RFC 2350 CSIRT-ITECH

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 29 Agustus 2025.

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.i-tech.ac.id/CSIRT-ITECH-RFC2350-Aug2025.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 CSIRT-ITECH;
Versi : 1.1;
Tanggal Publikasi : 29 Agustus 2025;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Incident Response Team Sekolah Tinggi Teknologi Informasi NIIT (I-Tech)
Disingkat : CSIRT-ITECH

2.2. Alamat

Jl. Asem Dua No.22, RT.11/RW.5, Cipete Sel., Kec. Cilandak, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12410

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 7515870

2.5. Telekomunikasi Lain

WA Resmi STTI NIIT 0897-0127001

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

csirt[at]i-tech[dot]ac[dot]id

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

Bits : 3072
ID : 0x1A48CD67CE01EC3F
Key Fingerprint : 8D3B 231A 98F1 925E 3A08 77EA 1A48 CD67 CE01 EC3F

Blok PGP Public Key Misalnya :
-----BEGIN PGP PUBLIC KEY BLOCK-----

xsDNBGi+UgcBDAChm8d8Lv/o9WXQakJtWL2YM8gfwZgjeIyKMnSV00ianQ6D+3o1
5tAP/Gz6xv5zjWN0/Swm0qV7shEa7mDgniCM1TadgLKfT8qHgNFRQuMvgG0VSkmL
nwIzq1CYkDHAcZOyfNuCM6R9125hVjm1XdEzGk7kf+syogFOHulppvl8CEim5i9x
xzQwebJarNUPMPINx4YrsFio40I9noAeKE1bkcyW/sz8CpPaiUjwULTfiVxmY46J
KNM577rGB213huAtceMVOkZo/80TgOhvEaveMhGZWtGdvSDKwMfwOrw/DcxnmHV3
7cgFzNxVshBkFavYnfCmQ5SnOjI5iRwpBeHhMpd0XxhG43kmEpF0gljTQ2AmS6eS
UI6iAtqaLxt3YIKobhFrm0wLeT8Ui/oYa/V0nninaflCjZoSiq3M3P6ojWa+EZCO
1ow0cLnNii0pd3tRoe6FLVytkCmOd+Ide1jDoxGcWEuc1kGXN8SkUKvO/DesquRO
N+i+WGq5ZOuvMuEAEQEAAc0kQ1NJUlQgU1RUSSBOSUlUIDxjc2lydEBpLXRlY2gu
YWMuaWQ+wsENBBMBCAA3FiEEjTsjGpjxkl46CHfqGkjNZ84B7D8FAmi+UggFCQWj
moACGwMECwkIBwUVCAkKCwUWAgMBAAAKCRAaSM1nzgHsP2QFDACZwFzs0cKUsdxn
IqP6738WURnSK2PrZrU0v88BWskMsD8gwApN08CgQQjvBeEKRJKXGvr6bDsMyNH7
jo+PLGC4SPKIlaKbbeYimMaIRmCPUv2m+OOKayVAL/dZcVh1wlR86mMXiK6PlHYq
wvth7ci+ySwxW4IQC3oW49tq40SL7aMo3oOPSC2vcmnVuhGXUHBol/63UlXklFiZ
OfgmEwTeHz+0x5LLxdritQM8bgXfGSV0TQp0OLkUnVzqquK+uSqMgop2X7VWTu8R
4eMzaWABFF3D6NISO/Zzvc/1aWpgzbqOQShvmUDxsuXcJ9o5vwo5n9XSkKeCNfFW

