RFC 2350 CSIRT ITB

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 04 Desember 2023.

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.itb.ac.id/rfc2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen telah ditanda tangani dengan PGP *Key* milik CSIRT ITB. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 CSIRT ITB;
Versi	: 1.1;
Tanggal Publikasi	: 11 September 2023;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Incident Response Team Institut Teknologi Bandung
Disingkat : CSIRT ITB.

2.2. Alamat

DTI Institut Teknologi Bandung
Kampus ITB, Gedung CRCS Lantai 4 – DTI, Jl. Ganeca No.10, Bandung 40132

2.3. Zona Waktu

Bandung (GMT+07:00)

2.4. Nomor Telepon

(022) 86010037

2.5. Nomor Fax

-

2.6. IT Helpdesk (Whatsapp)

+628111306666

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

csirt@itb.ac.id

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

Bits : 3072
ID : 0x70FC59D8B95E3612
Key Fingerprint : 5DAF 78B6 A885 5ED4 0D0C 44B8 70FC 59D8 B95E 3612


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

xsDNBGTA4QUBDACYRPa8yYvIAGKBJfhVGhgvmEEWa7q2qHTplLdqyrSRh+rasUPj
UjqjAi1U76Z9meRfDnviCWrv0i68hmSeJy15k7pXr/yBaZPwlyZCNP+ssyy/jQ1f
Osptkj2TmK2BeLwZbEbbod8eolIxxK/VviUKk0zC92TbTGlBU250UqEg5PbBHOTu
w/GPyFTZZQmJ6jpx6r2zhFiBRIIshSTMwS0xlVA9RFGqQFEdqJNVT9EVtju0tpjX
V65b1ReiwEzcSpWNW3cb9BCCndyeTwxUKTHBiz+r6OXnqtoQ0uNiP3b7AD16YWLR
t9RRmL1rPRfU1f+ZXNzF/71iWl+bcKK5/qlHSvQInp4jmV5q6L8AxdV9eg23+B4R
sdqezwyK08sfBIirQjHc6lfEtKHsuhP0av8og9+N5NRfFM0qJpbkVMvS3bluPJvI
0OAaUmLa5M8LAm2VgIWBYKtHqRjlEiz1Y9XirbE4MuhX8Tc3tWwiRw4OYn9MpewR
+p6xbcy5sa/IxmcAEQEAAc0bQ1NJUlQgSVRCIDxjc2lydEBpdGIuYWMuaWQ+wsEH
BBMBCAAxFiEEXa94tqiFXtQNDES4cPxZ2LleNhIFAmTA4QUCGwMECwkIBwUVCAkK
CwUWAgMBAAAKCRBw/FnYuV42EqnQC/0YdGN7KGDWmn6v+GGvtrK2nf7GV6CyYfkB
0vSW/JxmOf6rwMt5Q05vooprUs3ZX3DDPg/lj1/YFZnNhvHXZbGBmUBfpXheAxlg
Hs2NryxeWVPNT0uO/nrKAOQbU5mO4129ZVmMq1YtOmjvtLR8IL5boNBipGrVZjsk
vxmw9KBkF30dr7GYbsgVtMg8HoM1A6oqfF7auTH9YqZzXAs38Vqlcf41Vdj10BLo
xF4/71Fx2Xa4curijn5KPxe9X2zwsEtK0EbjxjuZ6flqMOPXAGTtlQtlPGC8a5EL
BDaHvjn3YC4eAmjenT9f41U2WPFHRKll2UjsrsXpZNicJqJb7QWU4JREmiUnHYnD
5SDDEGpmknFPd0grnH+pLnAhKdOrbQjQDnCaHC5sj67jPFQZDSbYvr79Tl7sCIjC
TIC/iFfWe381lkdu7ELyjWcmQuKnQAsyQ4pYHscQ9cMO8tUP4kkJcM5kNafiEhKM
m49Lf1Jp9aO1LhVXeeKx9G6/Oa3Fy/vOwM0EZMDhBQEMAOEj2sHxI/BOPAgO2Lhx
af919KOZ3qAXYn9Aor4hciyPJnWHKZHXROuR4lwb8Iz4IqulSCXdryBK37Fctn25
UxR1dFpYRr9fkfZsyikjbiDU25mX2q93c/csC2Q5x5fF3JVVdLnHbBfTv/z+ZG/g
37ciIQv/G8lY7s2XeZT+QuPvLuCnBTA92/QQYsgbg3h06CXgv3fTXgWFSW1V2Lfo
oOejNKymMeBV0Y3X5NBe1NHVz9uRHNhV1ilfEa7BjKRm1g8kJpqzhX0L0L7G8tLO
AloitltuGKHcVlyrEKcWIFmZfjY941+89c5rbajgEd1MPVhFEyAuW+GMX2FdpqcD
s1Xtk7gECeU0T7p/snKScrgSzNkG01KMULO+ldZXQ7kPbJZcxjI5dFrQdI9nOthw
QSdGaUUw6rAp3XOBGbuQEMttWKABnyldJ4l+PM8X1MKP6eTnhHEE1RhOYpXDTkMP
97t2BAeyO+LhIHqI9hryOGd840Iwc4KhTU2YDZaL/O5HWwARAQABwsD2BBgBCAAg
FiEEXa94tqiFXtQNDES4cPxZ2LleNhIFAmTA4QYCGwwACgkQcPxZ2LleNhK0agv9
E23vNXpeSwFgCwiOypk7bNXNxyJiXbKDlkWkW+FTCuMRdZ514XIqqm1BcfkCfJfF
uBINwWmD3RSHS8UBwLdkLPPFvHKL+YSflYGCW06/6npqPuatis81BZ0Q8DZ52fAn
24EHdagOjdGHtDYcNj8Mt/HjIKjyC+jA//YgC2Q2v8s/IGtBjpRu9pmlQw8cowQv
```

