RFC 2350 *COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT) UNIVERSITAS TERBUKA*

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi *Computer Security Incident Response Team (CSIRT) Universitas Terbuka* berdasarkan RFC 2350, yaitu informasi dasar mengenai *Computer Security Incident Response Team (CSIRT) Universitas Terbuka*, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi *Computer Security Incident Response Team (CSIRT) Universitas Terbuka*.

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 15 Mei 2025.

1.2. Daftar Distribusi untuk Pemberitahuan

1. Mahasiswa
2. Dosen dan Tenaga Pendidik
3. Tenaga Kependidikan (Staf Administratif)
4. Manajemen Universitas
5. Unit/Lembaga Teknologi Informasi
6. Alumni (jika masih memiliki akses sistem kampus)
7. Nat-CSIRT, Edu-CSIRT, dan ACAD-CSIRT

1.3. Lokasi dimana Dokumen ini bisa didapat

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

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP *Key* milik *Computer Security Incident Response Team (CSIRT) Universitas Terbuka*. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 Computer Security Incident Response Team (CSIRT) Universitas Terbuka;
Versi : 1.0;
Tanggal Publikasi : 16 Juli 2025;
Kedaluwarsa : Sampai dengan dokumen terbaru berlaku;

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Incident Response Team Universitas Terbuka
Disingkat : CSIRT-UT

2.2. Alamat

Direktorat Sistem Informasi (DSI), Kantor Universitas Terbuka (UT), Jalan Cabe Raya, Pondok Cabe, Pamulang, Tangerang Selatan 15437, Banten – Indonesia.

2.3. Zona Waktu

Kota Tangerang Selatan (GMT+07:00)

2.4. Nomor Telepon

(+6221) 7490941 ext. 1401

2.5. Nomor Fax

(021) 80639333

2.6. Telekomunikasi Lain

Hallo-UT 1500024

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

csirt-ut@ecampus.ut.ac.id

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

Bits : 3072
ID : 0xFACEB9B5B68B72A2
Key Fingerprint : 9580 CB4C AE1F 5A9B FC28 100B FACE B9B5 B68B 72A2

Blok PGP Public Key:

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

xsDNBGh0qvkBDACnJWH49OrDoG9aEFmaiKJqv/PtAvv/lqBVtMk+XjQUeXYcyo/j
X9DJN2OzOZ1GLYD6awEasMNiLFq090UCecXBmqFMRL7YoS231zShzhSv32YB3p3d
AhrEizsrRn9QvgTIh+tk3vWb0xsLqTZPK0c0A8zk/vBq3MmTiS/8u6QTMr4l7UbS
R3eqJENOCFr1h+p+KZ/r2V/KBNnLXHHFLgftAIdYVSC6pejr5xBWwjR+9M5ObAoP
tyTEI2d6dwVRVU5rbzQdtOtH2UhZtra1kGIQxK9h6NpNGcKDoIOzP/uV+V7oWgvk
iQE+42ZFOUDVVoeiHEqYuY2IxFJehhU4aiPaXGJBgfkCAfOvnoX3JUcQgTWVofXR
gQT13J9q0FZfm7fhB7ptOXZ/gMQKtYcuqJC2NC7SI7Dl3WxesOKwNuaAqtvGo4Ar
+gfx0m7Augm93B4MDZtSlSPBVYFWztuSqG6BJ2+2YSXrPgE6aa5K6e1plmqv8+2A
B2/149J7Vx4N4fkAEQEAAc0kQ1NJUlQtVVQgPGNzaXJ0LXV0QGVjYW1wdXMudXQu
YWMuaWQ+wsENBBMBCAA3FiEElYDLTK4fWpv8KBAL+s65tbaLcqIFAmh0qvoFCQWj
moACGwMECwkIBwUVCAkKCwUWAgMBAAAKCRD6zrm1totyos9DC/46iGJZrVEq4nIv
CSeD38NvBBOtlRGc0M2YWmV+zqF8Ih/6IwiS0rGVqWeaUR3NDq2wnHyB8rd8lSx7
j4gA60HmuLiVWFmsTm6djRmDGivOfkIWR1t5kf3Mua2S0R/h1uPlCEAsovadBflG
ah6H3sPo0/GBPo8qKA2L8lhXPSd7MiaKBJRI9+uair4+oz0vCQLAlmbuVNDgtpvo
/GK/iZ2Q5FiUrrVt+Af8A8qJkgpNpvBzC3t1VnaDgy6Gx1EY1IffwAelfd21Wz8F
K2iyljJEaXmRk+3VCrFlhoQnT0naHweFJv5zQXYV0O/PDtRfQHSM9u5iNe+tMlmw
KTJID+hKhPSxrMSvQo/G0Fqk9sm/deijBylMGJO1GzaBvTSFQz9kPcKCfFEVVQg/
GbeMynN8XT793br1Ziy/RMjGZXdNeFWQCOv0D/96HXV8S+VGW5vIWaw65JzL+bFk

