# RFC 2350 BPOLBF-CSIRT

## 1. Informasi Mengenai Dokumen

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

### 1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 18 September 2025.

### 1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan pembaruan dokumen.

### 1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://bpolbf.sgp1.digitaloceanspaces.com/uploads/PpidPublicInformation/z0UsmBgcVpIsSCWKQgibaShcQ4Tm4DkHbqxpz4bT.pdf (versi Bahasa Indonesia)

### 1.4. Keaslian Dokumen

Dokumen telah ditanda tangani dengan PGP *Key* milik BPOLBF-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

### 1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

| | |
|---|---|
| Judul | : RFC 2350 BPOLBF-CSIRT; |
| Versi | : 2.0; |
| Tanggal Publikasi | : 20 November 2025; |
| Kedaluwarsa | : Dokumen ini valid hingga dokumen terbaru dipublikasikan. |

## 2. Informasi Data/Kontak

### 2.1. Nama Tim

Kepanjangan dari Badan Pelaksana Otorita Labuan Bajo Flores-*Computer Security Incident Response Team*
Disingkat : BPOLBF-CSIRT.

### 2.2. Alamat

Badan Pelaksana Otorita Labuan Bajo Flores
Jln. Soekarno Hatta No.88, Labuan Bajo, Kec. Komodo, Kabupaten Manggarai Barat, Nusa Tenggara Timur

### 2.3. Zona Waktu

Labuan Bajo (GMT+08:00)

**2.4. Nomor Telepon**

(+62) 811-3879-4555

**2.5. Nomor Fax**

(tidak ada)

**2.6. Telekomunikasi Lain**

(tidak ada)

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

bpolbfcsirt@gmail.com

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

Bits : 255
ID : 0xC353B519DAE7CEB5
Key Fingerprint : B4CC 880F A79F 7D78 9681 BFEF C353 B519 DAE7 CEB5

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

mDMEaMkKtBYJKwYBBAHaRw8BAQdAUnEDSva2biYChn4oyZiMUx/RmnfDtZOyapi4
NHVs8/60JEJQT0xCRiBDU0lSVCA8YnBvbGJmY3NpcnRAZ21haWwuY29tPoiZBBMW
CgBBFiEEtMyID6effXiWgb/vw1O1GdrnzrUFAmjJCrQCGwMFCQWkwgwFCwkIBwIC
IgIGFQoJCAsCBBYCAwECHgcCF4AACgkQw1O1GdrnzrVD1wEApT0qnmFKywax13Iw
o+WWxnr4PAI1jwFE+O8LJwpbvfQBAPjzpjzOdypuVHr6oCBqCdBiTGd4OI6zMrzr
UYVj+XkKuDgEaMkKtBIKKwYBBAGXVQEFAQEHQMW49WTH/H+locAxVdks6wTutwyn
Wdoi5/V0RkRqDGQ2AwEIB4h+BBgWCgAmFiEEtMyID6effXiWgb/vw1O1GdrnzrUF
AmjJCrQCGwwFCQWkwgwACgkQw1O1GdrnzrW/IwD/fh48ShxweDyWVfTXXA7TolXT
5FZQ/xUdZMBL7gZUul0BAOl/lWJ/bdUf+Berb1ARHZWCCBhU0kQMBzkniGAnJs8B
=JuHU
-----END PGP PUBLIC KEY BLOCK-----

**2.9. Anggota Tim**

Ketua BPOLBF-CSIRT adalah Kepada Divisi Komunikasi Publik, dengan anggota tim adalah Staf BPOLBF sesuai dengan Keputusan Direktur Utama BPOLBF Nomor SK/40/UM.04.02/TTIS-CSIRT/BPO.3/2025 tahun 2025 tentang Penetapan Tim Tanggap Insiden Siber (TTIS) / *Computer Security Incident Response Team* (CSIRT) Badan Pelaksana Otorita Labuan Bajo Flores (BPOLBF - CSIRT).

**2.10. Informasi/Data lain**

(tidak ada)

**2.11. Catatan-catatan pada Kontak BPOLBF-CSIRT**

Metode yang disarankan untuk menghubungi BPOLBF-CSIRT adalah melalui *e-mail* pada alamat bpolbfcsirt@gmail.com atau melalui nomor telepon (+62) 811-3879-4555 pada hari kerja jam 8.30 - 17.00 WITA.

## 3. Mengenai BPOLBF-CSIRT

### 3.1. Visi

Visi BPOLBF-CSIRT adalah untuk melindungi infrastruktur Teknologi Informasi yang dimiliki oleh Instansi Pemerintah dalam memberikan layanan berbasis elektronik kepada para konstituennya terhadap berbagai kemungkinan Insiden Siber yang terjadi.

### 3.2. Misi

Misi dari BPOLBF-CSIRT, yaitu :

a. Memelihara keamanan operasional layanan TI;
b. Melakukan penanganan Insiden Siber yang mengganggu operasional layanan TI;
c. Melakukan pemulihan operasional TI pasca terjadinya Insiden Siber; dan
d. Melakukan mitigasi risiko dan potensi terjadinya Insiden Siber

### 3.3. Konstituen

Konstituen BPOLBF-CSIRT yakni semua pengguna layanan teknologi informasi di lingkungan Badan Pelaksana Otorita Labuan Bajo Flores.

