

RFC 2350 BRIN-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.3 yang diterbitkan pada tanggal 20 Agustus 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://csirt.brin.go.id/cs1rt_uploads/rfc2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 BRIN-CSIRT;

Versi : 1.3;

Tanggal Publikasi : 20 Agustus 2024;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Badan Riset dan Inovasi Nasional - *Computer Security Incident Response Team*
(CSIRT) Indonesia
Disingkat : BRIN-CSIRT.

2.2. Alamat

Gedung B.J. Habibie, Jl. M.H. Thamrin No. 8,
Jakarta Pusat 10340

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

Tidak ada

2.5. Nomor Fax

Tidak ada

2.6. Telekomunikasi Lain

Tidak ada

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

csirt[at]brin[dot]go[dot]id

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

Bits : 4096

ID : 208c f6ff e42d b942

Key Fingerprint : 12305EC3F1D92FE5248FAB35208CF6FFE42DB942

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

```
mQINBGI4WhUBEAC+uMRrPeyRqPCvWDMQK54MbqQ2Nm2AO8VoMsNyppCoOZ9Vr1FT
wU8w1IYCYyY0aF2x3KPtbxBBgW7cP8FiktamH8C0W7bHW5DmH6AGJfX5co88/Vn9
xK59E5A728kYOWjiSXsmJ2kr3uWKKWjnETMYwFYjOyqlqHwxgPVt1PDW3tYGP5C
CjdK6688sKkzJ0rfSsx6Hh0J5E1+6F6Vmk7byHs10N5yfDivzYeeSLt1VJsJIEDZ
FYu/6YsQMBzkI1ntowWvdkOG8AnbxeZowpRP3rfd/mtCpQaYeNMrdoYYajUIBFin
PZdz/t3QOvrn8N6K4eZRHDPDGIBL7TEcsP2G4jU9NXbaTdwBqq6t/ODNM5X7gdcCM
mV0cTUzDgCD1GleYayxsEsX4V0Q9h3aDvJ3m1oBzSggwZcPtRWp0ALXHNw8+8jGD
k69tTV8NXZZUQHupvJrIYmmP1qx+95xjZJJ7jqIklt3ytc6008zqzREX1KlmvUMP
rgkuYntwheQ9qc4/jNLpJjxb+s9medr2qGwzaWOC1hN3F+i1lM0NuGixy+OTry+E
FbFyph9qhYfGL5R98TrSIYzF2zHssKZTE22jbg5y6DE7JxnYg9ni/JY7G0CPrQcr
ZGfRPMr65cIgbKZvalOvvQUG4lrrkBqm97DPIoYh6ZHvEVpBAxFd145IqQARAQAB
tB1CUklOIENTSVJUIdXjc2lydEBicmluLmdvLmlkPokCTgQTAQgAOBYhBBiWxSPx
2S/1JI+rNSCM9v/kLb1CBQJiOfOVAHsDBQsJCAcCBhUKCQgLAGQWAgMBAh4BAheA
AAoJECCM9v/kLb1COG4P/3lyOLFHz6mLnc/2Htg6nWb/PXPN1UFnjc5BdPtGIGkM
HLwe02EMsqBKH5Kqi011+UP1DP6d4PMqVOVsAnKbQsMOGWLf+rZflvqz1wnihIsK
T1theURkwI8BeCM4deed9uZo8WjQmqu/c2/1g6ulWuyYAYGEhrOjtZuFlwrDQVNJ
