

RFC 2350 BINTAN-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 28 Agustus 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 website BINTAN-CSIRT :
<https://csirt.bintankab.go.id/storage/uploads/3.%20RFC2350.pdf> (Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen telah ditanda tangani dengan PGP Key milik Bidang Teknologi Informasi dan Komunikasi, Statistik, Persandian Dinas Komunikasi dan Informatika Kabupaten Bintan. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 BINTAN-CSIRT;

Versi : 1.0;

Tanggal Publikasi : 28 Agustus 2023;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Bintan Computer Security Incident Response Team
Disingkat : BINTAN-CSIRT.

2.2. Alamat

Dinas Komunikasi dan Informatika Kabupaten Bintan
Jalan Raya Tanjungpinang - Tanjung Uban KM.42, Bandar Seri Bentan.

2.3. Zona Waktu

Jakarta (GMT+07.00)

2.4. Nomor Telepon

082173815983

2.5. Nomor Fax

Tidak Ada

2.6. Telekomunikasi Lain

Tidak Ada

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

csirt@bintankab.go.id

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

Bits : 4096

ID : 0x3D223B068F6208CE

Key Fingerprint : 1C2B 17C1 D140 31A6 2B2F 72CC 3D22 3B06 8F62 08CE

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

```
xsFNBGV34kkBEADLGzHYqbR9gGXn9jXleaFj2VcFSNYGKDbUcvO/0jixShrLlr66
uKeK+Zr2SYADyDpNhVqhrmr3sMTVjh2nGINF0dik72wdcum1FzBst2X1Ely0PKTI
m+UstQjSsZsmim43H1vjVwoS7qFTp4h/T0b++urtt0B71+Qh1hpCWnh9j6M8vMSI
8aj/G51ufqryUsCxc/R4vpJlechwYSLokKukTNvM2G2p0KY0m6N4jGOd3rS8g2pNw
rBsf8AvfVpzzqy2SgLT/vLbNK6r6jj44KHYZ8Dbu702kFtr/bA8vDTdZ6tzGdpzM
eZDix/4sWXjebhaB/L21pr/Vgy+F29mBG9MtXHzJrfYes0du7ZyrLRGMOT5vR14M
OAqO/xnCVpxmpmZVPjJERkxHneK4AsLUiYvnM37NwP6mrgxbWPKktheBKQRQZKv
AtSlq+b/VdncSwbBbiFM1gupyggcc7E4wlCsYvpMO3ssZM3loYuptdixPISvpU0p
cQXroOMev4Bdollj0vUooL/4Ayyrl/re4vEoC53xy6ycwP93nz562IBnAm1JSt8H
1U+0i6kmXVoVujHjRm9XEqwamNhvLXi+2iFr25z3hP78/38EaNS8ZTcLLVBxpA
Xr8JPbAGXDbWaiNXknCxlHpzjk8OxJ2HWFLhre2Q+AB4nL6xbZ1OvjxgJwARAQAB
zSRCSU5UQUU4tQ1NjUIQgPGNzaXJ0QgJpbmRhbmtH5i5nby5pZD7CwY0EEwEIADcW
IQQcKxfB0UAXpivscsw9ljsGj2IlzgUCZxfiSgUJBaOagAlbAwQLCQgHBRUICQoL
BRYCAwEAAoJED0iOwaPYgiO1IIQAJpG7KCYnNkXySgHKbHq4fz0bi12uy2bUIS5
lgHs8Kuwp2hFaHtf0a4+DL+Vd3175qZbVISV8mRWTNqAyRmDNbFO/PEqFFe9+KwX
3GYI6g6XiuHLO28qIt0xBZoM+8LNI0t7UPO1KHzvohLYLeezTeQ1sP1uBjyoDg5U
eT8TZ3wVBuQsCCyWSd/zy1PHm0xldLM5MPFqBxDzLbTPtEYu0a6SGfl70ekd9X7k
v+mcPLA9kc9g7DPLJGMJL4RKivuZp2tXdT+M8i5na70Bxo2dxrOmYOE8MJO4NOXU
