

# RFC 2350 BengkayangKab-CSIRT

## 1. Informasi Mengenai Dokumen

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

### 1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 26 Juni 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.bengkayangkab.go.id/rfc2350>

### 1.4. Keaslian Dokumen

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

### 1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 BengkayangKab-CSIRT

Versi : 1.0

Tanggal Publikasi : 26 Juni 2025

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 Bengkayang*

Disingkat : BengkayangKab-CSIRT

### 2.2. Alamat

Dinas Komunikasi dan Informatika Kabupaten Bengkayang

Jalan Guna Baru Trans Rangkang Kantor Bupati Satu Atap Lt.1

### 2.3. Zona Waktu

Jakarta (GMT+07:00)

### 2.4. Nomor Telepon

0896-8243-4819

## 2.5. Nomor Fax

Tidak ada

## 2.6. Telekomunikasi Lain

Tidak ada

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

[csirt@bengkayangkab.go.id](mailto:csirt@bengkayangkab.go.id)

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

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

```
xsDNBGhaQisBDAClhZT8ydp1G6onof5CQnTn7BivgfKBRDCfeCpGwPM2PLNnfjF/h/09Ohk
GAkSPRhMQC5camITMDEld58OMAnCLGeG3gYc0+PkhvcUD6ufbpc98TW0CFZF763cUAI
wvZWNDjW6PyW+LuXExqmrPugQ0c+NiClJvKtw65MiODqM6WpOBdqnUSKxFL2WoPgZ1
FKXXGeF9ksbCPozUoFY/iNyMSaGk4KuDIBO7UNAdV9P3RvaAtpapppm4R1+v2T4oXvvg
pbgKTpiagAMEYO1zGu7rKl6zooHp5eWXNGF+NFnB3CyKTbY1wZWO6UCanA434RQoVP
MpCLr21+wt+wwRNR1+KM6DLpxfLuPinZDgASHl7w4kqaNtcgyQ/6wwK5kJlxQKPi7J0p
9pctSDksndvUGpGQcwah73cBbcjsSiea21zJcFKyMchyvFLI2IMppfUxHvy4yrr1fG/hXPjjw6lf
ueRn0AEakk9af0ikKe8EeB0LGdB0l34MZh+l9TTEDEAEQEAAc0mYmVuZ2theWFuZyA8Y3
NpcnRAYmVuZ2theWFuZ2thYi5nby5pZD7CwQ0EEwEIAdcWIQRPfmwmt6Yn1+ZjeaJLH8
SSMywztAUCaFpCKwUJBaOagAlbAwQLCQgHBRUICQoLBRYCAwEAAAoJEEsfxJlzLDO0
elgL/10VPC3XLMWXED3WCDBI73FuB0DgEQfFne4uZfM6+SaOJ3dmH/KhyPA2dkJi3e6a1
IgXkNU6oODF5cuyDKQZ/1/Lf3fg/QXNJZzH8sQC6ugzblgWwPGeJdd1tWWtXL2xRZ7g+Xf
US90qzuiqYdzyDljlkGT/DudNpw67N3Zzsk/q83Xfd6PahCDiAnCAoPyF42olp3NjY2srGXJ5kf
bxBEDFq9F6vN1gvfgNWSiXf41CCYT/asgt6EVQ7ZcUQzfjNf/3EeVJxNYKF5sJco4I8JKzIO
mnXI0X+OKzP2e3/DwcbFcP3r+zK140dZuM/MWPbQ12tV0PVgr5Dvm1XaceaD41lg9G
k8o52KeMm+Gg+FyZexOqP+aPJ2ZDQKTyfFu+JN+d6e3QQpTxBsfQsiTfDTXvvoU4LYOb
B1v0VTEfLnxVFtqDv4OZPN1d0By+q6Xha6tvMLC/SREG1aTi2ZI4E8tKIVMArt1gudRK3BrQ
tITG7SS6vaObsrgaIPMdgs7AzQRoWklsAQwAw+/WAo5bHPW+6tRWLUarX05IZt+e2pExL1
IRMjmnnPNqgouYgM3+wdHH2sUUkCxJlxPd5p/d8gYRyAnnOayWzMBNDnrZ3c0bzDe1kcd
78sE96f9WgLUaNcJbLKRzcxqwS0ZyGN8d0lZVjs/Hlb2yujxCr9VdpOph1Q8eFxgW7WZt2S
tm11hRiTubp+PCt3iaRDXJgMC2G++1Wy7mrjAoSiqv9twlsyYXKQ5297ziq8BMK6FEOtoZL
k6TBBZFnSYuslGAbVkCKMHfcQ3S7aB6lQ77NBOfdfXncvL0IBG7GVgfqf/ts63QiNgGkQt
PcaRfQ39JRyfascXf1eBhhC1UvHILsJaq+ak1l9cYxsumDO9Vzg75VwaxCiA0spqvmyzUWl
wZ84yHIFUkIrO/d0dtpQq0xYbEs3LtzQzVHL5ef83P1PMvf8rta0o1uub9Ux0d997joJS4JRYdD
qxqkXBeEsmQcx3xi1NqKrM4BpPBfhE2F4+DHYHNTseuR6euYVABEAAHCwPwEGAEIA
CYWIQRPfmwmt6Yn1+ZjeaJLH8SSMywztAUCaFpCLQUJBaOagAlbDAAKCRBLH8SSMyw
zthYWC/9onSqa39vcnE2s1e9he8oSpgSOguho4O7bnbLAK3d0p0xX3aAhBGCUCUtzpl9
wLHG45teNFSCoWo/rQY7w0KII2j/gf6Z3tk9ZpBFIsW23fRz+8EcF+Zw1FCsuCyaaxFkI6Q
dxdsM2LkVYDWa26SOI78LfRc6R1XcFNegEdXYp+cGXbZ3TtualH2FKgHMBEvXz4tOVL8
diexhg1LmykhyCBRm0qpK19G/2wNKX5bBtpotozz5vfzY3fAxClqEN+pTAKhYmTd1X/yujA3
eUwJgr9ULzdzRqAQencx1Q44tC7rzFdvuPfW88HNp9s177nCwlZHULHgVVadHaVXqUtyzV
cVzqjLCBg61dHPfs8unW+IIncZB9nJfrbjPGTEuxAEE5+xRSqfWjPy8AOZfdDJ296cMKR461
bgFpAWSDMGfAnIPLbnk/sOOyhx4oHEMTydwK1kwWB9KE1YpLnKAtqSTE5gxBr+hbmy6J
e7eSOjJ+IR0Q/XqXxafdMoZk0=
=EEKy
```

