RFC 2350 CSIRT-Kemhan

1. Document Information

This document contains a description of CSIRT-Kemhan in according to RFC 2350. It provides basic information about CSIRT-Kemhan, its channels of communication and its roles and responsibilities.

1.1. Date of Last Update

The Current version is 2.1 and published on March 10, 2025.

1.2. Daftar Distribusi untuk Pemberitahuan

Unit organizations in Ministry of Defence Republic of Indonesia

1.3. Locations where this document can be found

The latest version of this document available at :
https://csirt.kemhan.go.id/assets/rfc2350/rfc2350-en.pdf

1.4. Document Authenticity

Both documents (English and Indonesian version) have been signed with PGP key owned by Pusat Pertahanan Siber (Pushansiber) – Badan Instalasi Strategis Pertahanan Kementerian Pertahanan (Bainstrahan Kemhan). See section 2.8 for more details.

1.5 Document Identification

Both documents (English and Indonesian version) share same atributes :

Title	: RFC 2350 CSIRT-Kemhan
Version	: 2.1
Publications date	: March 10, 2025
Expirations date	: This document is valid until superseded by a later version

2. Contact Information

2.1. Teams Name

Computer Security Incident Response Team Kementerian Pertahanan (CSIRT-Kemhan)
abbreviated : CSIRT-Kemhan

2.2. Address

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. Time zone

Jakarta (GMT+07:00)

2.4. Phone Number

Phone (021) 29770001

2.5. Fax Number

N/A

2.6. Other Telecommunication

N/A

2.7. e-Mail Address

csirt[at]kemhan.go.id

2.8. Public Keys and Encryption Informations

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

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

mQINBGDIGZABEAC8qIID7LKwLksxs5Drm1WovnRwrutMVBNdEtjos+RiVP8tZfZ3
Whm5K0y16sCHOKxTC90J9Lva0fWP7G88PT06f5s1UNYUZZ5YmjqqnY7MHi/cpmpP
/olsasQr1AySmF1Ow1ZQqMZMbe+NgWvFwg1SisZA6g1XI27NWKqm+V9nU5b4mUHR
efaaAfwLpHGh1zv6yNwbB4bd/75Cv5WQnliyzES9O3S8QFraaQYcQC6nJ1w6ix8U
