RFC 2350 UNTAR CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 19 Agustus 2024.

1.2. Daftar Distribusi untuk Pemberitahuan

Rektorat Universitas Tarumanagara.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt.untar.ac.id/rfc2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Kedua dokumen telah ditandatangani dengan PGP Key milik UNTAR CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 UNTAR CSIRT;
Versi : 1.0;
Tanggal Publikasi : 19 Agustus 2024;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Universitas Tarumanagara Computer Security Incident Response Team
Disingkat: UNTAR CSIRT.

2.2. Alamat

Gedung Utama Kampus 1 Universitas Tarumanagara, Jl. Letjen S. Parman No. 1
Jakarta Barat

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

087771750509

2.5. Nomor Fax

021-5638331

2.6. Telekomunikasi Lain

081513027484 (Narahubung-1)
08119187711 (Narahubung-2)

2.7. Alamat Surat Elektronik (E-mail)

csirt@untar.ac.id

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

Bits : 4096
ID : 0xA10147FD
Key Fingerprint : D97F FA70 7941 FAA8 3316 4C8A AFD1 359B A101 47FD

-----BEGIN PGP PUBLIC KEY BLOCK-----
xsFNBGa1wzYBEADj4lzBkZ4zLHQ9+26KksiNVyc+7BeJFEiGlyM92iZ6dCxhXmDi
iazhzYdZm67JzlJ2v8YunsgSFEdxFz0zIliYfMiZPjEjRX10hRp1PenRXGzXQYCy
l+xBasWR/NSTz7mRrfJTSVxe7G6W27a1idBVPcGn28GJgjRUTC6VLlWbLYhyvdJH
VesjnSyamO4yV0IFlRAaVmTR/CVMCGQW/Ej9cuoWlmBSvwzP3qImtLDORkWhZNla
48wyVGDY0/FYGYgt3/vZTdrlqNaoVVYX2EYz6IMJI5w6RumSbWn9+WRBqe7cak1C
Au6LziErf32pP/g89uRTz0Iunk2knn5L9l0eP48q9bHqj+Aqm1ZfY0H0/MBMHrSU
RpEMVGGL/huEtIUBPXn99R/siBlF6tjFLIiC8cM9l5YumYAYgYMh2DG+v9RGnrIm
MtTDS43TZioKG0guSa/d/uwHSbBxmVgDIciZy4LdUCOFAYzEsjafUhMKUvORKvhc
nPls33dFT46rcaWowbmtY7Q64AXZyXsv/4OOsBhVxCqDyo8r/kPNOCAsJ8QSVhjD
8H6zCz1Q+wZwofpIewhIgWwRKbWvdm+PQdAN0UHPOq14x/GECXF1ppIzP023WNQc
vtRNd7aaboDM/t6WMBRMF3vb2RooZbeMsS+FQJ6+C2znPoPxKNIDte/GCwARAQAB
zR9VTlRBUiBDU0lSVCA8Y3NpcnRAdW50YXIuYWMuaWQ+wsF6BBMBCgAkBQJmtcM2
AhsvAwsJBwMVCggCHgECF4ADFgIBAhkBBQkAAAAAAAoJEK/RNZuhAUf98IMQAJY2
fnkjPTGPz2eJwxD7qevyzBvvaFyN0+u2iBDji4Z1LBjoIWXJipiVeEEi8q7e/2w4
LWjqKQ5mvWun/fjLaqqQ/fBGCtXb2Hpyd5Mbbv4nPogKE4kdBB5G0MH6tAeM2sXZ
IFKcFimmUu9h09cWxMryeAObQtRHPAdJeZRDy06SmvjymCpDyqhjSmFvLDMf/KUS
e1LHmx7hkc0Kcz/kwwdinaLp7sNBu5YzWGvqetfYpSN70A5WayppQfDZE6BNZNqi
LxxyjJgp8zGE+6xvfCCm0josuqvIgTJyTynITRQkNN5V3BkSp0131qhL8pncGacI
fJOHW1YO2oh4Dx9A7WT00WvUhnKSAPYzlj2rAkPt6roLy0PKJ7V+e0i93vZgSovt
ZZvvlcoKH9t3JUA12OMDnkWm6RsHR7K3J9bk/CGkSSEbOP55LTFoFlQjZox+oaLj
YeVTtANnFPMEKGhaJb2Nz3riWYdX28FbmtUZIM5VAq5tH5KFSnjTW6sntKjcjJFq
LIIzNWjy3l+zLiatOeF+liR6sSmUcJlGOI7FPUdBBmqX3uWoBvDjHaLgTdbQnMUl
KZlQiARpSBlhSa37YtjU/Gtr0mBcB1bEqUkf4gxXwC5en/xPh/GLQQSuL96fddWe
uOOZ0xh2DUDVgogcl4nvCkQB2c4eYFFJJuD3z14dzsFNBGa1wzYBEAC7irm5boSq
VgamzSyuhCF/yketCbyJkvmtkotF3RNXZNo5FzO2/zAcElrNstXafEfPsxx7APcY
49gSK8XWJcJZKyK5ks3ggTMPZzqjmSrVLxZbgEVSyCAgxnX0dDA3bSIfSnogrg/o
A0NIofRMxiwuXy0SxlqKA1Mx0gSTZL91ynRs6f9WARGplYpmWTvlddcGVLuzFmpk
L7we2GtoaegD87WiXW7OCgx2w8g/w7NtwRuzDWklY2+EZG0vhGfugakM9INAi0GE
oyJYgFVbEEUGiFkLC2epS8/RLFH8xZNf4LSkq61/Z8cknlDwzlIXlMu5lbB7ESbA
4cGLsdNcK+FQTva3rHoi4SP/AVgGyzRK9F8e1Gosb6CCGsBFBTLor4fu7OaJuEmC
81fBe5HRmlDAwgHcq92TNHWqFLzCBaNEtryeHQOqY0xEJDoTHcrhHMaJgs1YHjvl
/gqQgh7ValHA4JfRjsDqllzrd/V30h9NX07/kJTwBkxvTmHfIyxb9HUfOxO2+cwy
QaQQuFiL64umZcsLGC0yDTkuoLDVoKdahw3N+SN1hXTT3RhcQLq1Y8erMAVnIYzF
KbIZ9TsqGwpLKdHk4kt1htgSjVQF2Zl8ZlMMNJ9fpoiYX5PwL65Mej9MUgzRAbvW
v+N2XzL1MC5x6DiM5TNfMUqTxaDf+OPIeQARAQABwsOEBBgBCgAPBQJmtcM2BQkA