8uv37fTtUioLx7OGvMtBXosChGbGnudzfp4dAK04hSVSnx/Ag4/OwM0EaHSq+gEM
ANtCMdez2csNNJoAIqTt7o4ij7q1vo2M1p67QES+XI07WTbZfHDoElghqrHYNr2W
e+fe3WhPoABtw9W6SjwrcraZmIgf2glbAzEEnrrUHCnAbGbacWLIz1m/V18x1njG
2Q3p7M18tQEA+zdZSeXRbvPSzEHs9M7GlNtd1qVCFZdvT+eBAwgamyUS6ptISpWj
zh6lcXtV4T4VMuEE4o1Jp5gM+rPLqKbPfpPow5PszAq71YevSsHsXvYv5CSS8IXO
DvF6ZgGfcQixtfBL5J4r9+fR2q0nDOpuow7IDOJHbZRTOIFVrjXokTqUQ31aTpI0
IfVtXwMmw48KATJHaeVWFL5y4Fp8TBSEHZY5hptfddYqg8vjUKx4crh+jQlMTbl/
JB/e5iRckHpWPJ/g6tXVFYyGoXtUjO/JEiPi9SB+2KWUuST/MXu078Yi2oWajegV
ULHAOl8oxeA8p7GzPQdnjeQwzuRK4M5ExM8NYeQsvmXwTY+UK70fZGWTDGUIJ7eF
bwARAQABwsD8BBgBCAAmFiEElYDLTK4fWpv8KBAL+s65tbaLcqIFAmh0qvsFCQWj
moACGwwACgkQ+s65tbaLcqIyMQwAgFFV1SlW8OjEjDrWaMeBUBVIcxdx8ntziSyW
2d92DjjprQUZawykLUy1RPfGSlq8X2i1egcA6zmx9Vuyc3euVB7AVpvIWRobHzKm
jxndpqvAXjDmRczr/P8NNM5wl4rQ9qbDl4nMQTlDxWnJUoNknjNoe8Vmo10npKFi
MWJwPyfjjQlpE8MJDA+XF0d7D8ArqtHORzW8pCOlkS+alXPJILeljQK5I28jgySe
F+RQZLzOJat2If5ShCT/ycBRQPprTXP3iVS6oixzwilbdgggtPCQ3thjVXXHvbPt
5/izTWHzYVIQC1nkmgZ6sss5PufAlnG/ai04S8S/fc+P82cF9MGDhSOEN8mttAhi
jznYgY4BWTrxVoeTDFjb+3v0M5FyAvh8UCYZmYMiOpZ+jOG7XRO7BCSFXjPfdpAy
NdWSplbRBZ8vVYPazS2utoPKi4fVoNRwFZMRUKBPQ5dp9TCKz7fwus1INACjnd0D
v4e7HRKu/kKVnLN8LcehgjAmt9NY =vDuo

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

File PGP *key* ini tersedia pada :
https://dsi.ut.ac.id/csirt/publickey

2.9. Anggota Tim

Keanggotaan CSIRT-UT ditetapkan oleh Keputusan Rektor Universitas Terbuka Nomor 1259 Tahun 2025 tentang Computer Security Incident Response Team Universitas Terbuka (CSIRT-UT).

