

RFC 2350 BAZNAS-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 2.0 yang diterbitkan pada tanggal 12 Januari 2023.

1.2. Daftar Distribusi untuk Pemberitahuan

Menjabarkan pihak-pihak yang menjadi daftar distribusi untuk pemberitahuan RFC 2350, disesuaikan dengan kebutuhan masing-masing CSIRT.

- Direktorat Inovasi & Teknologi
- Biro Komunikasi Publik
- Biro Hukum & Kelembagaan

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :

<https://csirt.baznas.go.id/rfc2350.pdf> (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 BAZNAS-CSIRT;

Versi : 2.0;

Tanggal Publikasi : 12 Januari 2023;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Badan Amil Zakat Nasional CSIRT

Disingkat : BAZNAS-CSIRT.

2.2. Alamat

Jl. Matraman Raya No. 134 Kel. Kebon Manggis Kec. Matraman Jakarta

2.3. Zona Waktu

DKI Jakarta (GMT+07:00)

2.4. Nomor Telepon

(+62) 21-22897983

2.5. Nomor Fax

2.6. Telekomunikasi Lain

Sebutkan jika ada

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

csirt@baznas.go.id

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

Bits : angka jumlah bit

ID : 940F A880 91AC 69A2

Key Fingerprint : E0313FEF1D116A3E8BCEC949940FA88091AC69A2

Blok PGP Public Key:

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

```
mDMEY7+RAxYJKwYBBAHaRw8BAQdAzD9lIdODsNlgbmqRf7gp6tsCSmdBRvs2h3Ho
l4Bolzu0IUJBWk5BUy1DU0ISVCA8Y3NpcnRAYmF6bmFzLmdvLmlkPoiZBBMWCgBB
FiEE4DE/7x0Raj6LzslJIA+ogJGsaalFAmO/kQMCGwMFCQPDu00FCwklBwIClgIG
FQoJCAsCBBYCAwECHgcCF4AACgkQIA+ogJGsaalFAmO/kQMCGwMFCQPDu00FCwklBwIClgIG
wzoSS2yGu9+F7UtGUttU/tkBANvVx9RrWMv708b2DnhozXo12Ou5W5STfdBlmKIM
InlDuDgEY7+RAxIKKwYBBAGXVQEFAQEHPa/x6waL3l45GvY4rLd8OdduIFQCJ0s
vUpNhJWDu6U1AwEIB4h+BBgWCgAmFiEE4DE/7x0Raj6LzslJIA+ogJGsaalFAmO/
kQMCGwwFCQPDu00ACgkQIA+ogJGsaalFAmO/kQMCGwMFCQPDu00ACgkQIA+ogJGsaalFAmO/
WNJjODAGEMrgojYA+wZVklEeyr3Cxxs0xJuevqayFI6T15voS9j9z96VmYgL
=pYP6
```

-----END PGP PUBLIC KEY BLOCK-----

File PGP key ini tersedia pada :

<https://csirt.baznas.go.id/publickey.asc>

2.9. Anggota Tim

Ketua BAZNAS-CSIRT adalah Andrian.

Yang termasuk anggota tim adalah

1. Muhammad Munanto
2. Fajar Febri Susetyo
3. Agung Februanto
4. Ndari Rumi Widyawati
5. Yudhiarma MK
6. Muhammad Imam Nawawi Syujai
7. Almay Faizrivan
8. Ailsa Nabila Irvhan

2.10. Informasi/Data lain

-

2.11. Catatan-catatan pada Kontak BAZNAS-CSIRT

Metode yang disarankan untuk menghubungi BAZNAS-CSIRT adalah melalui *e-mail* pada alamat csirt@baznas.go.id atau melalui nomor telepon ke (+62) 21-22897983 pada hari kerja jam 08.00 - 17.00 atau melalui nomor 081298271935 siaga selama 24/7.

3. Mengenai Gov-CSIRT

3.1. Visi

Visi BAZNAS-CSIRT adalah terwujudnya ketahanan siber pada BAZNAS RI (BAZNAS Pusat) yang handal dan profesional.

3.2. Misi

Misi dari BAZNAS-CSIRT, yaitu :

- a. Mengkoordinasikan dan mengkolaborasikan layanan keamanan siber pada BAZNAS RI (BAZNAS Pusat)
- b. Membangun kapasitas sumber daya keamanan siber pada BAZNAS RI (BAZNAS Pusat)

3.3. Konstituen

Konstituen BAZNAS-CSIRT meliputi : seluruh unit kerja pada BAZNAS RI (BAZNAS Pusat)

3.4. Sponsorship dan/atau Afiliasi

Pendanaan BAZNAS-CSIRT bersumber dari dana zakat

3.5. Otoritas

BAZNAS-CSIRT memiliki kewenangan untuk Melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada BAZNAS RI (BAZNAS Pusat)

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

BAZNAS-CSIRT melayani penanganan insiden siber dengan jenis berikut :

- a. Malware;
- b. Distributed Denial Of Service (DDOS)
- c. Phishing;
- d. Ransomware;

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

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

5. Layanan

5.1. Layanan Utama

Layanan utama dari BAZNAS-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber (alert and warning)

Layanan ini dilaksanakan oleh BAZNAS-CSIRT insiden berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik.

5.1.2. Penanggulangan dan pemulihan insiden siber (incident handling)

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

5.1.3. Penanganan kerawanan (vulnerability handling)

Layanan ini diberikan oleh BAZNAS-CSIRT berupa koordinasi, analisis dan rekomendasi teknis dalam rangka penguatan keamanan (hardening), 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 kerawanan kerawanan tidak dapat ditangani;
- b. Layanan penanganan kerawanan yang dimaksud dapat juga merupakan tindak lanjut atas kegiatan *vulnerability assessment*.

5.1.4. Penanganan artifak (artifact handling)

Layanan penanganan artifak

6. Pelaporan Insiden

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

- a. Foto/*scan* kartu identitas
- b. Bukti insiden berupa foto atau *screenshot* atau *log file* yang ditemukan
- c. Atau sesuai dengan ketentuan lain yang berlaku

7. Disclaimer

Terkait penanganan jenis *malware* tergantung dari ketersediaan *tools* yang dimiliki.