AAAAAhsuAikJEK/RNZuhAUf9wV0gBBkBCgAGBQJmtcM2AAoJEICbQ/r7u/X/Ra8Q
AKjD07fIN7WaAdkjS0xEulaljiSjOsm0VCd0aF4dpInJ4xJHHn/qUtEBGdvI90H5
T5NfwLPTWFvz5AG5YiTwCwzxmQtR19f6cCC1I4XzAmVUliJyypcFydlNieeQBqWw
k3ExtZ/N/GB+KjJdncyATJgLVL5C/HkOfVLzQZim378o42yHjXq5jLYNbOSP6mIS
IcK0tUtbmJC2iFPkpYKfjxL7sBSkd5tbOZqVsGDCr5XETdaMINl2KXBPhOYkSgiP
c1IPEg8POPINrcV5xeXu6fDiNHdrt+5z89ZWdjjgCmsUxRivOgDM5/nbzzREAmM0
faZf11SwtdvETkI/k8JuyWxQf0xTxPHtIY0VW3kkWJNNEhVgx/nPDw5Sc9MlRBIM
AbHRnkPAA6CiIM23GVJBxGKLr2dBRq2rOfoKVpnMqkZQU3X9z7JMGXEcpS0LSO2f
2TkeR/yUH7MDfhA/988M5yBRcAMAtEMOGA5UJueVM9ApjBr9nzEtx+UkbKS1wVqf
LAYX3vwMQl1NP/TbEWtqon/qIaJyul6muUBCOK0XswR/jgIGHq4RtkoHegySfitG
hPmBY+C7aTNrkiR0ivT6cHezEZwtAVU70HU59eVqn6MLDqsvYjsqcu56rrYSdzps
f99w25jpNtGUmQhI474vCGTrwzFeVFdBrCxn1I0bYm46T5UQALHTWNMudPvXeHVj
a2h8GJ5ZSMeiYm9fnf0QgemDQrtRwxFH5SfqSNf/niIXr0Aud943KB9SoM0IJ0sa
VXnRvYiXYzGXJdNONZgXQg3/ClnJjtjjG6pH9NRyDwD8V6Y97JH+R8RuJIM/zDdf
99KlT7OP5JnBVbGgT/GRuYxWM+03bNDZ4sO2uWk6+MNI/z/bAJ4OZERlSDH/eCTH
xvxrfBexgFSFwfH049zq1caaBZJjRvrmklcrXwqsRJ0nxgjoTYXm6Pv5VP5a2wAY
Wwu39p9wHOZaGBIBG71NG44NmQHu2DBLVjyN/yG7PoZlpB46QR1NrbRa5cEoKWZk
IMpl/kdj4S2Vjl9r4t4wAQBxzoC1SyrPw1e3ghZN1USy93QIZuU2O4oyFphnRRWf
QvfvNxAWfwNzBWnFVNAFjdWmmSHUFsoO9/i8v19nOuND5t2+a8zbh77jsn44RWCo
xH2aOBXHTaBCKwIfq3Ih8KOCwm7C1UCPhrgBZRxy7eeRf5XpefgNRZ3WzwA/4gKn
FvvupnGJ4bOwmhRFlCw5K4WU373zQJSs/rLt8OMOeNflHJOWn1Lz4cveRPwc4jgI
sVBTkfVi7hO+qT4CEQ81Mp+WevAuln8ESWbJ9645Fml+DJ56e3APwTONLuYU1ZXu
yUaOU2ApbACRGhoQ4HwTiExbyfMnzsFNBGa1wzYBEACgsMGbVPAf549zYrP8wMxy
D+edU3Ch83Crv+aubKfu4E5rzOx8Vwmlxj1kiaVzL+Ghe5jnq+dAtsTmzgjfcTEu
UyM2q9lteNfMjIr9R033b8h8kPwGM3YdC3CzgggQacS1kpHm3nBCcY2VJobqZk66
uwDaA9Wx2PeChfAXhgmOyDqVtA8iZd6+0BPdEDKpbxKPcIsSwOvcMwi8BSB+Xiwo
Hk3OsEmnX4/BKe7UWGcD4H2f4FKleCklhgnc+v+BJxDu0Dp3mXFuiCioYUTuHRVX
