RFC 2350

Pesisir Barat - CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 10 September 2025.

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.pesisirbaratkab.go.id/rfc2350

1.4. Keaslian Dokumen

Dokumen telah ditandatangani dengan sertifikat elektronik milik Dinas Komunikasi dan Informatika Kabupaten Pesisir Barat.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 Pesisir Barat - CSIRT
Versi	: 1.0
Tanggal Publikasi	: 10 September 2025 ;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Tim Tanggap Insiden Siber Kabupaten Pesisir Barat - *Computer Security Incident Response Team*
Disingkat : Pesisir Barat – CSIRT

2.2. **Alamat**

Dinas Komunikasi dan Informatika Statistik dan Persandian kabupaten Pesisir Barat
Gedung A, Perkantoran Pemerintah Kabupaten Pesisir Barat Lantai 1
Jl Kusuma, Kecamatan Pesisir Tengah, Kabupaten Pesisir Barat, Provinsi Lampung

2.3. **Zona Waktu**

Jakarta (GMT+07:00)

2.4. **Nomor Telepon**

0822-8180-9139 (ANSORI, S.Pd – Kepala Bidang Statistik dan Persandian)
0851-2953-9545 (ILLAL AL FARIZ, S.Kom – Sandiman Ahli Pertama)
0851-5730-2272 (NABILA KARIMA AZKA,S.Kom – Penata Kelola Sistem & Teknologi Informasi)

2.5. **Nomor Fax**

Tidak Ada

2.6. **Telekomunikasi Lain**

Tidak ada

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

ttis@pesisirbaratkab.go.id

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

Bits : 4.096-bit
ID : pesibar-TTIS <ttis@pesisirbaratkab.go.id>
Key Fingerprint : D2A0 6D6D 89C1 D593 D6BC 8F14 4A9A B314 4168 8493 36EB
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGlcr3sBEADitbuSjjUsKzYjoHLDgd9LTWS6C7TMgOywwQC8XGDQ
SxzlnPPzvnUKRBBd7V75HPL7S5iu6Tt15VY8aqXAn6IEjcs9CxYx8N/m3vjn
a2lscsIGuSR9iE8QSf5OgECm0AioUQqlcSUOrTCRqtt5HdbS4vXFnRgERA
WcpAOiC1jCwXZFrist13smQ/mfdY6H+YQKe7mebxXIjIL7U4GSjDTmXlHstA
7+N8t4SFFmDf0VKOr2omYH3wf6VEXqd4fsBcuRjD4E1M7bmAhwq5BfCc1
YCyJxIcsEtNAHdwXQjMV+kj+NDw0nx79nRwd5JREJxKYeRrA6pW8xiXFA
G1Y/bwtm/QVhfpfYpiKVNgvEUQy94/ny8zYBY0cBeJ62LqR1WR749ABO7s
eRQ9D/QcSuxkUMlqM6jlOw4TdU+lplnjOL11CFPbPLx6aJvwNdSYeaAt5Vm
2iygq4GAonkdnlC2lB4Qf+hyWGBRRE8Vm7iIvl/OYodJKN9pUwxYhHaGRa