2.10. Informasi/Data lain

- Tidak Ada -

2.11. Catatan-catatan pada Kontak CSIRT-UT

Metode yang disarankan untuk menghubungi CSIRT-UT adalah melalui *e-mail* pada alamat csirt-ut@ecampus.ut.ac.id atau melalui nomor telepon 021-7490941 ext. 1401 ke Direktorat Sistem Informasi (DSI) pada hari kerja jam 08.00 - 16.30 atau siaga selama 24/7.

3. Mengenai CSIRT-UT

3.1. Visi

Visi CSIRT-UT adalah menjadi tim respons insiden keamanan siber yang andal, proaktif, dan terdepan dalam menjaga integritas, kerahasiaan, dan ketersediaan sistem informasi untuk mendukung ekosistem pembelajaran digital yang aman dan terpercaya di Universitas Terbuka.

3.2. Misi

Misi dari CSIRT-UT, yaitu :

1. Melindungi sistem informasi Universitas Terbuka melalui deteksi dini, respons cepat, dan pemulihan insiden siber untuk menjaga integritas, kerahasiaan, dan ketersediaan layanan digital.
2. Meningkatkan kesadaran dan budaya keamanan informasi di seluruh sivitas akademika melalui edukasi, pelatihan, dan sosialisasi berkelanjutan.
3. Membangun tata kelola keamanan siber yang adaptif dan kolaboratif, selaras dengan standar nasional dan internasional, guna mendukung transformasi digital UT yang aman dan terpercaya.
4. Mendorong budaya keamanan siber (*cybersecurity awareness*) di seluruh sivitas akademika dan tenaga kependidikan Universitas Terbuka melalui edukasi, sosialisasi, dan kebijakan pengamanan informasi yang konsisten.

3.3. Konstituen

Konstituen CSIRT-UT meliputi :

a. Mahasiswa
b. Dosen dan Tenaga Pendidik
c. Tenaga Kependidikan (Staf Administratif)
d. Manajemen Universitas
e. Unit/Lembaga Teknologi Informasi
f. Alumni (jika masih memiliki akses sistem kampus)

3.4. Sponsorship dan/atau Afiliasi

Pendanaan CSIRT-UT bersumber dari Dana PAGU PTNBH/Universitas Terbuka.

3.5. Otoritas

1. Memiliki mandat untuk menangani insiden siber di lingkungan universitas (sistem, jaringan, data, dan aset digital).
2. Akses terhadap sistem dan log untuk investigasi insiden.
3. Menentukan prioritas penanganan insiden berdasarkan tingkat keparahan dan dampaknya.
4. Mengambil langkah mitigasi langsung, seperti isolasi jaringan, blokir akses IP, atau pemutusan sementara layanan terdampak.
5. Menerapkan kebijakan keamanan, termasuk patching, update sistem, dan penguatan kontrol akses.
6. Berhak melakukan koordinasi lintas unit (TIK, Fakultas, Prodi, Pimpinan Unit).
7. Menghubungi pemilik sistem atau pengguna yang terlibat dalam insiden untuk klarifikasi atau edukasi.
8. Menjalin kerja sama teknis dengan pihak luar seperti BSSN, ID-SIRTII, penyedia layanan cloud, ISP, atau tim CSIRT lain.
9. Menyusun dan menyampaikan laporan insiden ke pimpinan universitas.
10. Menyampaikan peringatan atau himbauan keamanan kepada seluruh sivitas akademika.
11. Berhak melakukan pengujian keamanan sistem (penetration testing) setelah mendapat persetujuan dari pihak terkait.
12. Memberikan sosialisasi dan pelatihan keamanan siber.

