RFC 2350 CSIRT-UAD

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 27 Juni 2024.

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.uad.ac.id/CSIRT-UAD-RFC2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP *Key* milik CSIRT-UAD. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 CSIRT-UAD;
Versi : 1.0;
Tanggal Publikasi : 27 Juni 2024;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Incident Response Team Universitas Ahmad Dahlan
Disingkat : CSIRT-UAD.

2.2. Alamat

Gedung Kedokteran (Lantai 7) Kampus Utama Universitas Ahmad Dahlan
Jalan Ahmad Yani (Ringroad Selatan) Tamanan, Banguntapan, Bantul, Yogyakarta 55166

2.3. Zona Waktu

Yogyakarta (GMT+07:00)

2.4. Nomor Telepon

(0274) 563515, 511830, 379418, 371120

2.5. Nomor Fax

0274-564604

2.6. Telekomunikasi Lain

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

csirt@uad.ac.id
bsi@uad.ac.id

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

Bits : 4096
ID : 0x594768419F35635D
Key Fingerprint : 6784 81DB F98D 1F94 793B C3DD 5947 6841 9F35 635D

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

mQINBGZ8vnkBEAC721+lUraHevER4xHRtaKWbfADeVdxJAEJbeHiLhmnGkl8+yI9
1BISphETAg1d4nP/iEPISsoZFrjdRcTaheBHhpfCwbBIs4tplekUzUuHxgORub/m
Peh5bPKQRKoiUjs2Tknf9h2NV5QmD9T2OSJJxqjaHe9RMMTJuV1gcbFu9UZr4OVP
4qaKwf5p1xJPripM9lGs7Nr91cPZrZT6nbXF6/+EqlEu+lnqSrYxjEilqMTpbIRh
N3dXU9eVe8PVyPsZuXABMIMwZJLSynYe8dVk15mud7S06dJP6u/Vk9OgSMkk+ZWU
duTwtvRlQgSZd3QNPBkQ1dzt74wa0lJQoXQicMxBfsvfrV8CkbpryPdmwTnkQfUq
Pc4raiLrA03qAal6HZDYpXDCjAK/yijvbK9coCRJu/qQgE9COoTvpJ357LzI9IOs
uJLWXKzBYiQCOVh+30usu3c/Px2ifcWrGw6wyJMYNf3TPiFNDLGEcDq8ZN6rxwqa
b7+BwCLAxmmB8ViUuACVIkvVPOiPXtPiuh+MFpS0YWghdlX4jt1tu7eoaEzCeK2n
o8k83hV6ErP1wNC1kcMzbHc7eaL+m2cFwVliMCf1+rrwUvx52cvxygUHm0TBh+Wr
fUPCFtMqDckBok2UE3TxQqMC8fLE7ozwncl+8vvcM+LEVsY/ECpMst5EfwARAQAB
tCtDU0lSVC1VQUQgKFBHUCBDU0lSVC1VQUQpIDxjc2lydEB1YWQuYWMuaWQ+iQJU
BBMBCAA+FiEEZ4SB2/mNH5R5O8PdWUdoQZ81Y10FAmZ8vnkCGwMFCSh1B74FCwkI
BwIGFQoJCAsCBBYCAwECHgECF4AACgkQWUdoQZ81Y116ww//XZIJQ16bJay2a2Zs
gjVnfiubp1hWii5AAZfblvebYCZR7OB+f0gPUzSFjCt70PHR5Io+QRsWL0yxdWqH
h6oJdVpag6Mbsjr7byYDLjpiOiqOj7soewAHMt8JMYyDdRg5xZ7uQ0FJxQ7BD48x
dFe9vCTdAA5ItO9RnRHBv43AVluUbAwgoNqwBljdFdSis0/5lOp7EgKyTenmtwF8
1xB01p7Xnb1+2vmHKgTzsSKTWKvpZ2ZEDhOlo5sLh9C+t6z4Ia4rRqhEbFH5Sn+X
5TkWfeA8RuRpf5eCi6nE5hNp7/jC8WFLJh5GK8q4F0LykAoLNxZwti/58Vi7eg2L
YVFR4vqEHetVu4juLryboqNxTvr8vkVzNdFs6a/tjX7sm0tvfyNZq/y0dwcoMyNE
plsWjp1OxMvyFOsgSzT0g1rYzzi6Nm+9LthV4S62bVYC76wwX1sICzNaFuK6dvbg
W24JywkEVva5pcdNbXQ/I9dGQojmnguwmDMMwTzZWQU84s07f5/X9se6IsuVCbGj
iC+bSY95hihUOZy1C3tpfgQ6qNMDSd1Ae1qQ6r2EAUckgD5gScOAb/wl9NWQc6jB
vrzhrEF+jJY/r4nQR4ms9lF1mmm7ZVfQm3xDmq4Ds9hvKgToc6PJBkxdTMKQsHqv
omUqD+HcAuR41uAa/2mT1sNvQqa5Ag0EZny+eQEQANOJowmvSvWbtA17a2WqQKjY
57DjqqH7uvF26VvMSLr8q0vN2xkuaWS+xp5DBN30195YhXYXbaXsScPDTs97TQMX
5dArRXwzFrqkDDE3/tpmTJ2bwlI8G9EokSIuboZEMAvj4ZDz0r8Wp9n1757fkISy
byf6o8nzA6blgso9P+DHHuIRqGfPO2KnwPZG/Yd0xTDdM/DQEnKq78clfwRBEsbC
cyQNVw4pI2WCWUFSjLsHsGRciCCVAquVIksYgDdbMR5muhJ3lxW60Hb5q7KqKpeL
K+5+HdsgP/xj2clAgnKTcGQHa9ZVtH/kroV3mAwbof78Gb4kYANPYx6EgUT36qeI
Tyv3qT7xqU4dzAZUgy5TMqm94Un0b78UzVzvltIDnxrnNpnT98YUIb76Dr3UgYn5
dQD2opDVDJcdFfT9rBwM830T99kGMDFEjNWAxejIPgUyEwM7MMmVHGwQ7svlZFee
tZ+a22biMxtrexXmYjAc0dmnKIQsltuTCkpn05wSrITRYvOtzxf3vqr16AY3Co7T

