RFC 2350 CSIRT ITS

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 2 Mei 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://www.its.ac.id/dptsi/keamanan-siber/rfc2350-csirt-its/ (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 CSIRT ITS;
Versi	: 1.0;
Tanggal Publikasi	: 2 Mei 2024;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Incident Response Team Institut Teknologi Sepuluh Nopember.
Disingkat : CSIRT ITS.

2.2. Alamat

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI), Kampus ITS Sukolilo, Gedung Pusat Riset Lantai 4, Jl. Teknik Kimia, Keputih, Sukolilo, Surabaya, Jawa Timur, 60117

2.3. Zona Waktu

Surabaya (GMT+07:00)

2.4. Nomor Telepon

031-5947270

2.5. Nomor Fax

031-5922947

2.6. Telekomunikasi Lain

Tidak ada

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

csirt@its.ac.id

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

Bits : 4096
ID : CSIRT ITS
Key Fingerprint : 09C168290788BECE0A188A5A471A93977EAD8970

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

mQINBGYvk0MBEAD78pSxwoBbKjZZrNLpV8KZZI4YP7n4bZDGv+cv8/esHVSXi1py
RmPXxGaam0pbAoqzqsmzK+fa81nT+vZrVgQtiZx5VQnNY9/F30+/d7N3W7TkuVwS
578/bIEWcTCg6Tlzf7ullL3gBHfCVP720jyLpGf+kUpIth+lAAJqBzBYP0YG1FKn
//zoxFubY+TJKNH1uS6x44E6rFOMX2Z7QHTGwrMZTPptRr3eMoppuuKsR1Ct9C7Y
UJRxuge/orvRG8jy2gt4zHbJYP6sLdFVdZt5jeNUPk/QV0SAW0iJTIb4GRvAqvH0
gs8W9S9qhfuQPBY27pStVEfe4Lk8NilRnnb5NBegBj6X2aHPyMiYzelEO4/oA8aw
HIqaVw2nWr6SYNleILOLWX3zuBHqaKkeKCtfTA0o2vlQ7KsGdV0se7aH6SNd5CQ7
sb3MhLGtvzmaHLVl35drrVwKm0CKTjoC72koEok5qQCblbXr5RySMllc3ulUstLz
2tUrHjEGqCvQlzZ/OJVUAma5z6pth6s2Tk/xxKyBMNTt7nmyS5fWm+lst2Fr/b2S
B2bJVpqmMH7MJrkPr0lTJM0WY52xq73+mPw7JJqo46u30f3WwIlEQgHYA+XnnDT6
hU2hoFtRSIiuXstZtO/1rHN8XiLD0k2sw+4M7w2vwGRoOl3uP4pXG2FU8wARAQAB
tBtDU0lSVCBJVFMgPGNzaXJ0QGl0cy5hYy5pZD6JAk4EEwEKADgWIQQJwWgpB4i+
zgoYilpHGpOXfq2JcAUCZi+TQwIbAwULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAK
CRBHGpOXfq2JcI3dD/oCX+kvcWsqJOvXBxL4Yxy3sOnvUaOi7hRm7SnsFxb51a2u
9UN03j3AzwIRI8MFIpwJlKRe596oYEmttbhEtO2Ek1iGv9ci0Emj+Lv6gZ1LFYy6
f68s4JQ7AMSeTgtZX9XPrMi70svOqtghflkiVmTXVS2Kk9Gb1iv0hes+wR9Bc+BK
RoNoMAdslSC1sbzvzaJ1/oPJ/Ky3WCLCCF5GCN/u4XotkNkCw0EjTpgjhbXjlQ9X
B/K8FZdr7goEgI9WOZZympmd4NMUAKyEdRwhBsmOH8QRPX7NfGweUWFzEsIxHxdD
wh1cCjfBFStCrBjeQHloxOI+4wA23bVfJMeY0SF2tEaZH5a5cXvimi49kKwfLzyN
3GTS/7ZpXrCa6j7Nw6QiP1zKFBmGJt9w8scXqRdj8ulZ6c6PT7VzaPNhyxMAkQ0l
pGyl1HIDbJHQvziPih06ofu7cSn47fMFN2ca8AQCE5YcJVylq75/cvIzysDYTda/
YlCrsuqvO7put4jqHCl5lQ5dw3Er/Vy5i8bOo+6SrcnWmx1WnYLCw0iR9qLXqOS1
cRPd8rvfs/vICrEVzFSLicZAlfmzmiA32jRKGcIGVjQyarXzr843j97La9nDmrs3
dXehcTBw+Wlfl2DsS0Wzi3kzMwwS8L07sRqb8SfSe98MZMvH5NCM9wEMG+MASrkC
DQRmL5NDARAAyAwVlLyDkROWkB2DldZIGQBa3eYlHXebZZ1tuGMkPjBQSIVyXH0l
ckW2ikfdpItKOqgppcfFULnG5LtCtZid2tRF3AfecT9zICqyF+fcah7t3Ysi9L8M
f1uZ2ZQT/d6FefImATAsTvek0LKRBQAkPT/Q4QbjzphqLOiBVEGzPm3+bTwKnF/r
/VHED7FCLsse33wrqQMtiDtVRk6WVJ0O2o9pI2vHKlgJEMYueLr/XzXT/TYdCzoH
pBfFe+r/lD/NftD1T+6DemEkCjmbnj4gQ4oLaJeXTIcA5z7pHHDv54FOA57bkLaP
NxV39WEv89FHMALzZGIZJ7KyGvJq4/LzyGk0lN6H6CDyiCx8vtPrLdxOm8tOa10A
wCypKuQC3lLTMl43Km2r3ZhAep8wPzlscSzqjpa8dH5rBCbMI4Is/Erg6vq/VbUR
ALvOeZzEPUJf1ejMRcphvtHIvHxwOzwNlxBq8a8NCWXkw0mrED/7Xk7YTeaC6LC0
NbcU+Brh7Tv4Pv7nsU2UrskeIPJYTa/Cjk+lWpN0Cksbm2675JyTnbfFSpNHEGcb

