RFC 2350 BTN-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal *Update* Terakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 16 Maret 2026.

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.btn.co.id/id/About/ESG/ESG-Commitment/Management-Sustainability-Commitment/Cybersecurity`

1.4. Keaslian Dokumen

Dokumen ini ditandatangani digital menggunakan PGP Key BTN-CSIRT.
Untuk lebih jelas dapat dilihat pada point 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 BTN-CSIRT;
Versi	: 1.1;
Tanggal Publikasi	: 16 Maret 2026;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

BTN-CSIRT.

2.2. Alamat

Menara Bank BTN Jl. Gajah Mada No.1, RW.8, Petojo Utara, Gambir, Jakarta Pusat

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(+62) 150286

2.5. Nomor Fax

Tidak Ada

2.6. Telekomunikasi Lain

Tidak Ada

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

csirt@btn.co.id

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

Bits : 1024
ID : 0x036C03C4814F363B
Key Fingerprint : 97C0 2E13 1E0E 5517 154E 213E 036C 03C4 814F 363B

Blok PGP Public Key:

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

mDMEabdw3BYJKwYBBAHaRw8BAQdA+TGrND66ZWnx3p16cvoTqbpP1Gtvhjzpj GGB
dLTWpFq0G0JUTi1DU0lSVCA8Y3NpcnRAYnRuLmNvLmlkPoi1BBMWCgBdFiEEl8Au
Ex4OVRcVTiE+A2wDxIFPNjsFAmm3cNwbFIAAAAAABAAObWFudTIsMi41KzEuMTEs
MiwxAhsDBQkFpQl0BQsJCAcCAiICBhUKCQgLAgQWAgMBAh4HAheAAAoJEANsA8SB
TzY7oeIBAJAJJ9kcWBJCe9ybYpzugqRfZ6mqrJemdF4PRQTwUnm8AP4tRPjs27si
nIp2RLoi1m6WB3vCtCTYkcdcLeYgEgRsALg4BGm3cNwSCisGAQQBl1UBBQEBB0Dm
wNLpvREj0YEo3FEB7LQ5a7D1LMEG6zDcurBwA6gpDAMBCAeImgQYFgoAQhYhBJfA
LhMeDlUXFU4hPgNsA8SBTzY7BQJpt3DcGxSAAAAAAAQADm1hbnUyLDIuNSsxLjEx
LDIsMQIbDAUJBaUJdAAKCRADbAPEgU82O4GtAQDSjzQYjPKiwYZJptsPLZYOZS3i
Qnpq9m3xKCdaJHjvKAD8DEjh8sSrLRJvT/iP9n36V7u1lwL0D+v0YflrjxN3qAk=
=Es9e
-----END PGP PUBLIC KEY BLOCK-----
```

File PGP *key* ini tersedia pada :
https://www.btn.co.id/id/About/ESG/ESG-Commitment/Management-Sustainability-Commitment/Cybersecurity

2.9. Anggota Tim

Ketua BTN-CSIRT adalah *Computer Security Incident Coordinator* (CSIC) yang ditunjuk oleh Direktur IT & Digital. Untuk anggota tim merujuk kepada Surat Keputusan Bank BTN surat Nomor 5/M/SOC/IV/2026 dan Memo Nomor 32/M/ITSD/SOC/IV/2026 dan Tentang Pembaruan Surat Keputusan Pembentukan Anggota *Computer Security Incident Response* Team (CSIRT).

2.10. Informasi/Data lain

Tidak Ada.

2.11. Catatan-catatan pada Kontak BTN-CSIRT

Metode yang disarankan untuk menghubungi BTN-CSIRT adalah melalui *e-mail* pada alamat csirt@btn.co.id atau melalui nomor +6282298748166 dan +62817115333, yang tersedia selama 24 jam sehari dan 7 hari seminggu (24/7).

3. Mengenai BTN-CSIRT

3.1. Visi

Visi BTN-CSIRT adalah :

1. Terwujudnya ketahanan siber di Bank BTN yang andal dan profesional.
   Menciptakan kesadaran keamanan siber pada Sumber Daya Manusia di lingkungan Bank BTN.

3.2. Misi

Misi dari BTN-CSIRT, yaitu :

a. Mendorong kegiatan pengamanan informasi dan pencegahan insiden keamanan siber;
b. Membangun kesadaran keamanan siber pada sumber daya manusia di lingkungan Bank BTN;
c. Melakukan evaluasi berkala terhadap keandalan keamanan teknologi informasi di lingkungan Bank BTN.

3.3. Konstituen

Seluruh pengguna teknologi informasi di lingkungan Bank Tabungan Negara

3.4. *Sponsorship* dan/atau Afiliasi

Anggaran TI perusahaan

3.5. Otoritas