13. Mengembangkan pedoman penggunaan TIK yang aman untuk dosen, mahasiswa, dan tenaga kependidikan.

4. Kebijakan – Kebijakan

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

CSIRT-UT melayani penanganan insiden siber dengan jenis berikut :

a. Web Defacement: Perubahan atau perusakan tampilan situs web kampus oleh pihak tidak berwenang.
b. DDoS (Distributed Denial of Service): Serangan yang membuat situs atau layanan kampus tidak dapat diakses.
c. Malware: Perangkat lunak berbahaya yang dapat merusak sistem atau mencuri data.
d. Phishing: Upaya penipuan untuk memperoleh informasi sensitif seperti kata sandi atau data pribadi.
e. Pembajakan Akun: Akses ilegal ke akun pengguna kampus.
f. Akses Ilegal: Masuknya pihak tidak berwenang ke sistem kampus.
g. Spam: Pengiriman pesan tidak diinginkan dalam jumlah besar

Tingkat/*Level* Dukungan, meliputi:

1. **Pemberian Peringatan Terkait Keamanan Siber**: Memberikan informasi mengenai potensi ancaman siber yang dapat mempengaruhi sistem elektronik dan informasi yang dikelola oleh UT.
2. **Penanganan Insiden Siber**: Menyediakan koordinasi, analisis, rekomendasi teknis, dan bantuan kunjungan ke lokasi dalam rangka penanggulangan dan pemulihan insiden siber.
3. **Penanganan Kerawanan Sistem Elektronik**: Melakukan koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan sistem elektronik UT.
4. **Penanganan Artefak Digital**: Memberikan dukungan dalam pemulihan sistem elektronik terdampak dan investigasi insiden siber.
5. **Pemberitahuan Hasil Pengamatan Potensi Ancaman**: Memberikan informasi terkait potensi ancaman siber yang terdeteksi melalui sistem monitoring keamanan.
6. **Pendeteksian Serangan**: Melakukan pemantauan terhadap serangan siber yang terjadi dan memberikan respons yang sesuai.
7. **Analisis Risiko Keamanan Siber**: Melakukan identifikasi kerentanan dan penilaian risiko terhadap sistem elektronik UT.
8. **Konsultasi Terkait Kesiapan Penanganan Insiden Siber**: Memberikan konsultasi mengenai kesiapan UT dalam menghadapi dan menanggulangi insiden siber.
9. **Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber**: Melakukan sosialisasi dan pelatihan untuk meningkatkan kesadaran dan kepedulian sivitas akademika UT terhadap keamanan siber.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

1. Kolaborasi dengan CSIRT Lain dan Organisasi Terkait

Kolaborasi dengan CSIRT lain baru dilakukan dengan pihak BSSN.
Sedangkan kolaborasi organisasi terkait dalam lingkup keamanan siber, UT bekerjasama dengan beberapa penyedia (Pihak ke-3). Dengan ruang lingkup pekerjaan seperti : Pentest dan Pengadaan perangkat Firewall.

2. Partisipasi dalam Seminar Keamanan Siber

CSIRT juga aktif berpartisipasi dalam seminar nasional untuk berbagi pengetahuan dan pengalaman. Misalnya, mengirimkan pegawainya untuk mengikuti Seminar Nasional dan Munas II Acad-CSIRT 2022.

3. Pelatihan dan Workshop Bersama

Beberapa perguruan tinggi menyelenggarakan pelatihan dan workshop bersama untuk meningkatkan kompetensi civitas akademika dalam menghadapi ancaman siber.

CSIRT-UT harus menjaga kerahasiaan informasi yang diterima. Sebagian besar CSIRT-UT di perguruan tinggi memiliki kebijakan untuk merahasiakan informasi yang diterima, kecuali jika ada izin eksplisit dari pihak yang bersangkutan atau jika diharuskan oleh hukum.

4.3. Komunikasi dan Autentikasi

Untuk memastikan keamanan dalam berkomunikasi, CSIRT-UT di perguruan tinggi menggunakan metode autentikasi dan enkripsi yang sesuai. Beberapa CSIRT-UT menggunakan email terenkripsi dengan PGP *(Pretty Good Privacy)* untuk komunikasi yang memuat informasi sensitif atau terbatas. Selain itu, mereka juga dapat menggunakan email biasa dan telepon untuk komunikasi yang tidak memerlukan tingkat keamanan tinggi .

5. Layanan

5.1. Layanan Utama

Layanan utama dari CSIRT-UT, yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Memberikan informasi tentang potensi ancaman siber, kerentanan, dan serangan yang mungkin terjadi kepada seluruh pihak terkait. Penyebaran peringatan dilakukan melalui berbagai saluran komunikasi seperti email, notifikasi, atau portal keamanan internal untuk meningkatkan kesadaran dan kesiapsiagaan.