T5/t6/1tEx+fp0I6c3sX+KXIK9nTxxVrVD5empNKphCv/ytRh+GNphPjdrAhmDue
vSLRms3HURH+OyFriWT0UG/8PoYHMUofzbjbqSyJ2e0JzQ/DPgMda0cAEQEAAYkC
NgQYAQoAIBYhBAnBaCkHiL7OChiKWkcak5d+rYlwBQJmL5NDAhsMAAoJEEcak5d+
rYlwOmoQAJqFJiQvUcRwANdLScKMvNwWqlOCqzzfaXUlTadvrQmPTcTK4ysu/3Hv
Ne+UZ9N16WwocpymqmKj0s0rkv0dOz1B6BEp8kDV2uDJseLlRQmZ9vr+PcFZ1zee
7FVVM87dUPHZ00VsIDj8XHB1agRQ5l2YCGoBlI+JHGIzE9sNglrRa8MVrDfp8AqY
fBqE7bHNCi5nexRshjbtVh+1HVtZlPQANOJ0Fk5bVcIBHjUxU1huQL4llf/IRXR/
LeivXNTKwAr6ijPcW0eOewXAr+Unuld3xix1lG4X9ciYfMM7S+YEE/x6cuU8673J
DEXoK/5sxGjYD4IpIqMMEIIeB6Owgu2BXHQ2wHdMDnqthPnImpK4GCsUesQ8n1Aw
2yRG5pbNDiz91KXotQnJyX33y+49k21YfYk9KjLsHL4VSPInCUbm/RH4xysJYEvI
HKE7Ix0rj/aburcJMEJJNBzzDruuFd5BO1xopnA+mNQUJnvRegawWFaHKyp5eLG3
ZR6NIJ0tGZP6D6EQQlzm2sxTNZ706TUJ9qgM9D+okn34Q0UoGtl9eUAnOnj9Iupx
aFFnS0oacBcTB5CdRv8BtDJbrRm+MIQZ4Xy/72aJAmJnCLR2JhkyI31p4yv9mNqK
PpN49RqoqePKHw14BAzNphRC+0mQzgbR89i5HfH2zIYJ8ATjaUjE
=QAwB
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://keys.openpgp.org/vks/v1/by-fingerprint/09C168290788BECE0A188A5A471A93977EAD8970

2.9. Anggota Tim

Keanggotaan CSIRT ITS ditetapkan oleh Keputusan Rektor Institut Teknologi Sepuluh Nopember Nomor 147/IT2/T/HK.00.01/I/2024 tentang Tim Respon Insiden Keamanan Siber Institut Teknologi Sepuluh Nopember Tahun 2024.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak CSIRT ITS

Metode yang disarankan untuk menghubungi CSIRT ITS adalah melalui aplikasi tiket yang bisa diakses di https://servicedesk.its.ac.id/ atau melalui e-mail pada alamat csirt@its.ac.id yang siaga selama hari kerja (Senin-Jumat) jam 08.00-16.00.

3. Mengenai CSIRT ITS

3.1. Visi

Visi CSIRT ITS adalah terwujudnya ketahanan siber pada Institut Teknologi Sepuluh Nopember yang handal dan profesional.