Ja2+BxptzFjU2Wery1E0bfcezxi4JlX0P0D730obKhXtvP6JQM4hNT0VdQQPeKlj
yWx5sIfWcg351b751Ath1pvGoIqcayUM9zjE9N4JG8qmWEWYvcevCyws2ibN/3nv
O34a0vKnoZBgHMMprWRqZQvD6zE8X/kNlnmMhWb0GhY6P6d+t2F4bYXTjGWujvkz
GxFg8a2Tlq0V79yKgJnSBU2MRGvZShWWknjoN2nvrdkpGSZKsGyb2TrliksaJjzg
m1z17mbo+sHYxJp+ZtXD0TBb24nv7L4lJdyg5V1RCraDIc2b0XONZL1wNZyxUoRq
uFLT8tTvNlxcqHKyrxH9yRdUWPk6dHcGcIQm1DL4YGsUwd/3s0uXl/5+lr/rygzA
HqQTwTwMDvIn//E9/aMOILKQOMe9buHljQ9t9DGPULsFi0dyV9dqAfTWZQARAQAB
tCFDU0lSVC1LZW1oYW4gPGNzaXJ0QGtlbWhhbi5nby5pZD6JAk4EEwEIADgCGwMF
CwkIBwIGFQoJCAsCBBYCAwECHgECF4AWIQQkAV3cCygE9YN83tfOstyUrVkcVAUC
Z85PbwAKCRDOstyUrVkcVDWfD/4lvd41oa8QVD4++/O6EJjMxddYC2wBnEcb+Vib
rgqfji6UYu1M+7SyYiXPvlLi/8oZbtHp91WQtNmy74pNSAWb6RJ1OdK1gB9RT9EE
TwgYmW+u46/JRLz21pMQYHFyZU3DSHYVCKd+OPiuSJndQ6imjCn6F9rtHYKZa/0k
GQ4jG05ZwUIY5AeMoD9M/Opsk50CJjX8w+l++sMusE9nbgIxJqrMv7bXdcXzjYBm
K30VuPeC7BnctaSwKrjh93p3tTlhTIZS6SrWKQ9sjzw+L8tnnqw3f4+MFxG/YyTn
e+yrkpWSplOIUe1KyqtYzFbe8Js8gbDqDPubo01in13qibOaIvXZdygSZMtzfxyR
6Ecb3Fliaxhy3ba9Hns84d2l5RMaM+uXVA9HlEhnFqsLTz0JIgPP801a2WO4Uehx
oSI36deQDYeYY/llhzAu7zZdMTTaIHINf5CzVp/SkPIenhwyIPM+VbEur9tv1I+a
vmIYy1JiuMCERyFCuiefUHq0ZSG8ebtRWX7bkO7EGu26tK5hKEBZkfEjgqFA4vmh
FTOMcyLz/AZV6MVWGgMNQ8oVLRN/XHSGA8jLVJqZwT73DAXBlAsygiqgEZ9/c85g
BOIFt16mL1H/pfDn0fEcVF5Hzh4Gzxrvk6b4RGTHgGzP66FEDh5SadcGhQ3S0/2o
Y6AXPrkCDQRgyBmQARAAxYrEuB3IXKYwt6FbhHSac8KjOgqpCtjZZ1itXrJlGezb
8oaO68ItyEsv/QvmOhg0Gi/XzAQrYxkKqaX/o0ZPp0ImeuPzUh6fEkatxikP35VX
N1777Z6PAcnEfZp7WzzyFFvuzqR7w6Hs0iaABNLAX7LphX3Sp0l2mJjVMBd6lthY
7N/HJQI7tnazeYNlPIdnxFCf7UryQ7GuYPYcRZkVve2F6SJLuhRXadJX18Kg+auZ
vOXY+a6LlQauefqQ0j8BAJuSpXRRT+hysT9BdcXnbtsCyIH5bxfbJl+YZXaoQUcM
H1LQi6WwWL1NR7Qsmyp4Wb9B7bTXDbNEphHxA9Vh7OX7P72r0ZyPvIRuhqc0SMnq
IrqVG7aWqH3DSfeN06ZuzTG6vuBTQ4K0BZrcmpqTyjEMN5hwbV+OhYu7YMFQWKkb
FGSKxs88Tg6BBlRckGdzTRdBrcVJvNv9W5zPVOPw0KY42ETzkxvbfs23yzuJ2hUa
2SPmg5QZZQpqbHSIPZ4mXZh+DYqaPw8ShDnC/AVFpZSv1vtC1xo9qrMpV7MG52id
+NXjOLUw+NOvQ1ZgyEY3a+/A9Tbwf+PAypbRjD8W3bABluUZhIBM2k08qSEWNJeb
```

