RFC 2350 CSIRT-UBBG

1. Informasi Dasar

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

1.1. Tanggal update terakhir dokumen merupakan dokumen versi 1.3 yang diterbitkan pada tanggal 22 Maret 2024.

1.2. Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

1.3. Dokumen ini tersedia pada tautan:
https://csirt.bbg.ac.id/download/rfc-2350/?wpdmdl=16572

1.4. Keaslian dokumen ini yang telah ditanda tangani Rektor UBBG.

1.5. Identifikasi dokumen ini memiliki atribut, yaitu:

1.5.1	Judul	: RFC 2350 CSIRT-UBBG
1.5.2	Versi	: 1.3
1.5.3	Tanggal Publikasi	: 22 Maret 2024
1.5.4	Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim adalah Computer Security Incident Response Team Universitas Bina Bangsa Getsempena disingkat dengan CSIRT-UBBG.

2.2. Alamat di Jl. Tanggul Krueng Lamnyong No.34 Rukoh, Kec. Syiah Kuala, Banda Aceh, Aceh, Indonesia.

2.3. Zona Waktu Banda Aceh (GMT+07:00)

2.4. Nomor Telepon (+62) 852-9709-7995 / (+62) 852-7020-3925

2.5. Alamat Surat Elektronik (*E-mail*) csirt[at]bbg.ac.id

2.6. Kunci Publik *(Public Key)* menggunakan file PGP key

```
Fingerprint:
324E1A683AB4D64010550A49D8FA5F8A051FE913
Key ID:
0xD8FA5F8A051FE913
```

