

## **RFC 2350 CSIRT Kemhan**

### **1. Informasi Mengenai Dokumen**

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

#### **1.1. Tanggal Update Terakhir**

Dokumen merupakan dokumen versi 2.0 yang diterbitkan pada tanggal 23 September 2024.

#### **1.2. Daftar Distribusi untuk Pemberitahuan**

Satuan Kerja di lingkungan Kemhan

#### **1.3. Lokasi dimana Dokumen ini bisa didapat**

Versi terbaru dari dokumen ini tersedia pada :  
<https://csirt.kemhan.go.id/assets/rfc2350/rfc2350-id.pdf>

#### **1.4. Keaslian Dokumen**

Dokumen telah ditanda tangani dengan PGP Key milik Pusat Pertahanan Siber (Pushansiber) – Badan Instalasi Strategis Pertahanan Kementerian Pertahanan (Bainstrahan Kemhan). Untuk lebih jelas dapat dilihat pada Subbab 2.8.

#### **1.5 Identifikasi Dokumen**

Kedua dokumen (versi bahasa inggris dan bahasa Indonesia) memiliki atribut yang sama, yaitu :

|                   |                                                           |
|-------------------|-----------------------------------------------------------|
| Judul             | : RFC 2350 CSIRT Kemhan                                   |
| Versi             | : 2.0                                                     |
| Tanggal Publikasi | : 23 September 2024                                       |
| Kedaluwarsa       | : Dokumen ini valid hingga dokumen terbaru dipublikasikan |

### **2. Informasi Data/Kontak**

#### **2.1. Nama Tim**

*Computer Security Incident Response Team* Kementerian Pertahanan  
(CSIRT Kemhan)  
Disingkat : CSIRT Kemhan

## 2.2. Alamat

Pusat Pertahanan Siber  
Gedung Sutan Sjahrir  
Jl. Pondok Labu Raya RT.6 RW.6, Pondok Labu, Kec. Cilandak, Jakarta Selatan, DKI Jakarta 12450  
Indonesia

## 2.3. Zona Waktu

Jakarta (GMT+07:00)

## 2.4. Nomor Telepon

Telepon (021) 29770001

## 2.5. Nomor Fax

Tidak Ada

## 2.6. Telekomunikasi Lain

Tidak Ada

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

csirt[at]kemhan.go.id

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

Bits : 4096  
ID : 0xAD591C54  
Key Fingerprint : 2401 5DDC 0B28 04F5 837C DED7 CEB2 DC94 AD59 1C54

