# RFC 2350 SumselProv-CSIRT Indonesia

## 1. Document Information

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

### 1.1. Date of Last Update

The current version is 1.0 and published on April 15, 2021

### 1.2. Distribution List for Notifications

There is no distribution list for notifications.

### 1.3. Locations where this Document May Be Found

The current version of this document can always be found at
https://csirt.sumselprov.go.id/rfc2350.pdf (bahasa version)
https://csirt.sumselprov.go.id/rfc2350-en.pdf (english version)

### 1.4. Authenticating this Document

Both documents have been signed with the PGP Key of Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) - Badan Siber dan Sandi Negara (BSSN). See section 2.8 for more details.

### 1.5. Document Identification

Both documents share the same attributes
Title          : RFC 2350 SumselProv-CSIRT
Version        : 1.0
Document Date  : April 15, 2021
Expiration     : This document is valid until superseded by a later version

## 2. Contact Information

### 2.1. Name of the Team

SumselProv - Computer Security Incident Response Team (CSIRT)
Short name: Sumsel Prov-CSIRT

### 2.2. Address

Jalan Kapten A.Rivai Nomor 3 Palembang;

### 2.3. Time Zone

Jakarta (GMT+07:00)

## 2.4. Telephone Number

+62 7111 355699

## 2.5. Faximile Number

+62 711 355669

## 2.6. Other Telecommunication

None Available

## 2.7. Electronic Mail Address

csirt[at]sumselprov.go.id

## 2.8. Public Keys and Encryption Information

Bits : 3072 ID : 0x9AF8472A5016E226
Key Fingerprint : 3931 EEA4 697F AC38 80C6 AFDA 9AF8 472A 5016 E226
Blok PGP Public Key :

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQGNBGBtooEBDAChAAU85xD53+slRfS5ZCIqdxya+7SqVcvrNPGc+39f9SOqhkdR
5MMnaz/rG5YfnQ2OQrndLfuWEtEGwWN5itdy/AeLMk4YFELHNsvBZMiDGdF+lpis
fYL7Se7gJas+ke3YbCwyeVhogyyokzeXDR5u8QTNiIR8aTEpHauhgm60lm0rYRBR
QfcFJlGoIby9G7w1AmQJXehxsSgUuohWvbtsEjkNDL2wzeY1Ct3UbBEmKP+l9IPj
shBblwPK4RGU34A/+ZOFwqq4Pz5PL0S6ePIThhWh8czTgXaE0uywy/tPoa9Md4OP
/0ap1tZ/TMfo2Nb3llQ03poqVWqoYxW9ANZ/wCZFCOOTXo32QVaMqdfyRC0rZaHw
T9sA9i2oHDTM2Xg9c3wptoWWg985NLkIE7H7cYg8Oh6Uz5QIcYUYMYEwMMPdjQHn
ZBwZWOd0mqVKIR1PlmRVON26W+BK0BDAxQ2mGYnPK7a/09dXXRDiPaoF3oYWm1pt
Nnp4cpNj/j7qoB8AEQEAAbQpQ1NJUIRfU3Vtc2VsUHJvdiA8Y3NpcnRAc3Vtc2Vs
cHJvdi5nby5pZD6JAdQEEwEIAD4WIQQ5Me6kaX+sOIDGr9qa+EcqUBbiJgUCYG2i
gQIbAwUJA8IAzwULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRCa+EcqUBbiJrfg
DACV9WR6kL2RlFiDG2o5/jtcKC13iMCRyhgCUOhadmqfBNftpt0wuBEIUuWxrDoX
8BEU7+XcHUk0Rz34QsxpQd+lBobHG6GkJXg9l+6uHwKFQB5KwwkeqjoQ/hubv2U8
l+yld6BWeeGnNM8vhA1KiH9yGKPz8tfRMjW3pwdCb9Dl/70UhdTxPDBKp4gvUEOW
gOzPGIkEurjXE8iAPdlVH3o1kGMh3k+8+PKvfF7MBIJQEDaDiIZt+z0KgeIbFLGA
blMjQgTJLr1otpsdhJjcwuVFtvOEOdnLC2yDEot/a5fxV6gnPQlOeGuWdZcZ7es5
cpvTMxJe3tqZTR4SC0jcSUuQKb1jX4oFs9woJCldCS/AS7GBpL+UjywMUsNA5o/O
ZywTVU6GQysb/ZdIy5lowjjyofD92KNOB9hn/ZBQ8dvyIS5DaDLghujKN3X6+haS
7o9dUI0Ix4Gi9Deqa/esk7KRKVtm3T3CxFZTHZGPwOvAaX421lwo9hFXu75R1SG7
heS5AY0EYG2igQEMAN+VFdRTCEDiLq04WCWDWUraPZskxf8rpE4Yzlpm1hyklWUu
d0iCfuidhLcAdG++6KREHXyYCqUrfpH2pfj+JDf4AXC9W686UvjNzZr9PHSXR5lY
sisEIAHjWm83gvo5AcOufaJgg/Lk83d7Lpxr8A4jkxcTG/G4+mMr8x04FCnsOoZk
U1nJdnuQwylyZ+MawiRzDK00VhabZlnE1SIb4Q6nh/WKH4arGp9TPmdhBnII8mOF
qz3ZlAudxT4oaft6vEo9Auke3m2mMix8r1x0HrQQKLIIYLsJMx5aWzh5YEgtYgIW
9mLshIc3PD57jhcf6bwxAeD/yXtx9Q5tBe7KRupRk/aFrvvur+eAvBUNJghvCRkg
8GsZM4tAX1S34i6z2FpymsB+wV/S98G4ONMCJBt2JDIcz5s41MEqloXbwfktdBWa
va0qOSd36dxLJWldeqwEXvrmE2YIK5ggqf+rjl8hWXw+ymlU8PAr4OLzZSIq88Oq
RHpPI87d4Db1y74+wwARAQABiQG8BBgBCAAmFiEEOTHupGl/rDiAxq/amvhHKlAW
4iYFAmBtooECGwwFCQPCAM8ACgkQmvhHKlAW4iY08Qv/cadiAyXQVy1/QlykUjx5
dknls7sx1XqNDSovwfTU57Cx39RBNmoTWbXr/TXDGasevwudNIpuFDHM1tPnu5K3
m6lDR4O/Eb8tOzsvguXDo6WDaKxxsd8ZowbZYfdGQHPxEjJSU+5W4XHmTmMKNsmO
p3KTVNOja2mTMDhx3CttnNMxDQNHFyNs+QGT1Vfuo3kGeojZdRCxgnLAcuzmQRmb
YIeO35iSDOIVYnEjvfvv4JtPC6m9ZX8Sq+tsoVG3VKIznsTi//TvFosUk3QyhNMX
-----END PGP PUBLIC KEY BLOCK-----

