

# RFC 2350 Ciamiskab-CSIRT

## 1. Informasi Mengenai Dokumen

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

### 1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 04 Maret 2024.

### 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 :

<http://csirt.ciamiskab.go.id/rfc2350.pdf> (versi Bahasa Indonesia)

### 1.4. Keaslian Dokumen

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

### 1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

|                   |  |
|-------------------|--|
| Judul             | : RFC 2350 Ciamiskab-CSIRT;                                |
| Versi             | : 1.0;   |
| Tanggal Publikasi | : 13 Maret 2024;   |
| Kedaluwarsa       | : Dokumen ini valid hingga dokumen terbaru dipublikasikan. |

## 2. Informasi Data/Kontak

### 2.1. Nama Tim

Computer Security Incident Response Team (CSIRT) Kabupaten Ciamis  
Disingkat : Ciamiskab-CSIRT.

### 2.2. Alamat

Jl. Jend. Sudirman No.220 46215 Sindangrasa Jawa Barat

### 2.3. Zona Waktu

Ciamis (GMT+07:00 atau sesuai Kota dimana CSIRT berada)

#### 2.4. Nomor Telepon

(0265) 773000

#### 2.5. Nomor Fax

(0265) 774257

#### 2.6. Telekomunikasi Lain

-

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

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

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

Bits : 4096

ID : ciamiskab-csirt <csirt[at]ciamiskab.go.id>

Key Fingerprint : 52D163D3F68C3556D6F07683EA6329D7BE8C5333

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

```
mQINBGXb8u8BEADWJnCrzSbTJmhj35WiQD9F/JkdnuQEbnGwe3+9XYbN6GL5tp
Wa
QluqpKxuf8fg76ySMPth/VXChGXAfk/3Gik56bvKSCuWo3ZBlqtfAD1zEL93qpRm
sZE1qcBuX+mZcPpwb6/D0Z5Yw6RbqXeyjy1piPMrqU7xKbMXZPTdCekhRGQ8I57z
0hXAbyYI+gn9SXXRuflyjvaZe6HNUAZt+T0+TZ8hEpYPC3eL+dSoF/3k1WbujobW
tt7L/11JnY92/oLv8XzGFRKogZuQSsSSgw6R2sCMiBX1VMN2PtphQ03liac5+XaU
qe0axybflmBFbd+tnLTJcWDchJ8Q+pl3bVFBpG8F3cBUSH84kLirx6QkXmU9P6Nk
7rPMdskW09v/90IGPTSogq17kLsJxTMjlf9UzTtCVezWa2GgYrp7ZUM72+HVFgru
90pbor+Mz+LR0SF5Dbj6FcfI/t28wslUVGeJuW2oP+VCvje6wn8h0EqSbaPd3VpD
ojgvLWoiOGIRujJsMDoLrdV7jxZVgmXi0ylej2L75AZ3UkKone9nTb8Rd12yXVQ9
Eo3LGCqG8YHrfzcL9w8tJuPo6ifGSnYf9vIO2ZPwwgcX0ntD/cj8uHJRXCzimpvK
CPi2QsOPyGb8NQa/9wxMF6hlhFrpqLhUdecUgDN9+n0ttec0YFhHCKwNgwARAQA
B
tCdjaWFtaXNrYWIY3NpcnQgPGNzaXJ0QGNpYW1pc2thYi5nby5pZD6JAlcEEwEI
AEEWIQRS0WPT9ow1VtbwdoPqYynXvoxTMwUCZdvy7wblwUJBaUT4QULCQgH
Agli
AgYVCgkICwIEFgIDAQIeBwIXgAAKCRDqYynXvoxTM9InD/9C1b4lyzPqhRhIZO53
QYj9OON2Fv5cnmiA3TdWhyDdjKJqCNUvil1+C6w0uxRtS0y9DfNII7AX49mklebL
LyYvnQyCy4401hVmFq6j86FpfJaRKcp3NJqqd7brNCKgw3OPMRCKhSulK5uFtXAg
89ZMlrF7udCRzDJvIHxxKm0yOGvoN00VTFIdRrQnHS3FzKsDG0YGLDjiYgLwlgXw
YZOFV46li9GYBLRZST3jiuZqinQJ18J4MjC9Bzz0jYQSCm4aGsOz+QxtqHwbtXGu
kT91FIT7HeFpi8BubMQzat2M4Hsof/juOeU6AOHyEUE9Ni+785+GPUI8oiDahzHA
```