LdHzrsd8x8kBasG12NEvc4Y6fB6AowaTLh0xOLNplyDcOr7eMWricT/OmVgMOYXg
NSHx4ZKe35UshFWywlFCnn9uTfbkoQgEv70ZPc7ysWqTzs73TSBVJg7fy67dvt5J
xren2DQsKcVwnAdsX78pbVtBhGuEYdeKCaQ5ZwFjHErLYcP93Ce9u/Dq8NiJc5BY
CTiPvURsg59NMnmSdZLtPZA5r1W3/2Yh4RNhBA1RLELaClNZ3i26XAZs0E7UygM4
g35z/Ziayo5ESNP8gvvdgFUiYx3KdR//SFTwNWrixIEkOZsxyPa/KmRnyIMLGoSL
wIcY0BLvt6v32bqSwwJqx2wcbHsEpvHkc77s8dqyIHj10ancY6CY7k9hffu9Bu9g
LzkrploUvx8PYC2FN6ZMljTJ6zGU0NFKXPi1OuM1WusQHSaWhrFHdYKCaRqbI5ht
8Qgi71j6FMbaXI4Czik5ASXOmdrWYOo4Z2WX4L3MsGdRnAohDsVHJzPoFFZ6rshH
uQINBGI4WhUBEADfIgbKCRP+dnvQ4nd6I9BfwxGHvWgdI69aofbvkJ76c9EUd2G4
C3Zt7mNFV9PEg179Hx0mWCvieE1DXk+1d6Gqcs/C8EciwDPiQMTUf6TdosYSv/U0
o0WN9sSlf5f4nJ4KbHuzqKUoXAkIgj8lp9+SeRkOIIPLuqGhXUFTpXjhcDU12M/
MDW/ZTIctRVEhWRIS9uvy87K7RHnVF3pocygvw1PSnNOgTu+z2bAXjsY8Txaia1
MykVXe5jLnPtix9Sk2sAjBkZ+2fcwr1N1+niKaCVaBqfDh9ewVnN/CZIKhXD7Ioz
8j94E0m+6uh8QRz0wBfZAiuCV4zJavC+SwgxQuChld97WJklK1rQSBU1A8wH+bVn
```

```
A8n5CcgvmlsN1YVO64eDSFjgfc3TiYvFZbpYxqh0bujriaAqXlkrqgX/KUm7N1NO
IxLXeLWijO14rJFU1S0jjZa11SFifgJOBmF5RYSqAyhB3YeR+wn0YMPIpn43gziH
5g7ys6jp78fLS1J2Sul4IRSceHAG0ckrY7RiBYTUmTkJgaFxTPAtaTqgI1D4EF/P
hyCtgZAvAEEjsis4Gy8g/oIg33DaeNnsBAGVAud01HtHPFpn8T0gV+VHMIObap0K
3mGpAwq8vxqn2VD2fSrIRDvOICHgqTnmabVFdwaqtPJczHqDd3Lnz5gB0QARAQAB
iQI2BBgBCAAgFiEEEjBew/HZL+Ukj6s1IIz2/+QtuUIFAMI4WhUCGwwACgkQIIz2
/+QtuULQnRAAngeU2U153rNvLoTN/4PZI4ur1MC6EaSIoqZc9mr5eX0soNTM4/Mj
VQ1yFPz3N5z9oNHQ1aQx5BmY8KBN3L+O/iQK7eBJcWWCUkpGxJtUrtysquZdcYat
wVYzDw99vO/7KSgTo/iFO6BnUjuyzpmZnB8Jr4haQ1as7WOhQ7EKO9qzsBgiMsGO
vj2N3UXE+r3IyM5oJVA79X4StlqQ6fUVozxTdfksC9p6jWFLdCjKg1loZyk9Ah6R
eRTs6s0aIBrebs9jBlWyVLu/8UDnMOP2wqipmLjrBXvzNPUOC3TAK0Ts/0qhvT0Q
FIhTIEHfnJK3x9ybNr9D8jThrEAQNG1URPgnqiH2BLB09h30RkBtaCZxpfaPl/pC
KdDuTEcmk81enJwMMBwzAydNKN4esiGn6IXeJ6h92zLnY7mNj070taIp6Uy3ofQi
Cqy5X/BAae8WwD5sQ6C9o5/WWazN3H2dDWCXiwQxT4Z1is7tW6tBs6XNoFeI/O1W
QHYnnJ1tNG6oPyDT63tuWumg0Yo4eMUnWoDCGyn/vEgg6PPS1o91V6WD2/kZGOXW
hW/dzypMATxmJias2AxEvtnyhKbG5h88qxBIzTKc8T5mAw+fkH7FCUbdWala+VwS
N/reS1Fvx/5Y+IunQyQOR5a8XOSZPzLgAlwXjP9OH2rKuUKBWZsnlbI=
=BiYl
-----END PGP PUBLIC KEY BLOCK-----
```