DQtppW17yXcy66YIMtOAFkGFX5h2XUqo0bLu+1/mJ02FTMzc2XpPxTS7x
U8shC64zxEvYhjez5rGIYAd2vhunYiIF5DSnBdi54x3qhw6+emgot97lZK2q
fyaRYI9KXh5h1mgKBw1YqRlaWT7n3tjKDbhpzHTmpFVgn4neopWgyvD4X
wARAQABtClwZXNpYmFyLVRUSVMgPHR0aXNAcGVzaXNpcmJhcmF0a2
FiLmdvLmlkPokCVwQTAQgAQQIbAwULCQgHAgIiAgYVCgkICwIEFgIDAQI
eBwIXgBYhBNKgbW2JwdWT1ryPFEqasxRBaISTBQJpXLGtBQktJUzYAAo
JEEqasxRBaIST7H8QALafCXfLaV6vHRZoB4CHnVi5oG/U7GJuoaxBGc/2rz
YmquPGP/gVpjQb9mM6XnusL5yyyE5J62O4soUEoXoRTeIoMKyUpHU/eo9
4rZ2B8PijH5KpqgRUgGwR/he3OKXHXuVmqtcn1uUacVD7P5iyfpsQMyolJB
cFbNAAm7P7jEfUmcNzHnPI6jHDNskw5wGx9t7kfXgzREGp/MkJCcom6BZ
AUNAQ5mFAqxpz1oqsaST7tHPYz4eOpVo/tGNxfFqKwWns5z/fzzgF9RLc
/HMGUhdUA0fUVhZLihYFZoFyuRV7wJ1UblCMT7tZpUkgygBElLb21i9fzf5K
dOk9jziEvaek70QKsrCgv2vrlR3c9pQsFbO9f4XZI8ylvI0cDfB0nwy04lel1xjaX
oZbcnhAh7AiHdFzyqUQe7OFTjFEGFLPoykj4b2TrzVLzzynpUGlVbOseSNdr
1Ag6peVRD63YEv6UwFZElomsxmfcHH3mnNkG4ymsF29BxpkF7iQY2Ng1
BLQQlhXxqFtqoJMaDUngdhZGY5wIpbiBQ/6tJt8C6L/LyG81AvwGUGn2ab1
MDREBslNLfPCq7XCIyjJHhU4e5Ok0Q5OWNgA2rF70feWZr7QqMAJHUnG
D36qCLeTOTBsXhc4NOHlslgNuZDbBE2BhdsEeiwxRJByqY7QwROKop9tt
DJQZXNpc2lyIEJhcmF0IC0gQ1NJUlQgPHR0aXNAcGVzaXNpcmJhcmF0a2
FiLmdvLmlkPokCVwQTAQgAQRYhBNKgbW2JwdWT1ryPFEqasxRBaISTB
QJqMw9RAhsDBQktJUzYBQsJCAcCAiICBhUKCQgLAgQWAgMBAh4HAhe
AAAoJEEqasxRBaISTbukQAKoQW9LzaIqPG7zU9Adv7NGkN84reRiNuN1
Qnixc9T5p2NK4qAUiSim020Kse90JrTNcpxwSvAD/e8wK+AYIRG2+JoB+ay
h3cRv66UXtKsvpvY5WmAEmP13o9/QeCfI9ORAQpbm9cQpOmrrJ8r4nLee
+DDcOzw/hOP+XLH2+6PvI9RlzmYCXDn+ezVVddGcOfwWpm1qccAOdQB
aUPAcSRJqh0hteXfCgZRdI9wC5w8X7UVu24L+FeaT9ibPDzpx+i2XkfrOBzh
/aGxt65kJi6+CUa2VuMUP8hFccMtX5nrCUOMM0AX6GtQaH2BAZKSvkWa
0IV3HCOQA2YUku5LjMIFP/NvWI2ODOcWlSBAv6v1Xf/4uRpNpKTQQuOQ
pk7g7Y7yOBcmx3ol/86DXrzNyAmjC1Q8rJQOvBp9uUzeWIb9r68f5jEHhQuI
Wgp/KrKmBz1P1zljCPUgbxUFSFMzEGeGWSeb9zetUajRIwZl+qZ6rCop7Fp
1g1wA0zJhaEpBd3lmEOrqFjS7j7r1CrQWz9K5cTV62hBsBGwwv5z2p48oU
SNjDyzvA7RDO3JOs5xxlSDcgsXVzOVHcPbXRn6XA8N6AzNDgYxXvDJ12/
NzKz4BtpzG2fsBfyZlxTxFCz5IXbb3WaFC/8e6xeTlJxu4AHh1c8yCpAd5qzm
oDPCBNImqCjuQINBGlcr3sBEADl4IHBsIyHCGyORWUMgZEl+quVdXQcisq
VaUfXGiC+EGhuaNz0wzBtlTxexbja7FogUroth2v+Njd8XHa7SEiFLdrGUaiiM
Y3OZf6lDhmFIOVe49cKdHVn9qX1YlR33WcdFJ8oY4SLSDKwT0m6YVU+X
b+nHLinNYXT+AAa9MoFYJQRG9mwA5gHnxjFbTVW8xSNJEyKMpbWFqS
DZuxXrhEiAlopVZq5oNAoq3f1e0r8IkEZ+6ckJVDcsIMN25GQmGP8ZcklIUu6
NWjAPpAsacB1lueGp7XyWWEW1EZfXNg6DQjyiuyymDboEfFKZEiovQi2Nr
dH0o8pCqeDoEoE8w1e/RCrrkaXvReOHz+c5TrUv744KJ9k79gDyvXiB42Ar
Y7gqr/ZfDoJX3Y3W4iWTReFhWqr9mhe2vcy6j32EiDnW+uUe6AA3uGQV0x
fG7QNdPnLK05MJ0nwRiwzc6kRUyCi3ZMO9S1F/H9fGOugEAGSoIhzKRPv
ecXV5EQFtyEmXIJ3vUu9OVa7CGkqQOsbblkJU1IhYjAz50/vCn7Wb+bgfp1
MdgoiYqSnwgmBG7tGew16ustyQBPAqvOz0DWI2Xtd03n0P2KskYaKeu9Ri