snQeCW8XgEznqPe5nVXUmNBhAr5uVZlMrUGez/4dMuJYULw1KjUL1CvtP3vIIGEk
ZqaBXIRCaGEt6ihrNdDjSwRaKziPmote0k3sfENwhrCno4nJUwSp0v2T/4P0cPxE
jEc+iWK3FJIsW/5EJdhoCvlxfcFCnS9pMlYHI7LEyXbCXZeoKjr2Hx21yK6/2kBH
ORNT0pi/RBd7T9VXbq3qSglS57O7XYLKLINt1tHvdN3zgbeGTQlYOAI7wXbcHb0z
XyFIxoGP2uQb9Fxxxx+fk2k0yydtbfsiatC3XLTJesJ7XN8VgaQ5dmtSW12LPQ2p
T6MtL2qPMUlbaXpaFwONDN0z6yXdLgfdpxun9nqgFgsD3xlCIqie8QA4VAOkrOsn
5+TOLNY1BQtMdTGypkzcXwARAQABwsOEBBgBCgAPBQJmtcM2BQkAAAAAhsuAikJ
EK/RNZuhAUf9wV0gBBkBCgAGBQJmtcM2AAoJED63EC0PdMNY2G4P/1oc6M+kjkkD
Tva2mNRkUm9ErDIwdipyhuCzDygFbk6uemu/7kV0uIZE8Yzued8SXqemIFlf8e9n
j2xDKjfDBIz4IJKJMV/s+katUyvfrWoFaJ/sVo1Nz3kn2VwfNvD9YCiHgpOB6NPI
tS9SFrVPFYwsVxgTmkcxnTFOmcEzf7C4zlyONAK5Xc5Q/mPKC21u6aTkjMDz1JiW
TwCYe7Pp8PuvsoD1/OPi8A7TNKz/XXexCq7jGXJ8q6DhOei3i/72hrPHajqXVEWp
EFE8kWNY9lFXtMPPPTDSMK4uFXEDAjBn7CV4KzgG9EcPuYtkTgEu9CLb5KA0N2XC
6hFzs2wBVha+6lLrNIXURK/SFLaFn0m0IykIGHbf2fkrwvvvgZRK0tQcr64a2ixR
CROct7R2m4ZveGBtyby+6PsO4rO6CJ/uCMCjED14wfgbpArgNy48KU/HYNF+cZri
74qpnDNKMe9uhjlvMwzYRdm99PXfOQUBm0FbHNwMZq5BawoRU4ga5WoItd/6BKBi
AAaiUKPsOGleyZC7ICbbsw/sYXnQVOCDyBexqgwl3hYqW1nvmckrVloHG0fqcjAQ
ru/6cVepjdCihIhPqDHZMnuP7MY1J8P/NctFHVPCx7JE0JAuVY41EWE6MD08t2pT
oWfczVXHe/pBYNgFNLxN2L/dBBzESL+FLwEP/0y/H8cNxzpBosRXB4hhuge1m10J
36xR9XVr8YYGcE71uwOdXyQjQMYMrsEysZ073OvCHIT4ig9LFXVmWX7gjGsWAJxj
Qjm4GRtrXYRA6m0iYlsk3qTY2kaj82dsLjQEBqXlvj1spaDvcLublkRiMMnUwaNf
bEmtXZo0maZCKXcF4dCT9Ipxb0s+EMEmtwwiDjWh/itW2X0MRyPMN85XRDFhgBLO
kJJvVv7szi1+U2anCE5Bn4d43IVrNgII0ybGSTvZyjjPIkTYN87/5ONbon8vpp74
TfJCOA5q56UqIrzDW1INb4YmmMoi+XwldOP8NjIKkkRnqTEsbaM+/cMQCOaKpJof
a6AJByDcvAU12a5LYSR3zrjeE5gansamzA6H7bE9T2IaTcXboKiJynJqsiseKdAd
P5AdEjL26XbVJybnp8hM+9WSd9403VsYza1JaWgU5a/fMS5NQ6EtLxuhEFsRGjfJ
jGcpJNc/2kT0To7E+ejKEsYkrR5UtJwUaE/s8UyqHgnPnsDeUA2uel2MLQKy7PFZ