### 3.4. Sponsorship dan/atau Afiliasi

Pendanaan BPOLBF-CSIRT bersumber dari Anggaran Pendapatan dan Belanja Negara (APBN).

### 3.5. Otoritas

BPOLBF-CSIRT memiliki kewenangan dengan konstituennya dalam penanganan gangguan keamanan siber. BPOLBF-CSIRT dapat berkoordinasi serta bekerja sama dengan pihak lain yang mempunyai kompetensi untuk insiden yang tidak dapat ditangani.

## 4. Kebijakan – Kebijakan

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

BPOLBF-CSIRT melayani penanganan insiden siber dengan jenis berikut:

a. *Pishing*
b. Malware
c. Web-deface

### 4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

### 4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, BPOLBF-CSIRT dapat menggunakan 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. Penanggulanan dan Pemulihan Insiden Siber

#### 5.1.1. Deteksi Insiden

Layanan deteksi insiden dalam BPOLBF-CSIRT mencakup pemantauan berkelanjutan terhadap sistem dan jaringan untuk mengidentifikasi aktivitas mencurigakan, analisis ancaman untuk memahami potensi risiko, serta implementasi sistem peringatan dini yang memberikan notifikasi saat insiden terdeteksi. Tim BPOLBF-CSIRT bertanggung jawab untuk merespons insiden dengan prosedur yang jelas, memberikan rekomendasi teknis untuk meningkatkan keamanan, dan menyusun laporan mendetail mengenai insiden yang terjadi. Dengan demikian, layanan ini berperan penting dalam mempercepat respons terhadap insiden, meningkatkan kesadaran keamanan, dan mengurangi risiko terhadap organisasi.

#### 5.1.2. Analisis Insiden

Layanan analisis insiden dalam BPOLBF-CSIRT berfokus pada penyelidikan mendalam terhadap insiden keamanan yang terjadi, termasuk pengumpulan dan analisis data untuk memahami penyebab, dampak, dan metode serangan yang digunakan. Tim BPOLBF-CSIRT melakukan forensik digital untuk mengidentifikasi jejak penyerang, mengevaluasi kerentanan yang dieksploitasi, dan menilai kerusakan yang ditimbulkan. Selain itu, layanan ini mencakup penyusunan laporan analisis yang mendetail, yang berisi rekomendasi untuk mitigasi dan pencegahan insiden serupa di masa depan. Dengan layanan analisis insiden yang efektif, organisasi dapat meningkatkan pemahaman mereka tentang ancaman yang dihadapi dan memperkuat strategi keamanan siber mereka secara keseluruhan.

#### 5.1.3. Penilaian Risiko Keamanan Siber dan Mitigasi Insiden Siber

Layanan penilaian risiko keamanan siber dalam BPOLBF-CSIRT bertujuan untuk mengidentifikasi, menganalisis, dan mengevaluasi potensi risiko yang dapat mengancam aset informasi organisasi. Proses ini mencakup penilaian kerentanan (vulnerability assessment) untuk mengidentifikasi kelemahan

dalam sistem dan jaringan, serta pengujian penetrasi (penetration testing) yang mensimulasikan serangan nyata untuk menguji ketahanan sistem terhadap ancaman. Setelah penilaian dilakukan, tim BPOLBF-CSIRT menyusun rekomendasi mitigasi yang spesifik untuk mengurangi risiko yang teridentifikasi, termasuk langkah-langkah teknis dan kebijakan keamanan yang perlu diterapkan. Dengan layanan ini, organisasi dapat memahami profil risiko mereka secara menyeluruh dan mengambil tindakan proaktif untuk melindungi aset informasi serta meminimalkan dampak dari insiden siber yang mungkin terjadi.

### 5.1.4. Pemulihan

Layanan pemulihan insiden siber dalam BPOLBF-CSIRT berfokus pada proses pemulihan sistem dan layanan yang terpengaruh setelah terjadinya insiden keamanan. Tim BPOLBF-CSIRT bertanggung jawab untuk mengembangkan dan menerapkan rencana pemulihan yang mencakup langkah-langkah untuk mengembalikan data, memperbaiki kerusakan, dan memastikan bahwa sistem berfungsi kembali dengan aman. Proses ini melibatkan analisis dampak insiden, identifikasi sumber masalah, serta penerapan tindakan perbaikan yang diperlukan untuk mencegah terulangnya insiden serupa. Selain itu, layanan ini juga mencakup komunikasi dengan pemangku kepentingan dan penyusunan laporan pemulihan yang mendetail untuk evaluasi dan pembelajaran di masa depan. Dengan layanan pemulihan yang efektif, organisasi dapat meminimalkan waktu henti, mengurangi kerugian, dan memperkuat ketahanan mereka terhadap ancaman siber di masa mendatang.

