

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 1.0 and published on February 01, 2021.

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 :

<http://103.252.21.85/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 attributes :

Title : RFC 2350 CSIRT-Kemhan

Version : 1.0

Publications date : February 03, 2021

Expirations date : This document is valid until superseded by a later version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
Gd. Sutan Sjahrir Jl. Pd Labu Raya RT.6 RW.6
Cilandak, Jakarta Selatan
Indonesia

2.3. Time zone

Jakarta (GMT+07:00)

2.4. Phone Number

Phone (021) 75918947

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-----

mQINBGDIGZABEAC8qIID7LkWLksxs5DrmlWovnrwrutMVBNDetjos+RiVP8tZfZ3
Whm5K0y16sCHOKxTC90J9Lva0fWP7G88PT06f5s1UNYUZZ5YmjqqnY7MHi/cmpP
/olsasQr1AySmFlOw1ZQqMZMbe+NgWvFwglSisZA6g1XI27NWKqm+V9nU5b4mUHR
efaaAfwLpHGh1zv6yNwbB4bd/75Cv5WQnliyES903S8QFraaQYcQC6nJ1w6ix8U
Ja2+BxptzFjU2Wery1E0bfcezzi4J1X0P0D730obKhXtvP6JQM4hNT0VdQQPeKlj
yWx5sIfWcg351b751Ath1pvGoIqcaYUM9zjE9N4JG8qmWEWYvcevCyws2ibN/3nv
O34a0vKnoZBgHMMprWRqzQvD6zE8X/kNlnmMhWb0GhY6P6d+t2F4bYXTjGWujvkz
GxFg8a2Tlq0V79yKgjnsBU2MRGvzShWWknjOn2nvrdrkpGSZKsGyb2TrliksaJjzq
mlz17mbo+sHYxJp+ZtXD0TBb24nv7L4lJdyg5V1RCraDIc2b0XONZL1wNZyxUoRq
uFLT8tTvN1xcqHKYrxH9yRdUWPK6dHcGcIQm1DL4YGsUwd/3s0uXl/5+lR/rygzA
HqQTWtWMDvIn//E9/aMOILKQOMe9buHljQ9t9DGPULsFi0dyV9dqAfTWZQARAQAB
tCFDU01SVC1LZw1oYW4gPGNzaXJ0QgTlbWhhbi5nby5pZD6JAlQEEwEiAD4WIQQk
AV3cCygE9YN83tfOstyUrVkcVAUCYMGZkAIbAwUJB4YfgAULCQGHAgYVCgkICwIE
FgIDAQIeAQIXgAAKCRDOstyUrVkcVAUCYMGZkAIbAwUJB4YfgAULCQGHAgYVCgkICwIE
85dEqmMyZuiIiWka7TRbegg2tp0lqGDYHgY9ZfaRyE61ldLTnVeuQUY33NY+gmAV
oVh+E4tTqBx1Zcq8B0HDv1YZpHWQievC6vHEfA19JzG6Y+wS8KuX+4ZJwwIQ2vEL
aUKy8ZdH+BWQXwViOX7qrfW08IXMaGsyUSRSCcBpAEMqWYgr1L4PUHYv06tn0RL7
naPHYbOiRjtEk310trdSW4IAeYftrWEV16sGETxQD/MxTLWreCgfdNIGFsptCu57
91n15eQm0eSJeavv72jmmFmDR1Ogf7gb2Lyr8z+aW6fGzaDtJ3CBoKSAtMDhZYqP
wxmJ4fLZtGpkFwE+51MjNJsXFyTi00M7czvNo8b1stI26vj4Eui85H6FQVeXEdtg
yslw/40jImF1HUcuoMqwUQ7TYVb1YDEHhllwU2e6+4J8RIE20rCF+FSCkDbLnQv
O18GNddnMPoJL5Z1JNz5kJUF9NsLUBl4pbQi9dwcpIEauD+yKqY+ajjCy4uzpNrJ
kVtcxR5gQa2oKCAj3utoK2BkzKTtmM75oLWCdCfWF9HNzXPUBUrUg1kw4DbNnCVF
MmKjWE8Lvm9iAY1HmdbxFeSYjKB6Z+t+i/BDhU6jgfs0gzxLb8azx0sPS1s68Ce
jv6SSoRD6dTEA7kCDQRgyBmQARAAXYrEuB3IXKYwt6FbhHSac8KjOgqpCtjZz1it
XrJlGezb8oa068ItYEsV/QvmOhg0Gi/XzAQRyXkKqAX/o0ZPp0ImeuPzUh6fEkat
xikP35VXN1777Z6PACnEfZp7WzzyFFvuzqR7w6Hs0iaABNLAX7LphX3Sp012mJjV
MBd61thY7N/HJQI7tnazeYN1PidnxFCf7UryQ7GuYPYcRZkVve2F6SjLuhRXadJX
18Kg+auZvOXY+a6LlQauefqQ0j8BAJuSpXRRt+hyst9BdcXnbtscyIH5bxfBj1+Y
ZxaoQUcMH1LQi6WwWL1NR7Qsmyp4Wb9B7vTXDbNephHxA9Vh7OX7P72r0ZyPvIRu
hqc0SMnqIrrqVG7aWqH3DSfeN06ZuzTG6vubTQ4K0BZrcmpqTyjEMN5hwbV+OhYu7
YMFQWkbfGSKxs88Tg6BB1RcKgdzTRdBrCvJvNv9W5zPVOpW0KY42ETzkxvbfS23
yzuJ2hUa2SPmg5QZZQpqbHSIPZ4mXZh+DYqaPw8ShDnC/AVFpZSv1vtC1xo9qrMp