5rJ0MyqV23YU6GSluuvd0RA+9VZOb3T8uwm93vlaP98Qj3CZ5BpRcaRGk4Lm/ldM
vB3dmFQoM+1sP49aBdmoUSMR+/BBwZ0uuKBpitwKrBQsONO1sSmoVn11vIO+4BTf
kkYIX3vQ8I0qZm48FwbyZG+Fbr9csZVGTeARdRmwOCA3oNT6Mg+Haf3o4OYa6SSc
cWlCiMlrs2qsRJ52f1HTalZoc5ulY07IigjrA2ZhKIQY =1UJT

-----END PGP PUBLIC KEY BLOCK-----
File PGP key ini tersedia pada : https://websitecsirt.go.id /publickey.asc

### 2.9. Team Members

The Acting Head of the SumselProv-CSIRT is the Director of Response and Recovery for the Government Sector of South Sumatera. The team members include all OPD South Sumatera government sector.

### 2.10. Other Information

None available

### 2.11. Points of Customer Contact

The preferred method to contact SumselProv-CSIRT is to send an e-mail to Pusopskamsinas at csirt[at]sumselprov.go.id or call +62 711 355699 which is active 24/7.

## 3. About GovCSIRT

### 3.1. Vission Statement

The Realization of Cyber       Security in the South Sumatra Provincial Government

### 3.2. Constituency

The constituencies of SumselProv-CSIRT include: Regional Apparatus Organizations of South Sumatra Province

### 3.3. Sponsorship and/or Affiliation

The SumselProv-CSIRT funding is sourced from the South Sumatra Provincial Budget, Ministry of Communication and Information Technology, South Sumatra Province

### 3.4. Authority

Providing warnings related to cyber security, incident triage, coordination of cyber incidents, handling cyber incidents, building awareness and concern for cyber security, education and training.

## 4. Policies

### 4.1. Types of Incidents and Level of Support

The SumselProv-CSIRT Indonesia is authorized to address any kind of cyber security incidents, which occur or threaten the constituents (see section 3.2).
The level of support given by the SumselProv-CSIRT Indonesia will vary depending on the type and severity of the incident.

### 4.2. Co-operations, Interaction and Disclosure of Information

The SumselProv-CSIRT Indonesia highly regards the importance of operational cooperation and information-sharing between CSIRT, and also with other organisations which may contribute towards cyber security.
All information received will be kept confidential.

**4.3.  Communications and Authentication**

Use unencrypted e-mail and telephone for unclassified communication and use PGP-encrypted e-mail for sensitive/restricted/confidential information exchange.

# 5.  Services

## 5.1.  Incident Response

The SumselProv-CSIRT Indonesia assists the constituents to respond and recover from a cyber security incident related to the aspects of:

### 5.1.1. Incident Triage

a.  Determining whether the incident and reporter are authentic
b.  Assessing the impact and priority of incident

### 5.1.2. Incident Coordination

a.  Coordinating the incident with the constituents
b.  Determining possible cause of the incident
c.  Providing countermeasures recommendations based on guidelines/ standard operating procedures that SumselProv-CSIRT has for constituents
d.  Coordinating incident with CSIRT or other related parties

### 5.1.3. Incident Resolution

a.  Investigating and analyse the impact of incidents
b.  Providing technical recommendations for post-incident recovery
c.  Providing technical recommendations to correct system vulnerabilities

SumselProv-CSIRT presenting the government sector incidents statistical data as a serve government sector cyber security information centre.

## 5.2.  Additional Activities

a. Building awareness and concern for cyber security ;
b. Education and Training.

# 6.  Reporting Incident

Cyber security incident report can be sent to csrit[at]sumselprov.go.id by attaching:
a.  Photo/scan of identity card
b.  Incident's evidence, such as photos or screenshot or log file found

# 7.  Disclaimers

None Available