Public Key:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
xsDNBGXn7uIBDADGm5sgLSdnB/5CFD6nxpmhwHpYYfObnSjkAySJvYWnaor8syWp
jOV2xFt4jTn6EPYdolDi7ZnZqiX/uE1wKzxctmHkpGLjdU9xT01fK2rHp4QltWbj
JfbQ9Exc4Vl1cT+Mi4UBdISLnOS88LoN7Qqomfxrv+pwQkC3pRK8MFVY2dp4IN7R
W3QEExuxGD2/CXFWEUKKGeydSNCG6KPAE4gKi29jHrvhuVtdvO/rl0sxEPM4RKtX
lqWyWW/8fsogP07zB5FZDCzBLqo1FHVFk4uVUVG3w77M+zW4r7HPX5x2iB0Xp0eW
3Uxp2rco0CgFDX5fMbQNzK0fuzbZCtw+MSGzRZhFE+cma0dGG4q56i/t1EEEN2m7
qFqYt8DnLVN6+idgcW+KQ/fJvitv2+eNFRMEt8n8ByYkj2VzueFbDsZOvE4ra/5+
T9QOno4V5eR1i8fxNQd/N2i/3EPqCF2GwCBGGRN8o0w436JMFIcvKLfqmvmlyctr
0H3THaf+TfEdqOkAEQEAAc0cQ1NJUlQgVUJCRyA8Y3NpcnRAYmJnLmFjLmlkPsLB
BwQTAQgAMRYhBDJOGmg6tNZAEFUKSdj6X4oFH+kTBQJl5+7jAhsDBAsJCAcFFQgJ
CgsFFgIDAQAACgkQ2PpfigUf6RNE5Av/YqPEFhSLGTqnDyaZdiIEBuU8Dz7icpX3
vSlGN5l8TQ1y0/Yyd1w1RYfpmcIyu+jt/FzWBhm9oAWn8YGkG8ZhZBXvWeCtMGVq
pKeO/I6aVcYy7tI09chOEe7LsEZYnI0hPrTiJLQ3UPAiWzokRzbIEasJdmIweL/w
sl8mF8zYRVSuBVME25/7hqHGiOrnPcmFTN2IaeJzKDtDmnYCy413WvCk+d8qjE4Q
hEXWNQpVSxK17TnoxA5DBOGC0b6iogyDLfrWxwR5Ohp9Q94/jrfqKAzJksRvG3Xo
OKi7l6734fBXXuoD+arIb/nfazp/heaj1KZ+3mCWe4rQNL1G2f3325n1ORILCKLX
7dIWet3wDn34dlT1YF9EdM+9t8k3WlMZep0roXTGr4EOOTZqi3ozGBPKM7PSPPKR
Nlo+XyvEjqIvE9q6lTnyJTGlzaYNnx/9h4EZBxR9KXbErhIzM6nQps5Y53ai5p8g
lsF/x+Fsdw1HSQ1vwPDkmOptIaNHYl5nzsDNBGXn7uMBDADV8rWczpe+7eq7edcP
iEz2jqFJAWdXuLYbdmErJeGvpRGje8oCKZ8ID3Gp+u3jtEjGwsyqpa4X+xXFdnsT
PoAkgdC1Sy1EsNLrRDtDmQknqlb8Nsrg41UpjN4LgSP46cfKNLoA36E+7+PX3mnL
Y3BodGac3iCm8I08vS4ipSRjFDCsHBl3PnzdUeIv7CJ0V/18qftiD4Yqj84a9w+D
t2oP/tisb0PYIIMWDXEI1eDbZ+dV6a1hHM/GuivBdbW7k5OgaAHkpIKHepenRKso
jnLoP4nyCLqeEpC5CEGefE7YqBL2exYmv2mNFZqwi1o1tMG/tzFYCdQRkfVZN2+S
ZVvVrEVxXZrcYTdikLBt5/RjZT1Cdn6+7UvZLsBX26oYEE6UBLWQ6KVYFbBHPQEb
lKZ3poeosQTTfG7ambcOki3o3q3Vsmdw5uxQ9fWKffGzxtc4msH3md5rZyGRbQo0
yxwKAxR1QaD3hB09d/WF9mlkLvMmZO03BCaR59L4IfL9ubcAEQEAAcLA9gQYAQgA
IBYhBDJOGmg6tNZAEFUKSdj6X4oFH+kTBQJl5+7jAhsMAAoJENj6X4oFH+kTOXoL
/2xSUG31EZLrnd002NA4nuc5msCr3L6aIxoQ8TuHMapAIsU1Qnng+lU/N/XCYDNv
ocHh/7p2MxUArX3Y4ft9HisRF4og3c6g8v0nokI9u1KxneISHtHkbDBs3Z8MwQvE
xtZGWhPNQgGHbe/jARgwjvIdUPWH27TGy5VXchJlfS0N0Hix4EFMjZcsdGzcFtVj
meBmtGIy00cf2eZvUAUvfNEGFnKcdd7m0FrAxqWTRxmv8sN0fvvOEtRNh0E4zGm1
t8g9s25OmTAdOQJBjq0fDGvJbO1NqR2nAQLcRTrQ3rix1vn13eqhoBjobEBoC2yv
9Zwc6+Xca8xC2gSBlENyvYYiywACUQGN6D/CAkmU6oUSshdM4LSpadt1V2UI5l1l
YvvMc3jTfUD67mWFDy0YyOD6P+QDmH/qd2Ftf25MmhhcdIfytqNxawPTBo9fWqRr
lBBJrnQyytWy9Feyf32pf/cwiY8uBjvu9wK2ElPGdjOF1kUwSzjQZspXifCLnNcC
dg==
```