```
VpJIeDQ/kO7K9YBU5b1Zh3gFcl1iyHdEC4ChLAXExiI3nw6fOEA1eWxlEdM3RI8A
EQEAAYkCNgQYAQgAIAIbDBYhBCQBXdwLKAT1g3ze186y3JStWRxUBQJnzk+KAAoJ
EM6y3JStWRxUfi4QAJ7kqgXXEa0yM7tkG03WlIkrlkUsvsZTjvZS8tatXKDUL85c
Bi0bdIOq85dc9fprvkZD+9ApXt4gpG/WKIoVGJE/y21hFT7aMX242xo4azY/Tla8
l4mtmzO5C4KWTEpZsQdto16zSqydOUkmDtd0wy5MHE3vofPKXYPYSmiEinwWs0yu
rNyVlgGnyUDWz5jX98HM2DTnOu5QbojO5WHBtDJzqwCSHWDD+yhmedlyvaLY68cx
rD7nl8bjFRglfMt/GUlT7GQcLZcB9U7ANLSe07q1Nbu9zXFd/abfRSnhcfdT1WaE
eqG1Hy1hHxJS5vCDq0TnvaCNe7H4gVfQVdtNm1TLDdpxH+acu6QzO4EfGVxc+Shv
M03Oc4yHBEmYDbJK5oKBBPr8aUTFOLxDPWWdnvtW1AMe84NGwIg+7xulNHrkYs83
kEhNtuhBeU/nI4tkWwPzKjre1CUeCGv2Lyt3ixaf7gA4luVKZRl6wXXDUQQkrJDM
RAJUj5VdOR5fqAd9yJGT9b2h4oDuRT9TWHIZrzQ+L/iqVilDZbOMQerjcW+ITaLi
TMqbOZxZfGKK5U48WgJ+jn/ytjMQFG2nhZTdWqvleKShwVNa8AfycgcNtqNRcRAz
fo3fVxfVkZpaAmeiZ92QrlQAkee3wFt05tdwLcdAo59lrhHnpnqojgOwwCBW
=5ysC
-----END PGP PUBLIC KEY BLOCK-----
```


This PGP key available at :
https://csirt.kemhan.go.id/assets/CSIRT-Kemhan_0xAD591C54_public.asc

2.9. Team Members

Head of CSIRT-Kemhan is Kepala Pusat Pertahanan Siber Badan Instalasi Strategis Pertahanan Kementerian Pertahanan. The team members included all staff of Pushansiber Bainstrahan Kemhan and Bag Datin Satker U.O. Kemhan.

2.10. Other Information

N/A

2.11. Points of Customer Contact

The preferred method to contact CSIRT-Kemhan is to send *e-mail* to csirt[at]kemhan.go.id or call (021) 29770001 which is active 24/7.

3. About CSIRT-Kemhan

3.1. Vision

The realization of good and secure information security system management within the Ministry of Defense (Kemhan) to protect information assets owned by the Ministry of Defense.

3.2. Mission Statement

The missions of CSIRT-Kemhan Indonesia are:

a. Building a national defense capable of maintaining sovereignty in cyberspace, by securing critical defense infrastructure resources and establishing good defense information system governance.
b. Build coordination, cooperation and collaboration with related parties and other countries to build a resilient cyber defense.
c. Providing and optimizing cyber defense resources through a continuous learning and quality improvement processes.

3.3. Constituency

a. The constituents of the CSIRT Kemhan include users of electronic systems within the Ministry of Defense.
b. All constituents of CSIRT Kemhan implement the recommendations and/or appeals issued by the Head of Pushansiber Bainstrahan Kemhan related to cybersecurity in their respective work units

3.4. Sponsorship and/or Affiliation

CSIRT Kemhan is part of Pushansiber Bainstrahan Kemhan so that all funding for implementation is sourced from:

a. State Budget; and
b. Other legal and non-binding funding sources according to the provisions of laws and regulations

3.5. Authority

Based on the Regulation of the Head of the Defense Strategic Installation Agency Number: Year 2021 (Peraturan Kepala Badan Instalasi Strategis Pertahanan Nomor: Tahun 2021) concerning Guidelines for Implementing Cyber Incident Response Services within the Ministry of Defense, the Ministry of Defense CSIRT (CSIRT Kemhan) is a team tasked with providing cyber incident response services in the form of reactive services, proactive services and security quality management services within the Ministry of Defense.

4. Policies

4.1. Types of Incidents and Level of support

The Ministry of Defense CSIRT (CSIRT Kemhan) serves cyber incident handling of the following types:

a. Malware;
b. Web Defacement;
c. DDOS;
d. Phishing;
e. Advanced Persistent Threats (APT)

Support provided by the CSIRT Kemhan to constituents may vary depending on the type and impact of the incident.

4.2. Co-operations, Interactions, and Information Disclosure

a. Cooperation between Agencies can be carried out with the aim of sharing knowledge resources, skills and information regarding Cyber security.
b. Inter-agency cooperation is carried out while still paying attention to the policies, procedures system and protection of the interests of the Ministry of Defense

4.3. Communications and Authentications

For regular communications with CSIRT-Kemhan, please use e-mail without encryption and phone. However, for communications containing sesitive/restricted/confidential information, please use PGP encryption in e-mail.

5. Services

Cyber incident response services from the Ministry of Defense CSIRT (CSIRT Kemhan) are:

a. Reactive Services are services related to the need to respond to cyber incidents including deterrence, action and cyber recovery, including warning tasks, incident handling, vulnerabilities, artifacts, technical support, coordination and response, vulnerability analysis and interaction services (help desk).
b. Proactive Services are services that detect and prevent cyberattacks before there is any real impact, including announcement tasks, technology surveillance, conformance testing, device and infrastructure configuration, threat detection services and information dissemination.
c. Security Quality Management Services are services that support reactive and proactive activities, including policy tasks and risk analysis training, disaster recovery planning, continuity of activities, security consulting, vigilance enhancement, product certification/evaluation, CSIRT infrastructure management and specialized competency provision services in the context of proactive and reactive activities.

6. Reporting Incident

Cyber security incident report can be sent to csirt[at]kemhan.go.id by attaching :

a. Photos/scan of identity card
b. Evidence, such as : photos, screenshot or log file
c. Or in accordance with other applicable provisions

7. *Disclaimer*

N/A