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

```
mQINBGDIGZABEAC8qIID7LKwLksxs5DrmlWovnRwrutMVBNDetjos+RiVP8tZfZ3
Whm5K0y16sCHOKxTC90J9Lva0fWP7G88PT06f5s1UNYUZZ5YmjqqnY7MHi/cmpmp
/olsasQr1AySmF1Ow1ZQqMZMbe+NgWvFwg1SisZA6g1XI27NWKqm+V9nU5b4mUHR
efaaAfwLpHGh1zv6yNwbB4bd/75Cv5WQnliyzES903S8QFraaQYcQC6nJlW6ix8U
Ja2+BxptzFjU2Wery1E0bfcezxi4JlX0P0D730obKhXtvP6JQM4hNT0VdQQPeKlj
yWx5sIfWcg351b751Ath1pvGoIqayUM9zjE9N4JG8qmWEWYvcevCyws2ibN/3nv
O34a0vKnoZBgHMMprWRqZQvD6zE8X/kNlnmMhWb0GhY6P6d+t2F4bYXTjGWujvkz
GxFg8a2Tlq0V79yKgJnSBU2MRGvZShWWknjoN2nvrddkpgSZKsGyb2TrliksaJjzg
mlz17mbo+sHYxJp+ZtXD0TBb24nv7L41Jdyg5V1RCraDlc2b0XONZL1wNZyxUoRq
uFLT8tTvNlxcqHKyrxH9yRdUWPk6dHcGcIQm1DL4YGsUwd/3s0uXl/5+lr/rygzA
HqQTWtWMDvIn//E9/aMOILKQOMe9buHljQ9t9DGPULsFi0dyV9dqAftWZQARAQAB
tCFDU01SVC1LZW1oYW4gPGNzaXJ0QGt1bWhhbi5nby5pZD6JAlQEWEIAD4WIQQk
AV3cCygeY9N83tfOstyUrVkcVAUCYMgZkAIbAwUJB4YfgAULCQgHAgYVCgkICwIE
FgIDAQIEAQIXgAAKCRDOstyUrVkcVKUrD/4zmBQAb5KUjmPmWMP1x2Nne7NBQhFb
85dEqmMyZuiIiWka7TRbegg2tpOlqGDYHgY9ZfaRyE6l1dLTnVeuQUY33NY+gmAV
oVh+E4tTqBx1Zcq8B0HDv1YZpHWQieVC6vHEfA19JzG6Y+wS8KuX+4ZJwwIQ2vEL
aUKy8Zdh+BWQXwViOX7qrfW08IXMaGsyUSRSCcBpAEMqWYgr1L4PUHYv06tn0RL7
naPHYbOiRjtEk310trdSW4IAeYftrWEV16sGETxQD/MxTLWreCgfdNIGFsptCu57
91n15eQm0eSJeavv72jmmFmDR1Ogf7gb2Lyr8z+aW6fGzaDtJ3CBoKSAtMDhZYqP
wxmJ4fLZtGpkFwE+51mJnJsXfYTi00M7czvNo8b1sTi26vj4Eui85H6FQVeXEdtg
yslw/40jImF1HUcuoMqwUQ7TYVb1YDEHh1wU2e6+4J8RIE20rCF+FSCKdBbLnQv
Ol8GNddnMPOJL5Z1JNZ5kJUF9NsLUB4lpbQi9dwcpIEauD+yKqY+ajjCy4uzpNrJ
```

```
kVtcxR5gQa2oKCAj3utok2BkzKTtmM75oLWCdCfWF9HNzXPUBUrUg1kw4DbNnCVF
MmKjWE8Lvmm9iAYlHmdbxFeSYjKB6Z+t+i/BDhU6jgfs0gzxLb8azx0sPSls68Ce
jv6SSoRD6dTEA7kCDQRgyBmQARAAXrEuB3IXKYwt6FbhHSac8KjOgqpCtjZ21it
XrJlGezb8oa068ItYEsV/QvmOhg0Gi/XzAQrYxkKqaX/o0ZPp0ImeuPzUh6fEkat
xikP35VXN1777Z6PacnEfZp7WzzyFFvuzqR7w6Hs0iaABNLAX7LphX3Sp012mJjV
MBd6lthY7N/HJQI7tnazeYNlPidnxFCf7UryQ7GuYPYcRZkVve2F6SJLuhRXadJX
18Kg+auZvOXY+a6LlQauefqQ0j8BAJuSpXRRt+hyst9BdcXnbtsCyIH5bxfbj1+Y
ZXaoQUcMh1LQi6WwWL1NR7Qsmyp4Wb9B7bTXDbNEphHxA9Vh7OX7P72r0ZyPvIRu
hqc0SMnqIrrVG7aWqH3DSfeN06ZuzTG6vuBTQ4K0BZrcmpqTyjEMN5hwbV+OhYu7
YMFQWKkbFGSKxs88Tg6BB1RckGdzTRdBrcVJvNv9W5zPVOPw0KY42ETzkxvbfS23
yzuJ2hUa2SPmg5QZZQpqbHSIPZ4mXZh+DYqaPw8ShDnC/AVFpZSv1vtC1xo9qrMp
v7MG52id+NXjOLUw+NOvQ1ZgyEY3a+/A9Tbwf+PAypbRjD8W3bABluUZhIBM2k08
qSEWNJebVpJIeDQ/kO7K9YBU5b1Zh3gFcl1iyHdEC4ChLAXExiI3nw6fOEAlEWxl
EdM3RI8AEQEAAYkCPAQYAQgAJhYhBCQBxdlKAT1g3ze186y3JStWRxUBQJgyBmQ
AhsMBQkHhh+AAAoJEM6y3JStWRxU1gcP/3Q1t1HwP9PXT0VjB4f4qHnpbSCkP9Ae
HodiQFg5nqMdWwT8+PXyVubLf8cwq833uNvrdBfftWgDrj9u5Y+VGG12OQ8NlwpC
eGbnjtOeoMAQ+caitwQ2XuoyUe4nYiDhIMjiKmpNoDN12IS6VRRLZE/oDDt/A3NL
5A8/c0/n1Alf48nRoanLAuy7FoeeedlAuxdEHhpsx7FNggjgB6Atf+bysFT9EPWa1
iknEnyqoH1k3DhoeQPIZ7xOfzOfVefIPLK04/uB4sM5UoH6bSusn96Uzsm++8GB1
3X99SRXU18Hr/BveWk8dNHE+d5dtsvO5xJ04v8o02M88Mj8lvQWD96PF4Sk+yZDH
OEvnfnA902m9Xzvv9JDLJ0ssPMES51avMFAoBjYbp9GWn6czNjeAP9KnuVdz7YjK
itThXQWvc52qHI7IR37/diznAN0BhXibM0j2d7TTSguqg/Sru6YyEp2f6RHW73VX
vWu0TXb615qf6G1891t0W/6HLXkxEji+wrKfk+43rX1pfPWeObLr3btVxeLWNIZp
uoLuMhUxE+mEbgH+Vsv62UKQdevWCnNDsPK8yv043XGFOfdDCBGL7zUWesxeBbUr
iXwj8Dh86qSOspZn9+kTft2tn2SeU8Hiy0kJaY+T8w9X3Wu22KNR5LLRU6SLshwc
7+Tl1ely94G9
=m6ZZ
-----END PGP PUBLIC KEY BLOCK-----
```

File PGP key ini tersedia pada :

[https://csirt.kemhan.go.id/assets/CSIRT-Kemhan\\_0xAD591C54\\_public.asc](https://csirt.kemhan.go.id/assets/CSIRT-Kemhan_0xAD591C54_public.asc)

## 2.9. Anggota Tim

Ketua CSIRT Kemhan dijabat oleh Kepala Pusat Pertahanan Siber Badan Instalasi Strategis Pertahanan Kementerian Pertahanan. Yang termasuk anggota tim adalah seluruh anggota Pushansiber Bainstrahan Kemhan dan Bag Datin Satker U.O. Kemhan

## 2.10. Informasi/Data lain

Tidak ada.