```
=Wm+U
-----END PGP PUBLIC KEY BLOCK-----
```

File PGP key ini tersedia pada tautan:
https://keys.openpgp.org/vks/v1/by-fingerprint/324E1A683AB4D64010550A49D8FA5F8A051FE913

2.7. Tim CSIRT-UBBG diketuai oleh Achyar Munandar, S.Kom dengan anggota tim adalah Rivan Fitra Fahmiza, S.Pd dan Zaharatul Ulfa, S.Kom.

2.8. Catatan pada kontak CSIRT-UBBG antara lain metode yang disarankan untuk menghubungi CSIRT-UBBG adalah melalui e-mail pada alamat csirt[at]bbg.ac.id atau melalui nomor telepon (+62) 852-9709-7995 / (+62) 852-7020-3925 ke CSIRT-UBBG yang siaga selama 24/7.

3. Mengenai CSIRT-UBBG

3.1. Visi

Visi CSIRT-UBBG adalah terwujudnya ketahanan siber perguruan tinggi yang handal guna mewujudkan ekosistem akademik yang aman, terpercaya, dan inovatif.

3.2. Misi

Misi dari CSIRT-UBBG, yaitu :

a. Mengidentifikasi dan merespons secara proaktif terhadap insiden keamanan di lingkungan teknologi informasi perguruan tinggi guna melindungi data, sistem, dan infrastruktur dari ancaman siber.
b. Menyediakan dukungan dan bimbingan kepada para pengguna teknologi informasi dalam menghadapi risiko keamanan serta meningkatkan kesadaran tentang praktik keamanan yang baik.
c. Melakukan penyelidikan menyeluruh terhadap setiap insiden keamanan guna memahami sumber serangan dan menerapkan tindakan korektif yang tepat.
d. Berkoordinasi dengan berbagai pihak terkait di dalam dan di luar perguruan tinggi, termasuk pihak berwenang dan mitra akademik, untuk meningkatkan efektivitas dalam mengatasi ancaman keamanan.
e. Melakukan uji penetrasi, evaluasi keamanan, dan audit secara berkala untuk mengidentifikasi potensi kerentanan dan memastikan tingkat keamanan yang optimal.

f. Mengembangkan dan mengimplementasikan kebijakan keamanan teknologi informasi yang relevan dan sesuai dengan regulasi yang berlaku di perguruan tinggi.
g. Menjalin kemitraan dengan komunitas keamanan siber, berbagi informasi dan sumber daya untuk meningkatkan kapabilitas keamanan secara luas.
h. Memberikan pemahaman kepada civitas akademika perguruan tinggi untuk meningkatkan literasi keamanan siber di seluruh lingkungan kampus.
i. Berfokus pada pendekatan pencegahan, dengan membangun lapisan pertahanan keamanan yang kokoh untuk mencegah dan mengurangi potensi insiden keamanan.

3.3. Konstituen

Konstituen CSIRT-UBBG adalah seluruh satuan unit kerja Universitas Bina Bangsa Getsempena.

3.4. Sponsorship dan/atau Afiliasi

Sponsorship dan/atau afiliasi CSIRT-UBBG merupakan bagian dari Biro Teknologi Informasi dan Komunikasi UBBG sehingga seluruh pembiayaan bersumber dari anggaran Universitas Bina Bangsa Getsempena.

3.5. Otoritas

CSIRT-UBBG memiliki kewenangan untuk menangani gangguan keamanan siber, melakukan mitigasi, menyelidiki, dan menganalisis dampak insiden di lingkungan Universitas Bina Bangsa Getsempena. Selain itu, CSIRT-UBBG juga dapat berkoordinasi dan bekerja sama dengan pihak lain yang memiliki kompetensi dalam menangani insiden yang tidak dapat ditangani, seperti EduCSIRT Pusdatin Kemendikbud, BSSN, akademisi IT Security, atau ahli keamanan lainnya.

4. Kebijakan-Kebijakan

4.1. Jenis-jenis insiden dan tingkat/level dukungan CSIRT-UBBG 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-UBBG kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. CSIRT-UBBG akan melakukan kerja sama dan berbagi informasi dengan EduCSIRT Pusdatin Kemendikbud atau pihak lain yang terkait dalam hal keamanan siber. Segala informasi yang diterima oleh CSIRT-UBBG akan dijamin kerahasiaannya.

