

RFC 2350 Labusel-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 1 Juli 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://ttis.labuhanbatuselatankab.go.id>

1.4. Keaslian Dokumen

Dokumen telah ditandatangani dengan sertifikat elektronik milik Dinas Komunikasi dan Informatika Kabupaten Labuhanbatu Selatan.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 Labusel-CSIRT

Versi : 1.0

Tanggal Publikasi : 1 Juli 2026;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Tim Tanggap Insiden Siber - Computer Security Incident Response Team Kabupaten Labuhanbatu Selatan

Disingkat : Labusel-CSIRT

2.2. Alamat

Dinas Komunikasi dan Informatika kabupaten Labuhanbatu Selatan

Komplek Perkantoran Pemkab. Labuhanbatu Selatan Jalan Lintas Sumatera Desa Sosopan Kecamatan Kotapinang

2.3. Zona Waktu

xxx (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*)

ttis@labuhanbatuselatankab.go.id

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

Bits : -

ID : E4EC 62BA D746 8228

Key Fingerprint : 339D BE9E E7A5 9D54 5418 7898 E4EC 62BA D746 8228

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

```
mDMEag7L6xYJKwYBBAHaRw8BAQdALFvf8WlrrzK8aqF+08hKuKNiBdwpVIPuhIOj
LFeJk2C0NUxhYnVzZWwtQ1NJUIQgPGluZm9ybWFzaUBsYWJ1aGFuYmF0dXNlbGF0
YW5rYWluZ28uaWQ+ilUEExYKAF0WlQQzn6e56WdVFQYeJjk7GK610aCKAUCag7L
6xsUgAAAAAAEAA5tYW51MiwylJUrMS4xMiwylDECGwMFCQWksWUFCwkIBwIClgIG
FQoJCAAsCBBYCAwECHgcCF4AACGkQ5OxiutdGgihF8QEAo3FRn5jzcSVX9NVi9i/n
6UGaqkL02ZcPM3paV2W2dGYBAOhlWPVFqTB3IOyBMtu/YvV0QYixYD9YEP8a3fvF
m/YEuDgEag7L6xIKKwYBBAGXVQEFAQEHEQJNtJpFy1tH1Ned9ZvxcCClgBolUjlzs
EILGNCWil6w2AwEIB4iaBBgWCgBCFiEEM52+nuelnVRUGHiY5OxiutdGgigFAmoO
y+sbFIAAAAAABAAObWFudTIsMi41KzEuMTIsMiwxAhsMBQkFpLFIAAoJEOTsYrrX
Roloq7sA/06ECVG1EDcuJr9eMGSkMudMt25SmCuyGv7gfREsJY92AQDg5QjAnuPH
s6vKg/QWJ/ARmuFO4Dzyvtuqecg/vN08Dg==
=oykQ
```

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

File PGP key ini tersedia pada :

ttis@labuhanbatuselatankab.go.id

2.9. Anggota Tim

Ketua Labusel-CSIRT adalah Kepala Dinas Komunikasi dan Informatika kabupaten Labuhanbatu Selatan Yang termasuk anggota tim adalah seluruh staf pada Dinas Komunikasi dan Informatika dan Organisasi Perangkat Daerah Kabupaten Labuhanbatu Selatan adalah sebagai agen penanganan insiden siber pada Pemerintah Kabupaten Labuhanbatu Selatan.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak Labusel-CSIRT

Metode yang disarankan untuk menghubungi Labusel-CSIRT adalah melalui *e-mail* pada alamat ttis@labuhanbatuselatankab.go.id atau melalui nomor whatshap 082168787337 pada hari kerja jam 07.45 - 16.30 (Senin-Kamis) dan 07.45 - 16.00 (Jumat).

3. Mengenai Labusel-CSIRT

3.1. Visi

Visi Labusel-CSIRT adalah terwujudnya penyelenggaraan sistem elektronik yang baik memenuhi kaidah kerahasiaan, integritas, ketersediaan, keautentikan, otorisasi dan kenirsangkalan melalui penyelenggaraan keamanan siber yang handal dalam penanggulangan dan pemulihan insiden siber di lingkungan Pemerintah Kabupaten Labuhanbatu Selatan

3.2. Misi

Misi dari Labusel-CSIRT, yaitu :

- a. Membangun pusat pencatatan, pelaporan, penanggulangan dan pemulihan insiden siber di lingkungan Pemerintah Kabupaten Labuhanbatu Selatan;
- b. Menyelenggarakan penanggulangan dan pemulihan insiden siber melalui kegiatan mendeteksi, menganalisis, mitigasi, pemulihan dan melakukan upaya pencegahan terhadap insiden siber
- c. Membangun skema kerja dalam penanggulangan dan pemulihan dengan melakukan koordinasi dan kerja sama dalam rangka mencegah dan/atau mengurangi dampak dari Insiden Siber pada konstituen;
- d. Membangun kapasitas sumber daya keamanan siber pada sektor Pemerintah Kabupaten Labuhanbatu Selatan; dan
- e. Meningkatkan kesadaran pentingnya keamanan informasi bagi sumber daya manusia di lingkungan Pemerintah Kabupaten Labuhanbatu Selatan.

3.3. Konstituen

Konstituen Labusel-CSIRT meliputi Perangkat Daerah penyelenggara sistem elektronik di lingkungan Pemerintah Kabupaten Labuhanbatu Selatan.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan Labusel-CSIRT bersumber dari Anggaran Pendapatan dan Belanja Daerah (APBD).

3.5. Otoritas

Labusel-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber di lingkungan Pemerintah kabupaten Labuhanbatu Selatan.