FZdplkTlpW/CF6pxRPCqaf0eFW+R/y5x8/fxpkMMeI7+NNCX/HDFRaoPFNMAfF/B
FzT7eVSywS4Uj3wYx7pT+yr4NhfQdi+TbFDSlFsb26hGBfuT294aHsLOJdT9YiIo
WjcHGn5MoOkpVi6hlqidABEBAAGJAjwEGAEIACYWIQRnhIHb+Y0flHk7w91ZR2hB
nzVjXQUCZny+eQIbDAUJKHUHvgAKCRBZR2hBnzVjXTClEACb3x9Bhe4bVjE/vYLL
3SR+1tlQNo3L634ju9M/alXIJYPGteDOZEgj7xxt2bW7NC7K9uDx+ADvfYnq3zKj
/XsoFyXABR0PATe5C0GPhBry1nYgIzI7Wzz0/+lA5wjzW1GKnFUxaMGdzh5EpFXW
uRGzd+slwFByHBPzmrEAC32gNsnE8udVQmYWqKQu7kIagiop6DvKhUubMOfds+ys
jzyFeyRuPizxpGyoL2kQvaO9M9ReL/a9fkaho9WyCFXnFM3VewWMyF++JG88rQrx
NgR1cp5vYHTfBVbxsa2xOJnYsrneQuUlvfaDduvFb2FvxKUDqTg0TupyJK54UeUU
LwsLK6COerB2nSGZymImN54o8k8hZ+QacVFXicigld4IKAS0eOdAlcYebGQxQVYk
lyYDMs7Y3RAvwsCJ+qz1k/2gXfqPxR55bXtty3ZmpPmAiVOh9bv5CGdhQbLnNxmw
AbYml+MBxREwSgQLxPBqaK9SHmckeswL2zChgD2xEPMaNgskodQb09kiH3kHgmTd
7CjGoYumgA0NtAVzTZt/qOpFhIOI8wt3049Zdc25vKPL4TYZB0S0CpHX1WevbMlx
q3UCVbt+douztIIRAIWVvAPIO21UiaRO2Mrs/z1tbJSnRsugg90K7EaiQdq2b+sP
G6fbmoWxbtiDt2r4vuji4UqVqw==
=a361
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirt.uad.ac.id/publickey.asc