```
SNW8r3qxc/Er7f3CbfFWPwbXhF/Sd9zPxlPbrFvNq3mHYWzOFEuczCKug+JCDFCk
nMFc8p5L/zai7+P0k6Z920LaFQSw2dgLIS0T4FBzQibjhYQyaoAn7Dmve6EyXXGo
tPMFtK6iwZY6sD2yzBcLZmiISuoqlJQgyNMvjj+CvHUsvvNIFg6cGsb+6sMOhMPH
Zz87ZxaLDELKhUkSsVWdno0+QlMzg/HOWiJolNrHJzjpnAFeA5Ra4elBWALKX+Qj
hfXFWZyrFRh5z3Ys1KQ2srumolewAUiI+P7mJr5CCt17/DX/Vrh/KBuylkRbwb94
=pFc7
-----END PGP PUBLIC KEY BLOCK-----
```

File PGP *key* ini tersedia pada :
https://csirt.itb.ac.id/keys

2.9. Anggota Tim

Ketua CSIRT ITB adalah Direktur Teknologi Infomasi. Yang termasuk anggota tim adalah perwakilan di Sub Direktorat Perencanaan dan Pengembangan Teknologi Informasi dan Sub Direktorat Operasional dan Layanan Teknologi Informasi.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak CSIRT ITB

Metode yang disarankan untuk menghubungi CSIRT ITB adalah melalui e-mail pada alamat csirt@itb.ac.id atau melalui Whatsapp IT Helpdesk di nomor +628111306666 pada hari kerja jam 07.30 - 16.00 WIB.

3. Mengenai CSIRT ITB

3.1. Visi

Terwujudnya ketahanan siber yang handal di lingkungan Institut Teknologi Bandung

3.2. Misi

Misi dari CSIRT ITB, yaitu :

a. Mengkoordinasikan dan mengkolaborasikan layanan keamanan siber di Institut Teknologi Bandung baik dengan pihak internal maupun eksternal;
b. Mendorong kegiatan pengamanan informasi dan pencegahan insiden keamanan informasi;
c. Membangun kesadaran keamanan siber pada sumberdaya manusia di lingkungan Institut Teknologi Bandung;

3.3. Konstituen

Konstituen CSIRT ITB yaitu semua sivitas dan unit kerja di lingkungan Institut Teknologi Bandung.

3.4. Sponsorship dan/atau Afiliasi

CSIRT ITB merupakan bagian dari DTI ITB, sehingga pendanaan berasal dari RKA ITB.

4. Kebijakan – Kebijakan

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

Jenis-jenis insiden dan tingkat/level Dukungan CSIRT ITB memiliki otoritas untuk menangani insiden yaitu:

a. Web Defacement;
b. DDoS;
c. Malware;
d. Phising;
e. Pembajakan akun;
f. Akses Ilegal;
g. Spam;

Dukungan yang diberikan oleh CSIRT ITB kepada unit kerja dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

CSIRT ITB akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh CSIRT ITB akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, CSIRT ITB dapat menggunakan email tanpa enkripsi data (email konvensional) dan telepon. Namun, untuk komunikasi yang memuat data atau informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada email.

5. Layanan

5.1. Layanan Utama

Layanan utama dari CSIRT ITB yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik yang dikelola oleh masing-masing unit kerja di lingkungan Institut Teknologi Bandung.

5.1.2. Penanganan Insiden Siber

Layanan ini berupa koordinasi, analisis, rekomendasi teknis, dan bantuan *on-site* dalam rangka penanggulangan dan penanganan insiden keamanan siber di lingkungan Institut Teknologi Bandung.

5.2. Layanan Tambahan

Layanan tambahan dari CSIRT ITB yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini diberikan oleh CSIRT ITB berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (*hardening*), CSIRT ITB memberikan informasi statistik terkait layanan ini. Namun, layanan ini hanya berlaku apabila syarat-syarat berikut terpenuhi:

a. Pelapor atas kerawanan adalah pemilik sistem elektronik. Jika pelapor adalah bukan pemilik sistem, maka laporan kerawanannya tidak dapat ditangani;
b. Layanan penanganan kerawanan yang dimaksud dapat juga merupakan tindak lanjut atas kegiatan *Vulnerability Assessment*.

5.2.2. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini berupa penyampaian informasi kepada unit kerja terkait ancaman terhadap sistem elektronik yang dapat muncul akibat pengaruh dari perkembangan teknologi, politik, ekonomi, dan perkembangan lainnya.

5.2.3. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Dalam layanan ini CSIRT ITB mendokumentasikan dan mempublikasikan berbagai kegiatan yang dilakukan dalam rangka pembangunan kesadaran dan kepedulian terhadap keamanan siber.

6. Pelaporan Insiden

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

a. Identitas pelapor
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
c. Atau sesuai dengan ketentuan lain yang berlaku

7. *Disclaimer*

a. Terkait penanganan jenis *malware* tergantung dari ketersediaan *tools* yang dimiliki oleh Institut Teknologi Bandung.
b. Penanganan situs/website yang dikelola oleh Direktorat Teknologi Informasi bisa langsung ditangani oleh tim CSIRT ITB.
c. Penanganan situs/website yang dikelola oleh masing-masing Unit Kerja tidak bisa langsung ditangani oleh tim CSIRT ITB, harus oleh tim teknis situs/website masing-masing Unit Kerja.

Direktur Teknologi Informasi ITB,

INSTITUT TEKNOLOGI BANDUNG
DIREKTORAT TEKNOLOGI INFORMASI

Mugi Sugiarto, S.Si., M.A.B.