bPFHWtg4zb/nIH122VMxt6E3v+QRetLKKeMTff7aV26pbj0NnTPJZJKnbehEuq9N
f6L8Jyayz71aUotYSTsijz1CSZn8EQ2meyZoWwo6tvwdOCXIBdl3ACYwBotR8Zap
8VjqcMpAVSHIXAp30SA8ytd8Hj3t9vJ8reRwHRq8TsH4iYspsRW69N8g4L4Gqau4
KSfzAZCUwxlgTWQWCmwg73BnpkW0y5icuCcQhuhLGqGSKD064sk3z6RpDFp028UI
jLE+RSHldEvGD2VuT1HsZnWfKQ0RgYN93106hZrjZnE7skWfARcKY0+cuurdCiXK
rX5nXXqnQc1uwuB9X1rAJi0SxTmu6O6ChVUqdBs9f4or41W1YvE9ZF7pkUBxeKXU
HUXch/APzsFNBGV34ksBEACyJzPUM7v86h61N2KocEsXjEn9/VA6lWdpXmz3y4UF
muen9twOK4njgX4LMlqle1XPcloZ+zCSq3O7pvkwn8DD3W3Vdh4DIVQd7MmADEjc
izztiE1gMQJ9+1EklywOVSw46D84AHxCOjCzi7RLllkJa8/bAbpTWfCLAtsRoBhq
GkYFZL7TQkc8Y74a3UyZ2G7iT9E8Kzk4NMaqDZzoQb9tc/VQ2mVpMh7ChaXHSFU0
o6C6p+jlrRXou5wJ3buenh8ciRjVlHFptf4FAnXake6ifh8Ztg+vhcePDWPMSan8
towfAhbcezBlbbjPAY2D/O6rMaF9qqvPvqViArGOqnkl+10oUhaxJwe4/a1CIEdk
```

```
1SpaoqbKW/gzjb0HgayDdUP4uMx99BOAShHRZylRGbEf1mpUiQtu3PB7glWEQ0rk
jDVBtMFow9GTb8g3F9rLeWvNne0dKtT3n1kHkeJ4e7p2rOY/Ye8EVPtyeYSP0+0j
IFBH0JLVc6NbKz3c0ek8G+48jABmse6F6dKj/yHCrtLINqJnWoCkwsYX3uCwRjz
dhv7GeEo2sHFVadJnJRjhr7juR2IRsVQbYO0LRWt4YNc4tQ//utO1XEmR40doge
jCd6A4jpiSoDmX659MmGG+BWyeEDlyEknvrTgRuOAPZhooGRPzevNKQTn3LpWwCp
8QARAQABwsF8BBgBCAAmFiEEHCsXwdfAMaYrL3LMPSI7Bo9iCM4FAMV34k0FCQWj
moACGwwACgkQPSI7Bo9iCM7BxRAAgoXkCwqMfg5kFCE41jXVC73fw5FaWMSy/c+t
j05FGgEZnMVXkEYE3TLZChLnFG0YEZmTPa4yaZIJX76raloqWA1nW7gwzIGJI9UR
kAJPzDWb9sIDQwT24nMTvry7JpYpuKoTKwnzTXyOyc01FNz2Sn+drji8G54ZUTen
FHZP7wdAexpsU05rFQQ0J9yBAvdGZuKA75uW69pKfUhLJCvdSOS4UL5JI9pzhC1y
rY+EnVGeak98ILBTLDuOeLBOYh+PEHY6Rcdx+tx3nDdl8N2EP/3IBPER6tpzJTAq
wwMppj586YIPgzKQ2SDe9/SLAGQqzBj/gz6yRbamqL4xEuLyDKz+Mf2TcjMF8Txr
EA82uojTSaxLISNn27Zkhl+V1E/Kwxm+6uT0PZU369P6VMyPt0BqvXoo7orklesL
Ygt/yjC5DnDeT+Xk+LUkvE/mb6APqs5/LZzur1+XgqBxrgkWrwewNzQeiztkRQOP
DljZO/svatXJxQ9XNQtBBtOO3TKJeNisdMVB/Mq40wnK71MeA5mbFWtBj896E0fW
OqnJGMXZx4TpakVguW40XzsnP5smX1jbvKlOMriy0e/uKAlu2pcJaAW6vo+v2xnR
Sk7IlU6IGU1ynrywuvRoMMWig620YLSyJ4x+3MTsAoShpeQ0Lelwxi8Z89BjL6xKT
fRmLEL0=
=g7vA
-----END PGP PUBLIC KEY BLOCK-----
```

File PGP key ini tersedia pada :

<https://csirt.bintankab.go.id/storage/public-key/pgp-key-bintan.asc>

2.9. Anggota Tim

Ketua BINTAN-CSIRT adalah Kepala Dinas Komunikasi dan Informatika Kabupaten Bintan. Yang termasuk anggota tim adalah staf Dinas Komunikasi dan Informatika Kabupaten Bintan serta perwakilan pelaksana pada Organisasi Perangkat Daerah Kabupaten Bintan adalah sebagai Agen Siber pada Pemerintah Kabupaten Bintan.