2.9. Anggota Tim

Ketua CSIRT-UAD adalah Kepala Biro Sistem Informasi dan anggota CSIRT-UAD adalah staf di Bidang Operasional Biro Sistem Informasi beserta perwakilan Biro Sumber Daya Manusia dan Lembaga Bantuan Hukum UAD.

2.10. Informasi/Data lain

2.11. Catatan-catatan pada Kontak CSIRT-UAD

Metode yang disarankan untuk menghubungi CSIRT-UAD adalah melalui *e-mail* pada alamat csirt@uad.ac.id pada hari kerja jam 08.00 – 14.00 WIB.

3. Mengenai Gov-CSIRT

3.1. Visi

Terwujudnya ketahanan siber yang handal di lingkungan Universitas Ahmad Dahlan

3.2. Misi

Misi dari CSIRT-UAD, yaitu :

a. Mengkoordinasikan dan mengkolaborasikan layanan keamanan siber di Universitas Ahmad Dahlan baik 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 Ahmad Dahlan.

3.3. Konstituen

Konstituen CSIRT-UAD meliputi seluruh civitas akademika di lingkungan Universitas Ahmad Dahlan.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan CSIRT-UAD bersumber dari Universitas Ahmad Dahlan.

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 Ahmad Dahlan.

4. Kebijakan – Kebijakan

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

CSIRT-UAD melayani penanganan insiden siber dengan jenis berikut :

a. *Web Defacement*
b. DDoS
c. Malware
d. Phising
e. Pembajakan Akun
f. Akses illegal
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

CSIRT-UAD bekerjasama 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 ditandatangi dengan PGP *Key* milik CSIRT-UAD. Untuk lebih jelasnya dapat dilihat pada Subbab 2.8.

5. Layanan

5.1. Layanan Utama

Layanan utama dari CSIRT-UAD yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Peringatan diberikan kepada seluruh stakeholder di lingkungan Universitas Ahmad Dahlan dengan memperhatikan tanggung jawab masing-masing stakeholder yang ada di lingkungan Universitas Ahmad Dahlan.

5.1.2. Penanganan Insiden Siber

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

5.2. Layanan Tambahan

Layanan tambahan dari CSIRT-UAD yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan peanganan kerawanan sistem elektronik ini dilakukan dengan monitoring, analisis dan rekomendasi yang akan disampaikan kepada setiap pemangku kepentingan baik internal maupun eksternal yang terakit dengan Universitas Ahmad Dahlan.

5.2.2. Penanganan Artefak Digital

Layanan ini berupa penanganan artefak dalam rangka pemulihan system elektronik terdampak ataupun dukungan investigasi dengan memberikan informasi statistic terkait layanan di lingkungan Universitas Ahmad Dahlan.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

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

5.2.4. Pendeteksian Serangan

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

5.2.5. Analisis Risiko Keamanan Siber

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

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan konsultasi terkait kesiapan penanganan insiden siber di lingkungan UAD dilakukan berdasar permintaan dari stakeholder dan pemangku kepentingan di lingkungan Universitas Ahmad Dahlan.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

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

6. Pelaporan Insiden

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

a. Foto/*scan* kartu identitas
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
c. Dokumen berisi narasi insiden yang dialami/terjadi.

7. *Disclaimer*

Penanganan insiden tergantung dari ketersediaan sumber daya yang dimiliki oleh Universitas Ahmad Dahlan.