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

File PGP key ini tersedia pada :

<https://csirt.bengkayangkab.go.id/storage/Publickey.asc>

## **2.9. Anggota Tim**

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

## **2.10. Informasi/Data lain**

Tidak ada.

## **2.11. Catatan-catatan pada Kontak BengkayangKab-CSIRT**

Metode yang disarankan untuk menghubungi BengkayangKab-CSIRT adalah melalui *e-mail* pada alamat [csirt@bengkayangkab.go.id](mailto:csirt@bengkayangkab.go.id) atau melalui nomor telepon 0896-8243-4819 pada hari kerja jam 07.30 - 15.30 (Senin-Kamis) dan 07.30 - 14.30 (Jumat).

# **3. Mengenai BengkayangKab-CSIRT**

## **3.1. Visi**

Visi BengkayangKab-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 Bengkayang.

## **3.2. Misi**

Misi dari **BengkayangKab-CSIRT**, yaitu :

- a. Membangun pusat pencatatan, pelaporan, penanggulangan dan pemulihan insiden siber di lingkungan Pemerintah Kabupaten Bengkayang;
- b. Menyelenggarakan penanggulangan dan pemulihan insiden siber melalui kegiatan mendekripsi, 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 Bengkayang; dan
- e. Meningkatkan kesadaran pentingnya keamanan informasi bagi sumber daya manusia di lingkungan Pemerintah Kabupaten Bengkayang.

## **3.3. Konstituen**

Konstituen BengkayangKab-CSIRT meliputi Perangkat Daerah penyelenggara sistem elektronik di lingkungan Pemerintah Kabupaten Bengkayang.

## **3.4. Sponsorship dan/atau Afiliasi**

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

### **3.5. Otoritas**

BengkayangKab-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber di lingkungan Pemerintah Kabupaten Bengkayang.

BengkayangKab-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**

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

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

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

### **4.3. Komunikasi dan Autentikasi**

Untuk komunikasi biasa, BengkayangKab-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 BengkayangKab-CSIRT yaitu :

#### **5.1.1. Penanggulangan Dan Pemulihan Insiden Siber**

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

- a. deteksi insiden: mendekripsi 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 BengkayangKab-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. pemilihan (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 BengkayangKab-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 kerawannya 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. BengkayangKab-CSIRT memberikan informasi kepada penyelenggara sistem elektronik terkait layanan ini.

**5.2.2.4. Pendekripsi Serangan**

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

**5.2.2.5. Analisis Risiko Keamanan Siber**

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

**5.2.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber**

Layanan ini diberikan BengkayangKab-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**

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

**6. Pelaporan Insiden**

Laporan insiden keamanan siber dapat dikirimkan ke [csirt@bengkayangkab.go.id](mailto:csirt@bengkayangkab.go.id) dengan melampirkan sekurang-kurangnya:

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

## **7. *Disclaimer***

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