XwMTtoDCmMiqLw6OpErL7K29Fh2fbCmYY/g49xSoZ4XhSiX40oFB2Z3NFTXPua/N  
E  
H+KGezuNrGTEI3ggwJnDt3U1Leqvm1ozXTgZVgA+G5mV5HZF38QswJe0e/f359g4  
lhkj27QgCgCS2uL6VjJ7jm9XVO/wtI3BBALCpfr0gMX9nedXgTgIXmvDt3+vxvHB  
GYXdrFHM6cH3r/G+XqAmmd4+J2WGxrD9MpLLqMyhsajSVnPPMTD63bOnatAhO  
p2  
K75ZGwmHyeRQsJ9IKSLNIh6waOqra75NK0oYxq2LNgUwfxoZn1XBWEQENcbg2si  
D  
PkIt5/xZN1+J2ntkUb0CGBi6RLkCDQRI2/LvARAA6te7F3Fa+oSbaOUhXUUz3Qae  
md6Mle6IUdhCk05NEP6V5ggvDoyWHN8WfwkSPKVt59Mx9H6phAyZvf2/h/l7nnjv  
hJw58OxuvtSKUY0R0QWuqzNLAMBsdjBSKaUVSYywl3XFxJJ+mw3+IRVH8LDt8Ne  
x  
0IEMDtQz0UF8ts2/PXxII1MNIUZIjM70fkCaTnj1u65acJULpnOV7iCAi5sGpyKS  
vAVZ9pYa9jHgVQbYp+oH6ZxA0mtfcDBQqyVXqplH7IssolruSjS3Yyq5gA0jZ31t  
epgNW6zuOHFS23C47xmbcs5atiTPMKBQ18fMSkeLaLlpYxGAJT2vHGJTYRxaL3M  
E  
te2KCVd5UbexRc09VdGj6taStdHR1axeB/KbOz+iJtCvO9Uk/wPEqVcjl51ikFa  
9dpadB3aMoE2G0hA/Mztg4P9S/n016KSqYgq2BRs3pwh3S+S7iMhoiXMCmuNZa+d  
OafZY6wk+9HfqdCtUBlxEeMp7gEuj8YAD/7IPvYFZNVNuBSp71PUZCTkKGzoUy/A  
UWk0ZCe6B2LqLa9v8bSd6rUsUKUTb8n35J4AU5q9vgHBr1y+/5qXRCgYyG1uzHJf  
IAc8jdfR5ir1Ujqc8kMVjTxESDqtzXalax0kAtlogZFO4LMydOI9O+8loWI7p3  
ZSxGFzhUKSmeeEOFZBkAEQEAAyKCPAQYAQgAJhYhBFLRY9P2jDVW1vB2g+pj  
Kde+  
jFMzBQJI2/LvAhsMBQkFpRPhAAoJEOpjKde+jFMzyRkQAIJhWnfBx1kxU8+9zMIL  
JuTcS5MwgL0UDjp07Vor+maYux5LH/nVqgClbz0pT09lz+rzA2V4GLL/TxODgyT7  
+Nsmxk0akxeUUtd04+GoOxNA7R51JBqy0r60WKWPnphyqfvk3H1jhZflBhHFHPrM  
aDwRuqfEEtJoVNqa3k9xCwikGUUe/y7uGQRhu4B4OwY2LjXzXvy+8pvqxMRilk6j  
s7Ech8nVlzNyEUxXolieafY0xDY4etLF+RRsk5ztz2y7ay9aSvMbteltiBANZRy  
5k2oqOw/th+5CW2OytPpe93cqq3nxCXBQBaab/ZkRdVJyBHFfaE6HyeH+frnAnrM  
S1JtApyB1+qQx1dja2aKMkk3V4WYextz+KGCdDMffhpaBaXnx7WWs8VCW7x/N8O  
S  
LOziCF0yskh7F53u+9uMImz2kSnjQIF4k4L/UBa+zTUZSjEEZutBrSMz3zBGp4av  
feM1dthDSjh53OYKM2FIU6j8poBIMnpvSrzhODrTIB9KCQn3fF6MWUmpuRn35YeC  
nA092yBpXv+NhaP+BnpizCRu8SVZvDM9cKQMuLV89SpAhr2V5EKWJ1W1872IAB  
W6  
+VP7v53q/pzfYylv1I8xxoBQYtRBw1RcyOTOxOaijVEZShGV7Eu8Fpwd9+8kCM7x  
m9yCXy+BilQDtoKiSjObGmCK  
=2Q4u  
-----END PGP PUBLIC KEY BLOCK-----