4.3. Komunikasi dan autentikasi untuk komunikasi biasa dengan CSIRT-UBBG dapat menggunakan e-mail dengan enkripsi data dan telepon. Sedangkan komunikasi terkait laporan insiden dan pertukaran informasi ancaman insiden lainnya dapat menggunakan saluran komunikasi yang disediakan (e-mail, WhatsApp, call center) yang telah terenkripsi atau dilengkapi dengan kata sandi.

5. Layanan

5.1. Layanan Utama

Layanan utama dari CSIRT-UBBG yaitu:

5.1.1. Deteksi dan Respon Insiden Keamanan

Memberikan layanan deteksi proaktif untuk mendeteksi dan merespons insiden keamanan yang terjadi di lingkungan teknologi informasi perguruan tinggi. Ini mencakup pemantauan keamanan secara real-time, analisis log, dan deteksi ancaman potensial.

5.1.2. Penanganan dan Pemulihan Keamanan

Merespons secara cepat dan tepat terhadap insiden keamanan yang terdeteksi, melakukan tindakan mitigasi, dan mengatasi dampak yang mungkin timbul. Pemulihan keamanan mencakup pemulihan sistem, jaringan, dan data yang terpengaruh oleh insiden.

5.1.3. Investigasi Insiden

Menyelidiki secara menyeluruh insiden keamanan untuk mengidentifikasi sumber dan teknik serangan, serta menyusun laporan hasil penyelidikan yang dapat membantu meningkatkan keamanan secara keseluruhan.

5.1.4. Pemberdayaan Pengguna

Memberikan pemahaman kepada civitas akademika perguruan tinggi dalam hal keamanan siber. Ini termasuk edukasi tentang praktik keamanan yang baik, tips menghadapi ancaman siber, dan tindakan pencegahan.

5.1.5. Pengembangan Kebijakan Keamanan

Membantu dalam pengembangan, peninjauan, dan pembaruan kebijakan keamanan teknologi informasi perguruan tinggi, serta memastikan kepatuhan terhadap kebijakan yang ada.

5.2. Layanan Tambahan

Layanan tambahan dari CSIRT-UBBG yaitu:

5.2.1. Penilaian Keamanan

Melakukan penilaian keamanan, seperti uji penetrasi dan evaluasi keamanan, untuk mengidentifikasi kerentanan dalam sistem dan aplikasi perguruan tinggi serta memberikan rekomendasi peningkatan keamanan.

5.2.2. Layanan Konsultasi

Memberikan layanan konsultasi keamanan siber kepada berbagai unit dan departemen di perguruan tinggi untuk membantu mengatasi isu-isu keamanan yang khusus dan beragam.

5.2.3. Keamanan Jaringan

Membantu dalam pengaturan keamanan jaringan, pemantauan lalu lintas jaringan, dan penegakan kebijakan keamanan pada tingkat infrastruktur jaringan.

5.2.4. Peringatan Dini

Memberikan peringatan dini tentang tren ancaman keamanan terbaru dan peristiwa keamanan yang relevan untuk membantu perguruan tinggi tetap waspada dan menghadapi ancaman yang berkembang.

5.2.5. Penelitian dan Pengembangan

Melakukan penelitian tentang tren dan metode keamanan terbaru, serta mengembangkan solusi keamanan khusus untuk kebutuhan unik perguruan tinggi.

5.2.6. Kerjasama Eksternal

Berpartisipasi dalam kerjasama dengan CSIRT dari lembaga lain, mitra keamanan siber, dan pihak berwenang untuk berbagi informasi, menghadapi ancaman bersama, dan berkontribusi pada keamanan siber secara luas.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt[at]bbg.ac.id dengan melampirkan sekurang-kurangnya:

a. Foto/*scan* kartu identitas.
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan.

7. *Disclaimer*

a. Terkait penanganan jenis *malware* tergantung dari ketersediaan *tools* yang dimiliki.
b. Tingkat maturitas penanganan insiden siber sudah diukur.