Berdasarkan Dokumen Ketentuan Khusus PT. Bank Tabungan Negara Nomor KK.5-B Keamanan Teknologi Informasi pada point B.9 Kewenangan Organisasi Keamanan Informasi, Bank Tabungan Negara berwenang untuk melakukan pengelolaan insiden keamanan TI secara proaktif dan reaktif.

4. Kebijakan – Kebijakan

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

BTN-CSIRT memiliki otoritas untuk menangani berbagai insiden keamanan siber yang terjadi atau mengancam konstituen berupa :

a. *Web defacement,*
b. DDOS
c. Malware
d. Phising

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

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

5. Layanan

5.1. Layanan Utama

Layanan utama dari BTN-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

BTN-CSIRT menyediakan layanan pemberian peringatan dini (*early warning*) terkait potensi ancaman dan kerentanan keamanan siber yang dapat berdampak pada sistem elektronik di lingkungan Bank BTN.
Peringatan ini disampaikan berdasarkan hasil *monitoring* internal, analisis intelijen ancaman siber, maupun informasi dari pihak eksternal terpercaya.
Tujuan dari layanan ini adalah untuk meningkatkan kesiapsiagaan konstituen dalam menghadapi potensi serangan serta meminimalkan dampak yang ditimbulkan melalui langkah mitigasi yang tepat waktu.

5.1.2. Penanganan Insiden Siber

BTN-CSIRT memberikan layanan penanganan insiden keamanan siber yang terjadi pada sistem elektronik di lingkungan Bank BTN.
Penanganan insiden meliputi proses identifikasi, analisis, *containment*, eradikasi, serta pemulihan (*recovery*) terhadap insiden yang terjadi.
BTN-CSIRT juga melakukan koordinasi dengan unit kerja terkait guna memastikan proses penanganan berjalan efektif dan terdokumentasi dengan baik, serta meminimalkan dampak terhadap operasional bisnis.

5.1.3. Pencatatan Laporan/Aduan Insiden Siber

BTN-CSIRT menyediakan layanan pencatatan terhadap setiap laporan atau aduan insiden keamanan siber yang diterima dari konstituen maupun pihak terkait lainnya.
Seluruh laporan akan didokumentasikan secara sistematis sebagai bagian dari proses manajemen insiden, termasuk pencatatan waktu kejadian, jenis insiden, serta pihak yang terdampak.
Pencatatan ini bertujuan untuk memastikan setiap insiden dapat ditelusuri, dianalisis, serta menjadi bahan evaluasi dalam peningkatan keamanan siber ke depan.

5.1.4. Pemberian Rekomendasi Langkah Penanganan Awal

BTN-CSIRT memberikan rekomendasi langkah penanganan awal (*initial response*) kepada pihak terdampak insiden keamanan siber.
Rekomendasi yang diberikan bersifat praktis dan segera dapat diimplementasikan untuk mengurangi dampak insiden, seperti isolasi sistem, pemutusan akses, atau tindakan mitigasi lainnya.
Layanan ini bertujuan untuk membantu konstituen dalam melakukan respons cepat sebelum dilakukan penanganan lanjutan secara menyeluruh.

5.1.5. Pemilahan (*Triage*) Insiden Siber

BTN-CSIRT melakukan proses pemilahan (*triage*) terhadap insiden keamanan siber berdasarkan tingkat prioritas, dampak, dan urgensi penanganan.
Proses ini dilakukan dengan mengacu pada kriteria yang telah ditetapkan guna memastikan sumber daya penanganan difokuskan pada insiden yang memiliki risiko tertinggi terhadap operasional organisasi.
Dengan adanya *triage*, penanganan insiden dapat dilakukan secara lebih efektif dan efisien.

5.1.6. Koordinasi Penanganan Insiden Siber

BTN-CSIRT menyelenggarakan koordinasi penanganan insiden keamanan siber dengan pihak-pihak yang berkepentingan, baik internal maupun eksternal.