phD9tVekjtqE5FaCKD9S/kJvdlu+67+eEJ61+QFFeqblceVIANycovpB/+i5Rh4W
szmK/Pm4eW/jLNHUgxsCCBFXPDtBjQ3Aq2/CR4zobDJ4qOaAe0YSJQ9nC3IhOYw9
/0mlQdDtBqNcZotL
=f4u8
-----END PGP PUBLIC KEY BLOCK-----

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

2.9. Anggota Tim

Ketua UNTAR CSIRT adalah Kepala UPT Pusat Komputer, dengan anggota tercantum dalam SK Rektor Universitas Tarumanagara.

2.10. Informasi/Data lain

Tidak Ada

2.11. Catatan-catatan pada Kontak UNTAR CSIRT

Metode yang disarankan untuk menghubungi UNTAR CSIRT adalah melalui e-mail pada alamat csirt@untar.ac.id atau melalui nomor telepon 081513027484 (ketua csirt) atau 08119187711 (narahubung-2) UNTAR CSIRT pada hari Senin s/d Jumat jam 08.00 - 21.30 atau melalui nomor Whatsapp 087771750509 di jam atau hari yang lain dan siaga selama 7 hari 24 jam.

3. Mengenai UNTAR CSIRT

3.1. Visi

Visi UNTAR CSIRT adalah menjaga keamanan siber dan mencegah terjadinya kejahatan siber pada pengelolaan Teknologi Informasi di Universitas Tarumanagara.

3.2. Misi

Misi dari UNTAR CSIRT, yaitu :

a. Membangun, mengkoordinasikan, mengkolaborasikan, dan mengoperasionalkan sistem mitigasi, manajemen krisis, penanggulangan dan pemulihan terhadap insiden keamanan siber di lingkungan universitas Tarumanagara.
b. Membangun kerja sama dalam rangka penanggulangan dan pemulihan insiden keamanan siber pada Infrastruktur Teknologi Informasi di lingkup Universitas Tarumanagara
c. Membangun kapasitas sumber daya penanggulangan dan pemulihan insiden keamanan siber pada lingkungan universitas Tarumanagara

3.3. Konstituen

Konstituen UNTAR CSIRT meliputi :

a. Lingkungan kerja akademik Universitas Tarumangara
b. Lingkungan kerja non-akademik Universitas Tarumangara

3.4. Sponsorship dan/atau Afiliasi

Pendanaan UNTAR CSIRT bersumber dari Universitas Tarumanagara

3.5. Otoritas

Untar CSRIT memiliki wewenang untuk menangani insiden, melakukan mitigasi, investigasi, dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber di lingkungan Universitas Tarumanagara. Mereka juga dapat berkoordinasi dan bekerja sama dengan pihak lain yang memiliki kompetensi untuk menangani insiden yang tidak dapat mereka selesaikan sendiri.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

Untar CSIRT menangani berbagai jenis insiden siber, termasuk: a. Perusakan situs web; b. Serangan DDoS; c. Malware; d. Phishing; e. Pembajakan akun; f. Akses ilegal; g. Spam; h. Insiden siber lainnya.