K6msYK4oh6I4DX4SEWe8iR+7GMoJDJmuQGACIwZxPzpCrTT5DlHLEhqYbc+Uu
F05
6vV9lcW4c0pcy5IIrYF692kUrdUKYlHyM4iJnEY2tyKtp/Zx5oFgu6Un2ZVHJsOm
lbXquM3ry5eM2gkw+CsGG3w+o0v79h5+Nol1ZlCtV1iyn3qXotPOwM0EaL5SCQE
M
ALjyVYqvx1FZfwu/3fyEFCh+Tol4XFNRX3SqzYe0u01RnSplF7we9yHiGkbAVdnC
mw59toE2pbijJWQxJtXNuaIGAL/R9gX776kfnUO1qQrqr/zMow0W/FyqZon5RENv
bG0eDdV4zdv1xP1N5KtFhB0hGDoH1diFC5oISfZVxNMdWmG4rLuZAvF10r/cm0fn
edHJURiXoiKBQl31ClL8lzTHzwssOJxKsgFRAmyggkVuhjgZJjxKNKwarZvZuVLf
y3dK5Fd4jUOCwmUGNnRgzxISl7whU9nK+U1G9jmPoRtXZ+Jd8/XZC9o3J/4VcXZ
B
IXKVXwj9dlbHhBmihQtT7zyDArFVDVNEqOWtPgCPjHN2q/PbS40j7P8RT/ySJNFs
ByUUxb2AKH8S0Jmj5yPfN676+RxlvOxoB4BSS+K4QRo+04mS/Yn/SWEr33YUHP
UI
SuwUB6tLDwBPTbulRLqwxcvPmmej6eOQT4MAHAr622a+5KxLFNlRJ1vXQbRtPjJ
i
gwARAQABwsD8BBgBCAAmFiEEjTsjGpjxkl46CHfqGkjNZ84B7D8FAmi+UgkFCQ
Wj
moACGwwACgkQGkjNZ84B7D85AgwAiU8E/qnVl1ofzi8bxw7fcYUzYbhxPljPLFRW
jqhbAUdPotbUAirN0VM/4x84rodLgyQJ0QYMnulloH4Y4LsBPJAIqPUE6oFj78MK
HoZ6g38Wxgc/r+rtJIzjcxVXPxnHXbsWF+YpNyxy2D98rhZdP5SuaDVfHibxuDPY
iYcUpO8nwqwNK2/v/lCsFl6wPNh/RM6wAWyl3JD/REGMXyBoC50qq8ocyDWesbj
Y
ZFplFp6lBkk0jzi9L4pJErNOuGrIUpd/XI50aVMUq/M8+xBJDc9v6rKS8slQNQVf
14WISBS0c4zoVQHc/3pBu2JQ4Woqb+ffWiF1q/hXYn4tQlhuORRPl8otZuAhSekP
cKvhqtnnQyfTrJ9UOMUun/vHYfCh93DDrZxbz99lA76hi3PnIvHEih0cNwBDnIX0
emtHeB5xyLAR6DwrMxptEhauzc+H+9cPt0fpW5f9iPdOMNoQyfHN4AOQGKrSLF+
A
Es7HtCVfTNVfUyShILEjKPBggO0l
=hQBn
-----END PGP PUBLIC KEY BLOCK----

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

2.8. Anggota Tim

Ketua CSIRT-ITECH adalah Kepala Bagian Layanan Teknologi Informasi dengan anggota tim terdiri dari Kepala Program Studi Teknik Informatika, Dosen dan Staff Layanan IT Sekolah Tinggi Teknologi Informasi NIIT.

2.9. Informasi/Data lain

Tidak ada

2.10. Catatan-catatan pada Kontak CSIRT-ITECH

Metode yang disarankan untuk menghubungi CSIRT-ITECH adalah melalui *e-mail* pada alamat csirt[at]i-tech[dot]ac[dot]id atau melalui WA Resmi STTI NIIT 0897-0127001 pada hari kerja Senin-Sabtu jam 08.30 - 16.30 WIB.