3.2. Misi

Misi dari CSIRT ITS adalah:

A. Mengoordinasikan dan mengkolaborasikan layanan keamanan siber di Institut Teknologi Sepuluh Nopember.

B. Meningkatkan keandalan layanan TIK Institut Teknologi Sepuluh Nopember terhadap ancaman keamanan siber.

C. Meningkatkan kapasitas sumber daya manusia terhadap ancaman keamanan siber pada aspek pencegahan, penanggulangan, dan pemulihan insiden keamanan siber di lingkungan Institut Teknologi Sepuluh Nopember.

3.3. Konstituen

Konstituen CSIRT ITS meliputi seluruh unit kerja dalam lingkungan Institut Teknologi Sepuluh Nopember.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan CSIRT ITS berasal dari anggaran Institut Teknologi Sepuluh Nopember.

3.5. Otoritas

A. CSIRT ITS memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada Institut Teknologi Sepuluh Nopember.

B. CSIRT ITS melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya.

4. Kebijakan – Kebijakan

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

CSIRT ITS memiliki otoritas untuk menangani insiden siber terhadap layanan dan aset ITS yang mengganggu konstituen CSIRT ITS dan integritas ITS dengan jenis berikut:

a. Web defacement
b. Serangan DoS/DDoS
c. Phishing melalui email ITS
d. Pembajakan akun ITS
e. Data breach
f. Malware
g. Akses ilegal
h. Spam
i. dan lain-lain

Dukungan yang diberikan oleh CSIRT ITS kepada konstituen dapat bervariasi tergantung dari jenis dan dampak insiden. Segala bentuk pengamanan dan perbaikan yang dilakukan CSIRT ITS juga tergantung atas ketersediaan sumber daya yang dimiliki. Dalam menjalankan dukungannya, CSIRT ITS juga berwenang untuk melakukan koordinasi antar unit kerja di ITS. CSIRT ITS juga menerapkan tindakan pencegahan yang diperlukan dan berkomitmen untuk menginformasikan kemungkinan kerentanan pada konstituen.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

CSIRT ITS akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam ruang lingkup keamanan siber. Dalam komunikasinya CSIRT ITS akan menjaga kerahasiaan informasi.

4.3. Komunikasi dan Autentikasi

Komunikasi biasa dengan CSIRT ITS dapat menggunakan layanan tiket servicedesk dan alamat email tanpa enkripsi data (email konvensional). Namun komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat melalui email dengan enkripsi PGP.

5. Layanan

A. Layanan Reaktif (Korektif/Perbaikan)

Layanan ini meliputi kegiatan tanggap Insiden dan peristiwa lain yang berkaitan dengan Insiden guna membatasi kerusakan yang disebabkan oleh Insiden. Layanan ini terdiri dari:

1. layanan pemberian peringatan dini terkait keamanan siber;
2. layanan tanggap insiden keamanan siber;
3. layanan penanganan kerawanan sistem elektronik; dan
4. layanan penanganan artefak.

B. Layanan Proaktif (Preventif/Pencegahan)

Layanan ini meliputi kegiatan mendeteksi dan mengurangi potensi Insiden dan Security Event lainnya dengan tujuan untuk mencegah terjadinya Insiden. Layanan ini terdiri dari:

1. Pemberitahuan hasil pengamatan terkait dengan ancaman baru yang dapat muncul akibat perkembangan teknologi, politik, ekonomi dan perkembangan lainnya; dan
2. Dalam hal diperlukan dan tersedianya sumber daya dapat disediakan layanan pendeteksian serangan.
3. Layanan security assessment
4. Layanan security audit

C. Layanan Peningkatan Kapabilitas Kesiapan Penanggulangan dan Pemulihan Insiden Keamanan Siber

Layanan ini ditujukan untuk meningkatkan kualitas keamanan internal. CSIRT memberikan wawasan dari sudut pandang dan keahliannya, sehingga kegiatan secara efektif dapat dilakukan melalui kolaborasi dengan organisasi internal. CSIRT secara tidak langsung juga dapat mencegah terjadinya insiden.

1. Analisis Risiko;
2. Konsultasi terkait kesiapan penanggulangan dan pemulihan insiden keamanan siber; dan
3. Pembangunan kesadaran dan kepedulian terhadap keamanan siber.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan melalui aplikasi tiket https://servicedesk.its.ac.id/ dengan melampirkan sekurang-kurangnya :

a. Foto atau hasil pindai kartu identitas
b. Bukti insiden berupa foto atau screenshoot atau log file yang ditemukan
c. Laporan deskripsi singkat kronologi kejadian, analisis singkat, dan detail informasi lain.

Persyaratan ini juga dapat menyesuaikan dengan ketentuan lain yang berlaku.

7. ***Disclaimer***

Penanganan jenis insiden tergantung dari ketersediaan sumber daya yang yang dimiliki.

Penanganan insiden hanya meliputi insiden pada layanan elektronik yang dikendalikan ITS.