V7MG52id+NXjOLUw+NOvQ1ZgyEY3a+/A9Tbwf+PAypbRjD8W3bABluUZhIBM2k08
qSEWNJebVpJIEdQ/k07K9YBU5b1Zh3gFc11iyHdEC4ChLAXExiI3nw6fOEAlEwx1
EdM3RI8AEQEAAAYkCPAQYAQgAJhYhBCQBXdLkAT1g3ze186y3JStWRxUBQJgyBmQ
AhsMBQkHhh+AAAoJEM6y3JStWRxU1gcP/3Q1t1HwP9PXT0VjB4f4qHnpbSCkP9Ae
HodiQFg5nqMdWwT8+PXyVubLf8cwq833uNvrdBfftWgDrj9u5Y+VGG12OQ8N1wpC
eGbnjtOeoMAQ+caitwQ2XuoyUe4nYiDhIMjiKmpNoDN12IS6VRRLE/oDDt/A3NL
5A8/c0/n1Alf48nRoanLAuy7FooodlAuxdEHHpsx7FNggjgB6Atf+bysFT9EPWa1
iknEnyqoHlk3DhoeQPIZ7xOfzOfVefIPLKO4/uB4sM5UoH6bSusn96UszM++8GB1
3X99SRXU18Hr/BveWk8dNHE+d5dtsvO5xJ04v8oO2M88Mj8lvQWD96PF4Sk+yZDH
OEvnfnA902m9Xzvv9JDLJ0ssPMES51avMFAoBjYbp9GWn6czNjeAP9KnuVdz7YjK
itThXQWvc52qHI7IR37/diznAN0BhXibM0j2d7TTSGuqg/Sru6YyEp2f6RHw73VX
vWu0TXb615qf6G1891T0W/6HLXkxEji+wrKFk+43rX1pfPWeObLr3btVxeLWNIzP
uoLuMhUxE+mEbgH+Vsv62UKQdevWCnNDsPK8yv043XGFOfdDCBGL7zUWesxeBbUr
iXwj8Dh86qSOspZn9+kTFt2tn2SeU8Hiy0kJaY+T8w9X3Wu22KNR5LLRU6SLshw
7+T1lelY94G9
=m6ZZ
-----END PGP PUBLIC KEY BLOCK-----

This PGP key available at :

http://103.252.21.85/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 include all staff of Pushansiber Bainstrahan 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](mailto:csirt[at]kemhan.go.id) or call (021) 75918947 which is active 24/7.

3. About CSIRT-Kemhan

3.1. 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 process

3.2. Constituency

The constituency of CSIRT-Kemhan includes all organizations units within Ministry of Defense

3.3. Sponsorship and/or Affiliation

CSIRT-Kemhan is part of Pushansiber Bainstrahan Kemhan, therefore it is fully funded by ...

3.4. Authority

TBD

4. Policies

4.1. Types of Incidents and Level of support

TBD

4.2. Co-operations, Interactions, and Information Disclosure

TBD

4.3. Communications and Authentications

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

5. Services

5.1. Main Services

Main services of Kemhan-CSIRT including :

5.1.1. Giving Warning Regarding Cyber Security Incident

- a. tbd

5.1.2. Cyber Security Incident Handling

- a. tbd

5.2. Other Services

Other services of Kemhan-CSIRT including :

5.2.1. Electronic System Vulnerabilities Handling

- a. tbd

5.2.2. Digital Artifact Handling

- a. tbd

5.2.3. Giving Reports Regarding Potential Threats Observation

- a. tbd

5.2.4. Threats Detection

- a. tbd

5.2.5. Risk Analysis of Cyber Security

- a. tbd

5.2.6. Consultations Regarding Cyber Security Handling Readiness

- a. tbd

5.2.7. Building Cyber Security Awareness

- a. tbd

6. Reporting Incident

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

- a. Photos/scan of identity card
- b. Evidence, such as : photos, screenshot or log file

7. Disclaimer

N/A