3. **Mengenai** CSIRT-ITECH

3.1. Visi

Visi CSIRT-ITECH adalah terwujudnya ketahanan siber yang handal dan profesional di lingkungan Sekolah Tinggi Teknologi Informasi NIIT (I-Tech)

3.2. Misi

Misi dari CSIRT-ITECH, yaitu :

a. Menyediakan respons yang cepat dan efektif terhadap insiden keamanan siber untuk melindungi aset informasi, menjaga integritas data, dan memastikan kelangsungan operasional di STTI NIIT
b. Mengimplementasikan langkah-langkah pencegahan yang proaktif untuk mengurangi kemungkinan terjadinya insiden keamanan.
c. Menyediakan pelatihan dan sumber daya untuk meningkatkan kesadaran keamanan siber di kalangan staf, mahasiswa, dan pemangku kepentingan lainnya.

3.3. Konstituen

Konstituen CSIRT-ITECH adalah seluruh civitas akademika di lingkungan Sekolah Tinggi Teknologi Informasi NIIT (I-Tech)

3.4. Sponsorship dan/atau Afiliasi

Pendanaan CSIRT-ITECH bersumber dari Sekolah Tinggi Teknologi Informasi NIIT (I-Tech)

3.5. Otoritas

Memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada lingkungan Sekolah Tinggi Teknologi Informasi NIIT (I-Tech).

4. Kebijakan – Kebijakan

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

CSIRT-ITECH melayani penanganan insiden siber dengan jenis berikut :

a. Web defacement
b. DoS / DDoS
c. Malware
d. Phising
e. Pembajakan akun STTI NIIT
f. Akses ilegal
g. Spam

Dukungan yang diberikan oleh CSIRT-ITECH kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

CSIRT-ITECH kan melakukan kerja sama dan berbagi informasi dengan CSIRT dari Kementerian dan atau Lembaga lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh CSIRT-ITECH akan dirahasiakan

4.3. Komunikasi dan Autentikasi

Komunikasi dan Autentikasi untuk komunikasi biasa CSIRT-ITECH dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon.

Komunikasi terkait laporan insiden dan pertukaran informasi ancaman insiden lainnya dapat menggunakan saluran komunikasi yang disediakan (e-mail dan whatsapp) yang telah terenkripsi atau dilengkapi dengan kata sandi.

5. Layanan

5.1. Layanan Utama

Layanan utama dari CSIRT-ITECH yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini bertujuan untuk memberikan informasi dan peringatan kepada organisasi atau individu mengenai potensi ancaman dan kerentanan yang dapat mempengaruhi keamanan sistem informasi mereka. Pemberian peringatan ini mencakup beberapa aspek, antara lain:

- **Monitoring Ancaman:** CSIRT-ITECH secara aktif memantau perkembangan ancaman siber, termasuk malware, serangan phishing, dan kerentanan perangkat lunak. Informasi ini dikumpulkan dari berbagai sumber, termasuk laporan keamanan, komunitas siber, dan penelitian.
- **Pemberitahuan Dini:** Setelah mengidentifikasi ancaman yang relevan, CSIRT-ITECH akan mengeluarkan peringatan dini kepada pihak-pihak yang berpotensi terpengaruh. Peringatan ini dapat berupa buletin, email, atau notifikasi melalui platform tertentu.
- **Rekomendasi Tindakan:** Selain memberikan informasi tentang ancaman, layanan ini juga mencakup rekomendasi tindakan yang dapat diambil oleh organisasi untuk melindungi diri mereka. Ini bisa termasuk pembaruan perangkat lunak, penguatan kebijakan keamanan, atau pelatihan bagi karyawan.
- **Edukasi dan Kesadaran:** CSIRT-ITECH juga berperan dalam meningkatkan kesadaran tentang keamanan siber melalui seminar, workshop, dan materi edukasi lainnya, sehingga organisasi dapat lebih siap menghadapi ancaman yang ada.