Koordinasi ini mencakup komunikasi dengan unit kerja terkait, manajemen, serta apabila diperlukan dengan pihak eksternal seperti regulator atau organisasi lain dalam lingkup keamanan siber.
Tujuan dari layanan ini adalah untuk memastikan penanganan insiden berjalan secara terintegrasi, terarah, dan sesuai dengan ketentuan yang berlaku.

5.1.7. Penyelenggaraan Fungsi Lainnya Sesuai Kebutuhan

BTN-CSIRT dapat menyelenggarakan fungsi dan layanan tambahan lainnya yang relevan dengan kebutuhan penanganan dan peningkatan keamanan siber di lingkungan Bank BTN.
Fungsi ini bersifat dinamis dan dapat disesuaikan dengan perkembangan ancaman, kebutuhan organisasi, serta kebijakan yang berlaku, sepanjang masih dalam ruang lingkup tugas dan tanggung jawab BTN-CSIRT.

5.2. Layanan Tambahan

Layanan tambahan dari BTN-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

BTN-CSIRT menyediakan layanan identifikasi dan penanganan terhadap kerawanan (*vulnerability*) pada sistem elektronik.

Kegiatan ini mencakup penerimaan laporan kerawanan, validasi, analisis tingkat risiko, serta pemberian rekomendasi perbaikan guna mencegah potensi eksploitasi oleh pihak yang tidak bertanggung jawab.

5.2.2. Penanganan Artefak Digital

BTN-CSIRT melakukan pengelolaan dan analisis terhadap artefak digital yang berkaitan dengan insiden keamanan siber, seperti log sistem, *file* mencurigakan, *malware*, maupun bukti digital lainnya.

Layanan ini bertujuan untuk mendukung proses investigasi dan forensik digital dalam rangka memperoleh informasi yang akurat mengenai sumber dan metode serangan.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

BTN-CSIRT secara aktif melakukan pemantauan terhadap potensi ancaman siber yang berkembang.

Hasil pengamatan tersebut akan diinformasikan kepada konstituen dalam bentuk notifikasi atau laporan, sebagai dasar dalam melakukan langkah antisipasi dan penguatan keamanan sistem.

5.2.4. Pendeteksian Serangan

BTN-CSIRT menyediakan layanan pendeteksian serangan siber melalui kegiatan *monitoring* dan analisis terhadap aktivitas jaringan dan sistem.

Deteksi dilakukan menggunakan berbagai *tools* dan metode untuk mengidentifikasi indikasi serangan secara dini sehingga dapat segera dilakukan tindakan penanganan yang diperlukan.

5.2.5. Analisis Risiko Keamanan Siber

BTN-CSIRT memberikan layanan analisis risiko terhadap ancaman dan kerentanan keamanan siber yang berpotensi mempengaruhi sistem elektronik.

Analisis ini mencakup identifikasi aset, penilaian tingkat risiko, serta rekomendasi mitigasi guna meningkatkan postur keamanan siber organisasi.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

BTN-CSIRT menyediakan layanan konsultasi kepada konstituen terkait kesiapan dalam menghadapi dan menangani insiden keamanan siber.

Layanan ini meliputi pemberian saran, *best practice*, serta panduan dalam penyusunan prosedur dan mekanisme respons insiden.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

BTN-CSIRT berperan aktif dalam meningkatkan kesadaran dan kepedulian terhadap keamanan siber di lingkungan Bank BTN melalui kegiatan sosialisasi, edukasi, dan kampanye keamanan informasi.

Tujuan dari layanan ini adalah untuk membentuk budaya keamanan siber yang kuat dan meningkatkan peran aktif seluruh sumber daya manusia dalam menjaga keamanan informasi.

6. Pelaporan Insiden

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

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

7. *Disclaimer*

Tidak ada.