2.10. Informasi/Data lain

Tidak ada

2.11. Catatan-catatan pada Kontak BINTAN-CSIRT

Metode yang disarankan untuk menghubungi BINTAN-CSIRT adalah melalui e-mail pada alamat csirt@bintankab.go.id ke Dinas Komunikasi dan Informatika Kabupaten Bintan yang siaga selama hari dan jam kerja.

3. Mengenai BINTAN-CSIRT

3.1. Visi

Visi BINTAN-CSIRT adalah terwujudnya pengelolaan keamanan informasi di lingkungan Pemerintah Kabupaten Bintan sesuai dengan prinsip keamanan informasi untuk menjamin ketersediaan (availability), keutuhan (integrity), dan kerahasiaan (confidentiality).

3.2. Misi

Misi dari BINTAN-CSIRT, yaitu :

- a. Mendorong kegiatan pengamanan informasi dan pencegahan insiden keamanan informasi.
- b. Membangun kesadaran keamanan informasi pada sumber daya manusia di lingkungan Pemerintah Kabupaten Bintan.

3.3. Konstituen

Konstituen BINTAN-CSIRT meliputi Organisasi Perangkat Daerah (OPD) sebagai pengguna Teknologi Informasi dan Komunikasi di lingkungan Pemerintah Kabupaten Bintan.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan BINTAN-CSIRT bersumber dari Anggaran Pendapatan dan Belanja Daerah Kabupaten Bintan.

3.5. Otoritas

BINTAN-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan secara administratif dengan konstituennya pasca insiden keamanan siber pada Pemerintah Kabupaten Bintan. BINTAN-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya namun tidak pada persoalan hukum dan dapat bekerjasama dengan pihak lain yang mempunyai kompetensi untuk insiden yang tidak dapat ditangani.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

BINTAN-CSIRT menangani insiden yaitu:

- a. Web Defacement;
- b. Distributed Denial Of Service (DDOS);
- c. Malware;
- d. Ransomware;
- e. Spamming;
- f. Phising.

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

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

5. Layanan

5.1. Layanan Utama

Layanan utama dari BINTAN-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh BINTAN-CSIRT berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik terkait layanan ini diberikan oleh BINTAN-CSIRT.

5.1.2. Penanganan Insiden Siber

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

5.2. Layanan Tambahan

Layanan tambahan dari BINTAN-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini diberikan oleh BINTAN-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 kerawanannya tidak dapat ditangani;
- b. Layanan penanganan kerawanan yang dimaksud dapat juga merupakan tindak lanjut atas kegiatan Vulnerability Assessment.

5.2.2. Penanganan Artefak Digital

Layanan ini diberikan oleh BINTAN-CSIRT berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi. BINTAN-CSIRT memberikan informasi statistik terkait layanan ini.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan pemberitahuan hasil pengamatan potensi ancaman yang dimiliki BINTAN-CSIRT ditujukan kepada Organisasi Perangkat Daerah (OPD) di Lingkungan Pemerintah Kabupaten Bintan sebagai Pengguna Teknologi Informasi dan Komunikasi.

5.2.4. Analisis Risiko Keamanan Siber

Layanan ini diberikan BINTAN-CSIRT berupa analisis resiko terhadap insiden keamanan siber serta pemberian rekomendasi teknis berdasarkan hasil analisis tersebut.

5.2.5. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan konsultasi terkait kesiapan penanganan insiden siber di Lingkungan Pemerintah Kabupaten Bintan dilakukan berdasarkan permintaan dari Organisasi Perangkat Daerah (OPD) sebagai Pengguna Teknologi Informasi dan Komunikasi.

5.2.6. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Dalam layanan ini BINTAN-CSIRT mendokumentasikan dan mempublikasikan berbagai kegiatan yang dilakukan oleh Dinas Komunikasi dan Informatika Kabupaten Bintan dalam rangka pembangunan kesadaran dan kepedulian terhadap keamanan siber.

6. Pelaporan Insiden

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

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

7. Disclaimer

1. BINTAN-CSIRT hanya merespon dan menangani insiden keamanan siber yang terjadi pada Perangkat Daerah di Lingkungan Pemerintah Kabupaten Bintan;
2. Terkait penanganan insiden jenis malware tergantung dari ketersediaan *tools* yang dimiliki;
3. Setiap tindak pencegahan akan diambil dalam penyusunan informasi, pemberitahuan dan peringatan, maka BINTAN-CSIRT tidak bertanggung jawab atas kesalahan dan kelalaian atau kerusakan yang diakibatkan dari penggunaan informasi yang terkandung dalamnya. BINTAN-CSIRT juga tidak memiliki wewenang dalam persoalan hukum.