Labusel-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya namun tidak ada persoalan hukum dan dapat berkoordinasi serta bekerjasama dengan BSSN/ Akademisi bidang IT Security/ Tenaga Ahli Security/pihak lain untuk insiden yang tidak dapat ditangani.

4. Kebijakan – Kebijakan

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

Labusel-CSIRT melayani penanganan insiden siber dengan jenis berikut :

- a. *Web defacement*
- b. *DDOS (Distributed Denial of Service)*
- c. *Malware*
- d. *Phising*

Dukungan yang diberikan oleh Labusel-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis, dampak insiden dan layanan yang digunakan.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Labusel-CSIRT akan melakukan kerjasama dan berbagi informasi dengan Dinas Komunikasi dan Informatika Propinsi Sumatera Utara, BSSN selaku Gov-CSIRT dan TTIS atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh Labusel-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, Labusel-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 dan Fungsi

5.1. Layanan

Layanan dari Labusel-CSIRT yaitu :

5.1.1. Penanggulangan Dan Pemulihan Insiden Siber

TTIS memiliki peran penting dalam melakukan penanggulangan dan pemulihan dengan melakukan kegiatan mendeteksi, merespons, dan mengatasi insiden keamanan siber. Berikut adalah beberapa layanan dalam konteks penanggulangan dan pemulihan insiden siber:

- a. deteksi insiden: mendeteksi aktivitas mencurigakan atau tanda-tanda insiden keamanan siber.
- b. analisis insiden: menganalisis insiden untuk memahami asal usul, dampak, dan metode serangan.
- c. mitigasi dan penanggulangan: mengambil tindakan cepat untuk mengurangi dampak insiden dan menghentikan serangan.
- d. pemulihan: membantu organisasi dalam pemulihan operasi normal setelah insiden.
- e. analisis forensik: menyelidiki asal usul insiden dan mengumpulkan bukti forensik jika diperlukan.
- f. rekomendasi pencegahan: memberikan saran untuk mencegah insiden serupa di masa depan.

5.1.2. Penyampaian informasi insiden siber kepada pihak terkait

Pemberian informasi insiden siber bertujuan untuk memberikan informasi dan peringatan yang relevan tentang potensi ancaman atau kerentanan keamanan siber kepada pemilik sistem elektronik.

Pemberian informasi penting dalam membantu organisasi untuk membantu pihak terkait dalam merespons ancaman dengan cepat dan efektif.

5.1.3. Diseminasi Informasi Untuk Mencegah dan/atau Mengurangi Dampak dari Insiden Siber

Desiminasi informasi penting dalam membantu organisasi untuk menjaga keamanan informasi dalam upaya mencegah dan/atau mengurangi dampak dari insiden siber. Dengan informasi yang tepat, penyelenggara sistem elektronik dapat menyusun kebijakan dan melakukan tindakan yang sesuai guna mengurangi risiko dan merespons insiden keamanan siber dengan lebih baik.

5.2. Fungsi

5.2.1. Fungsi Utama atas layanan Labusel-CSIRT

- 5.2.1.1. pemberian peringatan terkait Keamanan Siber;
- 5.2.1.1. perumusan panduan teknis penanganan Insiden Siber;
- 5.2.1.1. pencatatan setiap laporan/aduan yang dilaporkan, pemberian rekomendasi langkah penanganan awal kepada pihak terdampak;
- 5.2.1.1. pemilahan (triage) Insiden Siber sesuai dengan kriteria yang ditetapkan dalam rangka memprioritaskan Insiden Siber yang akan ditangani;
- 5.2.1.1. penyelenggaraan koordinasi penanganan Insiden Siber kepada pihak yang berkepentingan; dan
- 5.2.1.1. diseminasi informasi untuk mencegah dan/atau mengurangi dampak dari Insiden Siber.

5.2.2. Fungsi Lain atas layanan Labusel-CSIRT

5.2.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini diberikan 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 berupa tindak lanjut atas kegiatan *Vulnerability Assessment*.

5.2.2.2. Penanganan Artefak Digital

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

5.2.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini diberikan berupa pemberitahuan hasil pengamatan potensi ancaman dan sistem deteksi yang dilakukan mandiri maupun dari BSSN. Labusel-CSIRT memberikan informasi kepada penyelenggara sistem elektronik terkait layanan ini.

5.2.2.4. Pendeteksian Serangan

Layanan ini berupa identifikasi kerentanan, penilaian risiko atas kerentanan, serta hasil dari perangkat pendeteksi serangan yang ditemukan. Labusel-CSIRT memberikan informasi terkait layanan ini.

5.2.2.5. Analisis Risiko Keamanan Siber

Layanan ini berupa analisis risiko keamanan siber. Labusel-CSIRT memberikan informasi terkait layanan ini

5.2.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan ini diberikan Labusel-CSIRT berupa konsultasi terkait prosedur, metode dan teknis penanganan insiden siber dalam upaya penanggulangan dan pemulihan insiden.

5.2.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Labusel-CSIRT melaksanakan, mendokumentasikan, dan mempublikasikan kegiatan Dinas Komunikasi dan Informatika Kabupaten Labuhanbatu Selatan dalam rangka pembangunan kesadaran dan kepedulian terhadap keamanan siber.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke <http://ttis.labuhanbatuselatankab.go.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

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

Kotapinang, Juli 2026
Kepala Dinas Komunikasi dan Informatika
Kabupaten Labuhanbatu Selatan



Muhd Iqbal Nasution, S.STP, M.Si
NIP.198503302003121001