## 2.11. Catatan-catatan pada Kontak CSIRT Kemhan Indonesia

Metode yang disarankan untuk menghubungi CSIRT Kemhan Indonesia adalah melalui *e-mail* pada alamat [csirt\[at\]kemhan.go.id](mailto:csirt[at]kemhan.go.id) atau melalui nomor telepon (021) 29770001 ke Pushansiber yang siaga selama 24/7.

## 3. Mengenai CSIRT Kemhan

### 3.1. Visi

Terwujudnya pengelolaan sistem keamanan informasi dengan baik dan aman di Lingkungan Kementerian Pertahanan untuk melindungi aset informasi yang dimiliki oleh Kementerian Pertahanan.

### **3.2. Misi**

Tujuan dari CSIRT Kemhan, yaitu :

- a. Membangun pertahanan negara yang mampu menjaga kedaulatan di ruang siber, dengan mengamankan sumber daya infrastruktur kritis pertahanan. membangun tata kelola sistem informasi pertahanan yang baik.
- b. Membangun koordinasi, kerjasama dan kolaborasi dengan pihak terkait dan negara lain untuk membangun pertahanan siber yang Tangguh.
- c. Menyediakan dan mengoptimalkan sumber daya pertahanan siber melalui proses pembelajaran dan peningkatan kualitas yang berkelanjutan

### **3.3. Konstituen**

- a. Konstituen CSIRT Kemhan meliputi pengguna sistem elektronik di lingkungan Kementerian Pertahanan
- b. Seluruh konstituen CSIRT Kemhan melaksanakan rekomendasi dan/atau imbauan yang dikeluarkan oleh Kepala Pushansiber Bainsrahan Kemhan berkaitan dengan keamanan siber di lingkungan satkernya masing-masing

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

CSIRT Kemhan merupakan bagian dari Pushansiber Bainsrahan Kemhan sehingga seluruh pendanaan untuk penyelenggaraan bersumber dari :

- a. Anggaran Pendapatan dan Belanja Negara; dan
- b. Sumber pendanaan lain yang sah dan tidak mengikat menurut ketentuan peraturan perundang-undangan.

### **3.5. Otoritas**

Berdasarkan Peraturan Kepala Badan Instalasi Strategis Pertahanan Nomor: Tahun 2021 tentang Pedoman Penyelenggaraan Layanan Tanggap Insiden Siber di Lingkungan Kementerian Pertahanan, CSIRT Kemhan adalah tim yang bertugas memberikan layanan tanggap insiden siber berupa layanan reaktif, layanan proaktif dan layanan manajemen kualitas keamanan di lingkungan Kementerian Pertahanan.

## **4. Kebijakan – Kebijakan**

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

CSIRT Kemhan melayani penanganan insiden siber dengan jenis berikut :

- a. *Malware*;
- b. *Web Defacement*;
- c. *DDOS*;
- d. *Phising*;

e. *Advanced Persistent Threats (APT)*

Dukungan yang diberikan oleh CSIRT Kemhan kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden

#### **4.2. Kerja sama**

- a. Kerja sama antar Instansi dapat dilaksanakan dengan tujuan untuk saling berbagi sumber daya pengetahuan, keterampilan dan informasi mengenai keamanan Siber.
- b. Kerja sama antar instansi dilakukan dengan tetap memperhatikan kebijakan, sistem prosedur dan perlindungan kepentingan Kementerian Pertahanan

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

Untuk komunikasi biasa CSIRT Kemhan Indonesia 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**

Layanan tanggap insiden siber dari CSIRT Kemhan berupa :

- a. Layanan Reaktif adalah layanan yang terkait dengan kebutuhan melakukan respons terhadap insiden siber termasuk penangkalan, penindakan dan pemulihan siber, meliputi tugas peringatan, penanganan insiden, kerentanan, artefak, dukungan teknis, koordinasi dan respons, analisis kerentanan dan layanan interaksi (*help desk*).
- b. Layanan Proaktif adalah layanan yang mendeteksi dan mencegah serangan siber sebelum ada dampak nyata, meliputi tugas pengumuman, pengawasan teknologi, uji kesesuaian, konfigurasi perangkat dan infrastruktur, layanan deteksi ancaman dan diseminasi informasi.
- c. Layanan Manajemen Kualitas Keamanan adalah layanan yang mendukung kegiatan reaktif dan proaktif, meliputi tugas kebijakan dan pelatihan analisis risiko, perencanaan pemulihan bencana, kelangsungan kegiatan, konsultasi keamanan, peningkatan kewaspadaan, sertifikasi/evaluasi produk, pengelolaan infrastruktur CSIRT dan layanan penyediaan kompetensi khusus dalam rangka kegiatan proaktif dan reaktif.

### **6. Pelaporan Insiden**

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

Tidak ada