r2MIELyDoeS2WTJN7YGGJikLqEP6dHg8iXqNT0iibdKCk0pjdVWxu2y1h83
XMGZHNDAXQARAQABiQI8BBgBCAAmAhsMFiEE0qBtbYnB1ZPWvI8USp
qzFEFohJMFAmlcsa0FCS0lTNgACgkQSpqzFEFohJOrzg/7BqD2lspszo5NG
ljK8SUOM5D28m+tW9c1qfp5AnQ/+GrY7QM0c3GFvO7JDHCdOD74zpBw5i
cpgQhQQNWDB+Y9nGTVMw2iTAyHYzxuoMRZqPpU2HQwTdP/f9d7MSJ+
dMWfFOT9W6XjpPyNUhLexwOOSo9NYO+u6KmcZHA1s52ILvUb8o1zf2bQ
LjVnFts3e0wgTQ0dPdtyMZ46NSpTuy0c3zzap91+teXBtLeOG5ocDsYcFzO
YsKBc04C9BHQlLtO5MFd21pkMCt4pPeQD08SBKdArlmJnsvhIqDlFp2nng
mOxp/ZK/YZLGObG/9TgpepeNqW+D5RHPZsxNzlj1SrvFimf1tY8NLrCG869
YmVD6ZlZ7N4IsH/x8lUXzeMSWfM0ZswrwB8DjfbF+2O0NbfAC/w3vAglJtW
CE/7dFCc6a19ROtwcI82O0HYdnNJAEeqdyNRFa9pVHC/1/gOvAehqWVM8
giDx0V8ycCxZ3OzoJGvhzu5n3Dlt9UUjF6JeqkcdCKpoyZH2cgza/5uR32X21
kEQJqkkIKlbbV0KIqhSlNRbv9Hl02ibSB4zO+HVOK/ewqwtt0zCPHLXFicsh6
wg6FtgJFxyRUZVRMzM7V2t2J5vcJ6V2u993gAUo91JtTmBAfp7Jj1FdbH9s
dVassMdp9X/jTUNAUKsl2S77A9Cxoo=
=YV+j
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirt.pesisirbaratkab.go.id/rfc2350

2.9. **Anggota Tim**

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

2.10. **Informasi/Data lain**

Tidak ada.

2.11. **Catatan-catatan pada Kontak** Pesisir Barat - CSIRT

Metode yang disarankan untuk menghubungi Pesisir Barat - CSIRT adalah melalui *e-mail* pada alamat ttis@pesisirbaratkab.go.id atau melalui nomor telepon 089633796074 pada hari kerja jam 07.30 - 15.30 (Senin-Kamis) dan 07.30 - 14.30 (Jumat).

3. Mengenai Pesisir Barat - *CSIRT*

3.1. **Visi**

3.2. Visi Pesisir Barat – CSIRT adalah terwujudnya penyelenggaraan sistem eletronik 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 Pesisir Barat.

3.3. **Misi**

Misi dari Pesisir Barat - CSIRT, yaitu :

a. Membangun pusat pencatatan, pelaporan, penanggulangan dan pemulihan insiden siber di lingkungan Pemerintah Kabupaten Pesisir Barat;
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 Pesisir Barat; dan
e. Meningkatkan kesadaran pentingnya keamanan informasi bagi sumber daya manusia di lingkungan Pemerintah Kabupaten Pesisir Barat.

3.4. **Konstituen**

Konstituen Pesisir Barat - CSIRT meliputi Perangkat Daerah penyelenggara sistem elektronik di lingkungan Pemerintah Kabupaten Pesisir Barat.

3.5. **Sponsorship dan/atau Afiliasi**

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

3.6. **Otoritas**

Pesisir Barat - CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber di lingkungan Pemerintah kabupaten/Kota Pesisir Barat.

Pesisir Barat - 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

Pesisir Barat - 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 Pesisir Barat - CSIRT kepada konstituen dapat bervariasi bergantung dari jenis, dampak insiden dan layanan yang digunakan.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Pesisir Barat - CSIRT akan melakukan kerjasama dan berbagi informasi dengan Pesisir Barat - CSIRT, BSSN selaku Gov-CSIRT dan TTIS atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh Pesisir Barat - CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, Pesisir Barat - CSIRT dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional), telepon atau fax. 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 Pesisir Barat - CSIRT yaitu :

5.1.1. Penanggulangan Dan Pemulihan Insiden Siber

TTIS/CSIRT 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 Pesisir Barat - 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 Pesisir Barat - 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. Pesisir Barat - 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. Pesisir Barat - CSIRT memberikan informasi terkait layanan ini.

5.2.2.5. Analisis Risiko Keamanan Siber

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

5.2.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan ini diberikan Pesisir Barat - 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

Pesisir Barat - CSIRT melaksanakan, mendokumentasikan, dan mempublikasikan kegiatan Dinas Komunikasi dan Informatika Kabupaten/Kota Pesisir Barat dalam rangka pembangunan kesadaran dan kepedulian terhadap keamanan siber.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke ttis@pesisirbaratkab.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. Pesisir Barat - CSIRT hanya merespon dan menangani insiden keamanan siber yang terjadi pada Perangkat Daerah di Lingkungan Pemerintah Kabupaten Pesisir Barat;

b. Terkait penanganan insiden siber tergantung dari ketersediaan *tools* yang dimiliki;

c. Setiap tindak pencegahan akan diambil dalam penyusunan informasi, pemberitahuan dan peringatan, maka Pesisir Barat - CSIRT tidak bertanggung jawab atas kesalahan dan kelalaian atau kerusakan yang diakibatkan dari penggunaan informasi yang terkandung dalamnya. Pesisir Barat - CSIRT juga tidak memiliki wewenang dalam persoalan hukum.