File PGP key ini tersedia pada :  
<https://csirt.ciamiskab.go.id/RFC2350/publickey.asc>

## **2.9. Anggota Tim**

Ketua Ciamiskab-CSIRT adalah Kepala Dinas Komunikasi dan Informatika Kabupaten Ciamis. Yang termasuk anggota tim adalah seluruh staf Dinas Komunikasi dan Informatika Kabupaten Ciamis.

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

Tidak ada

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

Metode yang disarankan untuk menghubungi Ciamiskab-CSIRT adalah melalui *e-mail* pada alamat [csirt@ciamiskab.go.id](mailto:csirt@ciamiskab.go.id) atau melalui nomor telepon (0265) 773000/774257 pada hari kerja jam 07.30 – 15.30 atau siaga selama 24/7.

## **3. Mengenai Gov-CSIRT**

### **3.1. Visi**

Visi Ciamiskab-CSIRT adalah terwujudnya ketahanan siber dan layanan keamanan yang responsif dan profesional pada pemerintah Kabupaten Ciamis

### **3.2. Misi**

Misi dari Ciamiskab-CSIRT, yaitu :

- a. Membangun, mengkoordinasikan, mengkolaborasikan system mitigasi, penanggulangan dan pemulihan terhadap insiden keamanan siber dilingkungan Pemerintah Kabupaten Ciamis.
- b. Membangun sumber daya keamanan siber di lingkungan Pemerintah Kabupaten Ciamis.
- c. Membangun kerja sama dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber.

### **3.3. Konstituen**

Ciamiskab-CSIRT memiliki : Konstituen yaitu pengguna TIK di lingkungan Perintah Daerah Kabupaten Ciamis.

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

Pendanaan Ciamiskab-CSIRT bersumber dari Anggaran Pendapatan dan Belanja Daerah Kabupaten Ciamis.

### **3.5. Otoritas**

Ciamiskab-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada Pemerintah Kabupaten Ciamis. Ciamiskab-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya

## **4. Kebijakan – Kebijakan**

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

Ciamiskab-CSIRT menangani insiden yaitu:

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

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

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

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

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

Untuk komunikasi biasa Ciamiskab-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 Ciamiskab-CSIRT yaitu :

#### **5.1.1. Pemberian Peringatan Terkait Keamanan Siber**

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

#### **5.1.2. Penanganan Insiden Siber**

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

### **5.2. Layanan Tambahan**

Layanan tambahan dari Ciamiskab-CSIRT yaitu :

#### **5.2.1. Penanganan Kerawanan Sistem Elektronik**

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

#### **5.2.3. Audit dan Penilaian Keamanan**

Layanan ini diberikan oleh Ciamiskab-CSIRT berupa audit dan penilaian keamanan sistem elektronik

#### **5.2.4. Analisis Resiko**

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

#### **5.2.5. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber**

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

## **6. Pelaporan Insiden**

Laporan insiden keamanan siber dapat dikirimkan ke [csirt\[at\]ciamiskab.go.id](mailto:csirt[at]ciamiskab.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**

Terkait penanganan jenis malware tergantung dari ketersediaan tools yang dimiliki.