File PGP key ini tersedia pada :

https://csirt.brin.go.id/BRIN_CSIRT_public.asc

2.9. Anggota Tim

Ketua BRIN-CSIRT adalah Kepala Pusat Data dan Informasi BRIN. Yang termasuk anggota tim adalah personil pada Lingkungan Pusat Data dan Informasi BRIN.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak BRIN-CSIRT

Metode yang disarankan untuk menghubungi BRIN-CSIRT adalah melalui *e-mail* pada alamat [csirt\[at\]brin\[dot\]go\[dot\]id](mailto:csirt@brin.go.id) yang siaga jam 08:00 - 15:30 WIB pada hari Senin - Jumat.

3. Mengenai BRIN-CSIRT

3.1. Misi

Misi dari BRIN-CSIRT, yaitu :

- Membangun pusat pencatatan, pelaporan, dan penanggulangan insiden keamanan siber di lingkungan Badan Riset dan Inovasi Nasional;
- Membangun kerjasama dalam rangka pengamanan siber terhadap layanan TI di lingkungan Badan Riset dan Inovasi Nasional;
- Meningkatkan kapasitas sumber daya manusia terhadap ancaman keamanan siber pada aspek pencegahan, penanggulangan dan pemulihan insiden keamanan siber di lingkungan Badan Riset dan Inovasi Nasional.

3.2. Konstituen

Konstituen BRIN-CSIRT meliputi pengguna Sistem Pemerintahan Berbasis

Elektronik di lingkungan Badan Riset dan Inovasi Nasional.

3.3. Sponsorship dan/atau Afiliasi

BRIN-CSIRT merupakan bagian dari BRIN sehingga seluruh pembiayaan bersumber dari APBN.

3.4. Otoritas

BRIN-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada Badan Riset dan Inovasi Nasional dan dapat berkoordinasi serta bekerjasama dengan BSSN / Akademisi IT Security / Principal IT Security / Ahli Security untuk insiden yang tidak dapat ditangani.

BRIN-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

BRIN-CSIRT melayani penanganan insiden siber dengan jenis berikut :

- a. *Web Defacement*;
- b. Distributed Denial of Service (DDOS);
- c. Malware;
- d. Phishing.

Dukungan yang diberikan oleh BRIN-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden. Dukungan yang diberikan terbatas pada perangkat kedinasan BRIN.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

BRIN-CSIRT akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber.

Seluruh informasi yang diterima oleh BRIN-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa BRIN-CSIRT dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional). Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada e-mail.

5. Layanan

5.1. Layanan Reaktif

Layanan reaktif dari BRIN-CSIRT merupakan layanan utama dan bersifat prioritas yaitu :

5.1.1. Pemberian peringatan terkait dengan laporan insiden siber

Layanan ini dilaksanakan berupa pemberian peringatan adanya insiden siber dan juga informasi statistik terkait layanan kepada pemilik sistem elektronik.

5.1.2. Layanan penanggulangan dan pemulihan Insiden

Layanan ini diberikan berupa koordinasi, analisis, rekomendasi teknis, dan bantuan on-site dalam rangka penanggulangan dan pemulihan insiden siber.

5.1.3. Layanan penanganan kerawanan

Layanan ini diberikan berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (hardening). 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 akan dikoordinasikan dengan pemilik sistem;
- b. Layanan penanganan kerawanan yang dimaksud dapat juga merupakan tindak lanjut atas kegiatan Vulnerability Assessment.

5.1.4. Layanan penanganan artefak

Layanan ini diberikan berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi.

5.2. Layanan Proaktif

- a. Menyelenggarakan kegiatan workshop keamanan siber kepada pihak konstituen.
- b. Menyelenggarakan kegiatan Drill Test Insiden Keamanan Siber kepada pihak konstituen.
- c. Menyelenggarakan sosialisasi keamanan siber kepada konstituen

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke [csirt\[at\]brin\[dot\]go\[dot\]id](mailto:csirt@brin.go.id) dengan melampirkan sekurang-kurangnya :

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

7. Disclaimer

Tidak ada.