5.1.2. Penanganan Insiden Siber

Layanan penanganan insiden siber berfokus pada respons dan pemulihan dari insiden keamanan yang telah terjadi. Proses ini melibatkan beberapa langkah penting, antara lain:

- **Deteksi Insiden:** CSIRT-ITECH membantu organisasi dalam mendeteksi insiden keamanan siber melalui analisis log, pemantauan sistem, dan penggunaan alat deteksi intrusi. Deteksi yang cepat sangat penting untuk meminimalkan dampak dari insiden.
- **Respons Insiden:** Setelah insiden terdeteksi, tim CSIRT-ITECH akan segera merespons dengan melakukan analisis untuk menentukan sifat dan skala insiden. Ini termasuk mengidentifikasi sumber serangan, jenis data yang terpengaruh, dan potensi kerugian.
- **Mitigasi dan Pemulihan:** Tim akan mengambil langkah-langkah untuk mengurangi dampak insiden, seperti memutuskan akses ke sistem yang terpengaruh, menghapus malware, dan memperbaiki kerentanan. Setelah mitigasi, fokus beralih ke pemulihan sistem agar dapat beroperasi kembali dengan aman.
- **Pascainsiden:** Setelah insiden ditangani, CSIRT-ITECH melakukan evaluasi untuk memahami penyebab insiden dan mengidentifikasi langkah-langkah pencegahan yang dapat diambil di masa depan. Ini termasuk pembaruan kebijakan keamanan, pelatihan tambahan untuk staf, dan peningkatan infrastruktur keamanan.
- **Laporan dan Dokumentasi:** Layanan ini juga mencakup penyusunan laporan insiden yang mendetail, yang dapat digunakan untuk analisis lebih lanjut dan sebagai referensi untuk perbaikan di masa mendatang.

5.2. Layanan Tambahan

Layanan tambahan dari CSIRT-ITECH yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini berfokus pada identifikasi, analisis, dan mitigasi kerawanan yang ada dalam sistem elektronik, termasuk perangkat keras dan perangkat lunak. Proses ini meliputi:

- **Identifikasi Kerawanan:** Melakukan pemindaian dan analisis untuk menemukan kerentanan dalam sistem yang dapat dieksploitasi oleh penyerang.
- **Penyusunan Rencana Mitigasi:** Mengembangkan strategi untuk mengatasi kerawanan yang teridentifikasi, termasuk pembaruan perangkat lunak, penguatan konfigurasi, dan penerapan kontrol keamanan tambahan.
- **Uji Coba dan Validasi:** Melakukan pengujian untuk memastikan bahwa langkah-langkah mitigasi yang diambil efektif dalam mengurangi risiko.

5.2.2. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini bertujuan untuk memberikan informasi terkini mengenai potensi ancaman yang dapat mempengaruhi organisasi. Proses ini meliputi:

- **Monitoring Ancaman:** Memantau berbagai sumber informasi untuk mengidentifikasi ancaman baru yang muncul, termasuk tren serangan dan teknik yang digunakan oleh penyerang.

- **Pemberitahuan kepada Klien:** Menginformasikan klien tentang potensi ancaman yang relevan, termasuk rekomendasi untuk mitigasi.
- **Edukasi dan Kesadaran:** Memberikan informasi tambahan untuk meningkatkan kesadaran tentang ancaman yang ada dan cara melindungi diri.

5.2.3. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini bertujuan untuk meningkatkan kesadaran dan kepedulian terhadap keamanan siber di dalam organisasi. Ini mencakup:

- **Program Edukasi:** Mengembangkan program pelatihan untuk karyawan mengenai praktik terbaik keamanan siber, termasuk pengenalan terhadap ancaman dan cara melindungi informasi.
- **Kampanye Kesadaran:** Melaksanakan kampanye untuk meningkatkan kesadaran tentang pentingnya keamanan siber di seluruh organisasi.
- **Evaluasi dan Umpan Balik:** Mengukur efektivitas program kesadaran dan melakukan penyesuaian berdasarkan umpan balik dari peserta.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt[at]i-tech[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
c. Atau sesuai dengan ketentuan lain yang berlaku

7. *Disclaimer*

Penanganan insiden tergantung dari ketersediaan sumber daya yang dimiliki oleh Sekolah Tinggi Teknologi Informasi NIIT (I-Tech).