5.1.2. Penanganan Insiden Siber

Menyusun panduan teknis mengenai langkah-langkah penanganan insiden siber untuk memastikan respons yang efektif dan konsisten. Panduan ini mencakup prosedur identifikasi, isolasi, mitigasi, dan pemulihan dari berbagai jenis insiden siber.

5.2. Layanan Tambahan

Layanan tambahan dari CSIRT-UT, yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

- Melakukan identifikasi dan mitigasi kerentanannya untuk mencegah potensi eksploitasi.
- Penyusunan rekomendasi teknis untuk penguatan sistem.

5.2.2. Penanganan Artefak Digital

Melakukan identifikasi artefak digital terkait dengan insiden, pengumpulan (collection), analisis artefak, pelestarian, dokumentasi dan pelaporan, pemulihan dan pencegahan, serta evaluasi dan pembelajaran.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

- Memberikan informasi terkait potensi ancaman siber yang terdeteksi melalui sistem monitoring keamanan.
- Penyebaran informasi ini bertujuan untuk meningkatkan kewaspadaan dan kesiapsiagaan.

5.2.4. Pendeteksian Serangan

- Melakukan pemantauan terhadap aktivitas mencurigakan dan serangan siber dalam jaringan dan sistem organisasi.
- Penggunaan sistem deteksi intrusi (IDS), pemantauan log, dan analitik perilaku untuk mendeteksi tanda-tanda serangan.

5.2.5. Analisis Risiko Keamanan Siber

- Melakukan evaluasi terhadap sistem, jaringan, dan aplikasi untuk mengidentifikasi kelemahan dan menilai dampak serta kemungkinan dari berbagai jenis ancaman.
- Penyusunan rekomendasi untuk mitigasi risiko yang teridentifikasi.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

- Memberikan konsultasi mengenai kesiapan organisasi dalam menghadapi dan menanggulangi insiden siber.
- Evaluasi terhadap rencana respons insiden dan pelaksanaan latihan simulasi serangan.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

- Melakukan sosialisasi dan pelatihan untuk meningkatkan kesadaran dan kepedulian sivitas akademika terhadap keamanan siber.
- Penyediaan materi edukatif dan penyelenggaraan webinar atau workshop terkait keamanan siber.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt-ut@ecampus.ut.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*

Batasan Tanggung Jawab:

- CSIRT-UT tidak bertanggung jawab atas kerugian langsung, tidak langsung, khusus, atau konsekuensial yang timbul akibat penggunaan atau ketergantungan pada informasi atau rekomendasi yang diberikan.
- Informasi yang disediakan bersifat umum dan tidak dapat dianggap sebagai nasihat profesional untuk situasi spesifik.

Ketepatan dan Kelengkapan Informasi:

- CSIRT-UT berusaha menyediakan informasi yang akurat dan terkini, namun tidak menjamin bahwa semua informasi bebas dari kesalahan atau kelalaian.
- Pengguna disarankan untuk memverifikasi keakuratan dan kelengkapan informasi sebelum menggunakannya.

Konten Pihak Ketiga:

- Tautan atau referensi ke situs web atau materi pihak ketiga disediakan untuk kenyamanan pengguna dan tidak menunjukkan dukungan atau afiliasi dengan CSIRT-UT.
- CSIRT-UT tidak bertanggung jawab atas konten atau praktik privasi situs pihak ketiga.

Penggunaan Informasi:

- Informasi yang diberikan oleh CSIRT-UT hanya boleh digunakan untuk tujuan yang sah dan sesuai dengan hukum yang berlaku.
- Pengguna bertanggung jawab penuh atas penggunaan informasi tersebut.

Perubahan dan Pembaruan:

- CSIRT-UT berhak untuk mengubah atau memperbarui informasi dan layanan yang disediakan tanpa pemberitahuan sebelumnya.
- Pengguna disarankan untuk secara berkala memeriksa pembaruan pada situs resmi CSIRT-UT.