### 5.1.5. Analisis Forensik

Layanan analisis forensik dalam BPOLBF-CSIRT bertujuan untuk melakukan penyelidikan mendalam terhadap insiden keamanan siber dengan mengumpulkan, menganalisis, dan menyimpan bukti digital secara sistematis. Tim forensik bertugas untuk mengidentifikasi jejak penyerang, memahami metode serangan, dan menentukan dampak dari insiden tersebut. Proses ini mencakup pengumpulan data dari berbagai sumber, seperti log sistem, perangkat jaringan, dan perangkat penyimpanan, serta penerapan teknik analisis forensik untuk mengungkap informasi yang relevan. Hasil dari analisis ini akan disusun dalam laporan yang mendetail, yang dapat digunakan untuk tindakan hukum, perbaikan kebijakan

keamanan, dan peningkatan kesadaran di dalam organisasi. Dengan layanan analisis forensik yang efektif, organisasi dapat memperkuat pertahanan mereka, memahami pola serangan, dan mengambil langkah-langkah proaktif untuk mencegah insiden di masa depan.

### 5.1.6. Rekomendasi Pencegahan

Layanan rekomendasi pencegahan dalam BPOLBF-CSIRT bertujuan untuk memberikan saran dan strategi yang efektif untuk mengurangi risiko insiden keamanan siber di masa depan. Tim BPOLBF-CSIRT menganalisis data dari insiden yang telah terjadi, serta hasil penilaian risiko dan analisis kerentanan, untuk mengidentifikasi langkah-langkah pencegahan yang tepat. Rekomendasi ini mencakup penerapan kebijakan keamanan yang lebih ketat, peningkatan kontrol akses, pelatihan kesadaran keamanan bagi karyawan, serta penerapan teknologi keamanan terbaru, seperti firewall, sistem deteksi intrusi, dan perangkat lunak antivirus. Selain itu, layanan ini juga mencakup pengembangan rencana respons insiden yang komprehensif untuk memastikan bahwa organisasi siap menghadapi potensi ancaman. Dengan layanan rekomendasi pencegahan yang proaktif, organisasi dapat memperkuat postur keamanan mereka, mengurangi kemungkinan terjadinya insiden, dan menciptakan lingkungan yang lebih aman bagi aset informasi mereka.

## 5.2. Penyampaian Informasi Insiden Siber Kepada Pihak Terkait

Layanan koordinasi insiden kepada pihak terkait dalam BPOLBF-CSIRT berfokus pada pengelolaan komunikasi dan kolaborasi yang efektif antara berbagai pemangku kepentingan selama dan setelah terjadinya insiden keamanan siber. Tim BPOLBF-CSIRT bertanggung jawab untuk menginformasikan dan berkoordinasi dengan pihak-pihak yang terlibat, termasuk manajemen, tim IT, penyedia layanan eksternal, lembaga penegak hukum, dan Gov-CSIRT, untuk memastikan respons yang terkoordinasi dan efisien. Layanan ini mencakup penyusunan rencana komunikasi yang jelas, penyampaian pembaruan situasi secara berkala, serta pengumpulan umpan balik dari pihak terkait untuk meningkatkan respons. Selain itu, BPOLBF-CSIRT juga berperan dalam mengedukasi pemangku kepentingan tentang langkah-langkah yang diambil dan tindakan pencegahan yang perlu dilakukan di masa depan. Dengan melibatkan Gov-CSIRT, organisasi dapat memastikan bahwa langkah-langkah yang diambil sesuai dengan kebijakan dan prosedur yang berlaku di tingkat nasional. Dengan layanan koordinasi insiden yang

efektif, organisasi dapat memastikan bahwa semua pihak terlibat memiliki pemahaman yang sama tentang situasi yang dihadapi, mempercepat proses pemulihan, dan meminimalkan dampak dari insiden yang terjadi.

### 5.3. Diseminasi Informasi untuk Mencegah dan/atau Mengurangi Dampak dari Insiden Siber

Layanan diseminasi informasi dalam BPOLBF-CSIRT bertujuan untuk menyebarluaskan pengetahuan dan informasi yang relevan kepada pemangku kepentingan untuk mencegah dan mengurangi dampak dari insiden keamanan siber. Tim BPOLBF-CSIRT bertanggung jawab untuk mengumpulkan, menganalisis, dan menyajikan informasi terkini mengenai ancaman, kerentanan, dan praktik terbaik dalam keamanan siber. Layanan ini mencakup penyusunan buletin keamanan, laporan analisis ancaman, dan panduan mitigasi yang dapat diakses oleh seluruh anggota organisasi serta pihak terkait lainnya. Selain itu, BPOLBF-CSIRT juga mengadakan sesi pelatihan dan workshop untuk meningkatkan kesadaran dan pemahaman tentang keamanan siber di kalangan karyawan. Dengan diseminasi informasi yang efektif, organisasi dapat memastikan bahwa semua pihak memiliki pengetahuan yang diperlukan untuk mengenali potensi ancaman, mengambil tindakan pencegahan yang tepat, dan merespons insiden dengan cepat, sehingga meminimalkan dampak yang mungkin terjadi.

## 6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke bpolbfcsirt@gmail.com 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)