Dukungan yang diberikan oleh Untar CSIRT kepada konstituen bervariasi tergantung pada jenis dan dampak insiden. Layanan penanganan insiden didasarkan pada laporan dari konstituen.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Untar CSIRT akan bekerja sama dan berbagi informasi dengan CSIRT atau organisasi lain yang terkait dengan keamanan siber. Semua informasi yang diterima oleh Untar CSIRT akan dijaga kerahasiaannya.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, Untar CSIRT dapat menggunakan email tanpa enkripsi data dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif, terbatas, atau rahasia, mereka dapat menggunakan enkripsi PGP pada email.

5. Layanan

5.1. Layanan Utama

Layanan utama dari UNTAR CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Pemberian peringatan terkait keamanan siber adalah layanan yang bertujuan untuk menyebarluaskan informasi mengenai ancaman atau insiden siber kepada pihak yang berkepentingan. Layanan ini dilakukan oleh tim tanggap insiden siber Untar CSIRT atau organisasi yang bertanggung jawab atas keamanan siber.

5.1.2. Penanganan Insiden Siber

Serangkaian langkah yang diambil oleh Untar CSRIT untuk mengidentifikasi, menganalisis, dan menanggulangi insiden keamanan siber di lingkungan Universitas Tarumangara.

5.2. Layanan Tambahan

Layanan tambahan dari UNTAR CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Penanganan kerawanan sistem elektronik bertujuan untuk melindungi sistem dan data dari berbagai ancaman siber yang dapat merusak atau mengganggu operasional.

5.2.2. Penanganan Artefak Digital

Layanan ini melibatkan pengumpulan, analisis, dan pemulihan artefak digital yang terkait dengan insiden siber. Artefak digital bisa berupa log file, file yang terinfeksi malware, atau data lain yang relevan. Tujuan utama dari layanan ini adalah untuk mendukung investigasi insiden, memulihkan sistem yang terdampak, dan menjaga integritas bukti digital.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini bertujuan untuk memberikan informasi kepada konstituen mengenai potensi ancaman siber yang terdeteksi. Informasi ini dapat mencakup deskripsi ancaman, indikator kompromi, dan rekomendasi tindakan pencegahan. Dengan pemberitahuan ini, organisasi dapat mengambil langkah proaktif untuk melindungi sistem mereka dari ancaman yang mungkin terjadi.

5.2.4. Pendeteksian Serangan

Layanan pendeteksian serangan melibatkan penggunaan sistem deteksi intrusi (IDS) dan alat pemantauan lainnya untuk mengidentifikasi aktivitas mencurigakan atau serangan siber yang sedang berlangsung. IDS dapat mendeteksi berbagai jenis serangan, seperti serangan DDoS, malware, dan upaya akses ilegal, dengan membandingkan pola lalu lintas jaringan dengan tanda-tanda serangan yang dikenal.

5.2.5. Analisis Risiko Keamanan Siber

Layanan ini melibatkan identifikasi, penilaian, dan prioritisasi risiko keamanan siber yang dihadapi oleh organisasi. Proses ini mencakup evaluasi kerentanan, analisis dampak potensial, dan pengembangan strategi mitigasi untuk mengurangi risiko. Analisis risiko membantu organisasi memahami ancaman yang mereka hadapi dan mengambil langkah-langkah yang tepat untuk melindungi aset mereka.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan konsultasi ini menyediakan pendampingan dan saran kepada organisasi mengenai kesiapan mereka dalam menangani insiden siber. Konsultasi ini mencakup penilaian kesiapan, pengembangan rencana respons insiden, dan pelatihan untuk meningkatkan kemampuan tim dalam merespons dan memulihkan diri dari insiden siber.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini bertujuan untuk meningkatkan kesadaran dan pemahaman tentang keamanan siber di kalangan karyawan dan pengguna sistem. Ini mencakup program pelatihan, kampanye kesadaran, dan sosialisasi mengenai praktik keamanan terbaik. Dengan meningkatkan kesadaran, organisasi dapat mengurangi risiko insiden siber yang disebabkan oleh kesalahan manusia.

6. Pelaporan Insiden

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

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

7. Disclaimer

a. Sampai saat ini UNTAR CSIRT hanya merespon dan menangani insiden keamanan siber yang terjadi pada perangkat kerja yang ada di lingkungan Universitas Tarumanagara.
b. Penanganan insiden jenis malware tergantung pada ketersediaan tools yang dimiliki.