang dilakukan oleh UII-CSIRT berupa monitoring, analisis, rekomendasi teknis dan koordinasi serta pendampingan dalam rangka penguatan keamanan siber.

5.2. Layanan Tambahan

Layanan tambahan dari UII-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan penanganan kerawanan sistem elektronik ini dilakukan dengan monitoring, analisis dan rekomendasi yang akan disampaikan kepada setiap pemangku kepentingan baik internal maupun eksternal yang terkait dengan Universitas Islam Indonesia.

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 lingkungan Universitas Islam Indonesia.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan pemberitahuan hasil pengamatan potensi ancaman yang dimiliki UII-CSIRT ditujukan kepada seluruh sivitas akademika UII, baik mahasiswa,dosen,tenaga kependidikan maupun pihak eksternal yang ada kaitanya dengan UII sebagai pengguna layanan teknologi informasi atau pengguna sumberdaya yang berada di lingkungan UII.

5.2.4. Pendeteksian Serangan

Layanan pendeteksian serangan ini menggunakan menggunakan firewall yang telah dimiliki oleh UII.

5.2.5. Analisis Risiko Keamanan Siber

Layanan analisis risiko keamanan siber dilakukan oleh UII-CSIRT menggunakan berbagai sumber data yang dimiliki oleh Badan Sistem Informasi UII.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan konsultasi terkait kesiapan penanganan insiden siber di lingkungan UII dilakukan berdasar permintaan dari stakeholder dan pemangku kepentingan di lingkungan Universitas Islam Indonesia

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan pembangunan kesadaran dan kepedulian terhadap keamanan siber dilakukan oleh UII-CSIRT adalah dengan memberikan edukasi terhadap user dan stakeholder terkait yang menggunakan layanan UII di berbagai forum yang ada di UII (UIIAcademy dan Techtalk) .

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke abuse[at]uii[dot]ac[dot]id dengan melampirkan sekurang-kurangnya :

a. Foto/*scan* kartu identitas
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan

7. *Disclaimer*

Penanganan insiden tergantung dari ketersediaan *tools* yang dimiliki oleh Universitas Islam Indonesia.