RFC 2350 JabarProv-CSIRT

1. Document Information

This document contains a description of JabarProv-CSIRT in according to RFC 2350. It provides basic information about the JabarProv-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 June 22, 2020.

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.jabarprov.go.id/static/rfc2350/rfc2350-id.pdf (bahasa version)

https://csirt.jabarprov.go.id/static/rfc2350/rfc2350-en.pdf (english version)

1.4. Authenticating this Document

Both documents have been signed with the PGP Key of Bidang Persandian dan Keamanan Informasi, Dinas Komunikasi dan Informatika Provinsi Jawa Barat. See section 2.8 for more details.

1.5. Document Identification

Both documents share the same attributes

Title	:	RFC 2350 JabarProv-CSIRT
Version	:	1.0
Document Date	:	June 22, 2020
Expiration	:	This document is valid until superseded by a later version

2. Contact Information

2.1. Name of the Team

Jawa Barat Provincial Government - Computer Security Incident Response Team.

Short name: JabarProv- CSIRT.

2.2. Address

Dinas Komunikasi dan Informatika Provinsi Jawa Barat

Jalan Tamansari No. 55 Kota Bandung

Jawa Barat Indonesia

2.3. Time Zone

Kota Bandung (GMT + 07:00)

2.4. Telephone Number

+6222 2502898

2.5. Faximile Number

+6222 2511505

2.6. Other Telecommunication

None Available

2.7. Electronic Mail Address

csirt[at]JabarProv.go.id

2.8. Public Keys and Encryption Information

Bits   : 4096

ID   : 0x15017BFB

Key Fingerprint : 7E01 E3FA 517E 3F7B 069F 62D0 9BD4 F6FB
                   1501 7BFB

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

xsFNBGHv6qYBEADO0Iz0aU0Ymi+4WUCucaEWexbuxtf5GJzmOT4s97iUnCzpzc9z
Pb+2ZeGWZCe1/YTNJAW2LnybhmBbbLm25rwlYvICzfwPgvYaxDjSZ1LYVt6ztliq
AmB2lagM4VVM/icM7eDcARYLPEByuVCY6/AkclYkzEG3jriJWOGEND7Jf44cX4YJ
vYJ4HQ4jexzqPlktyq8X3/WbNTCph4qJYAfWcTNJodPW7Elt55PCsgL5eHe0D66y
UocYRBXZVmDed9XHUn6hibBvByhdl6SzVEEuMva2zl/rbu8FMKy08xwtwdYXVrxf
2DJ1kb1TukuG2LnytWuxBpqSUq82T/OsT7511WaFAT31oxT02GedMYy3qXOMqZt5
x1pG6x9vJewq1PnNtDax1D/ONQaSfdhXLW5UdGss3K9c9a6LTbtHoP7JVsAO9GsF
xVzQN/h4vogLqLAsR2H0Ft8AtVxLQu7LnvI2qDLqgzL5sM3M+mEfrkpxqJxCDNkS
iVBuB2w/aJf43gTDyCn3sYkOIjVw0uKwZZJIpYwYjMRQxvkmTu00/ZXZa+nCDDoc
/wuMlELQtuy3PZQdfEfBfMPFVJndXtjAs7sNVZMSoLafCMNEBVidxtaKHtQB/Rgy
bkKgy7Jti5tXZEuyzLj51mEcrSxIZZqushtoB9nYP7QLa+Syo6+MLDFrHQARAQAB
zSdKYWJhclByb3YtQ1NJUlQgPGNzaXJ0QGphYmFycHJvdi5nby5pZD7CwY8EEwEI
ADkwIQR+AeP6UX4/ewafYtCb1Pb7FQF7+wUCYe/qqAUJBaOagAIbAwULCQgHAgYV
CAkKCwIFFgIDAQACgkQm9T2+xUBe/surA//WZ1CnYRAo7J/baz2jjwUe31DhuaH
ha7smay6nUn4D4d4YYAfhGTW8auVxyKQQhhXHe9QXRjX5W+IJQDrf7UAooHzcjQz
udW4wVpl7zzzGI+EadvJ+NUkEdEf/KLJWZOt1aFxkvyzmFzxksvnMzFqGsZZ4vW3
MK2ZqVVQ6e0bxjqcmhaval7KVLRE6XKcg2mopFPD2nYhZ0nUrXmt1lfFXlTp3H8C
xVbxkfe0zVV7/NCnkEiLz91LXgbv1zxi0DZKPJ+5hakwZZEri06QFDYOEUmaWeW1
nS6Fkkmalnta5WChw/f6n/WBhOgyVtZas4Khz45qpBjBtmGoH9ohZlUB20yH/SV3
ebyEUeAJfcCuw+IGEN9vb2MLvHPaR8Aq7l+OBA8KZ8kfuvLKKj3VAI/s2ChKP0Ls
Q5Cr2cyumX5iKIb4WWiI3CErsH8348Z4Q2W/s6EGzlfMw4IW9x7kLt+uJzc1uuCY
4GYXEWLrufu0a7IQZ/ucxNCSrAJx4o/xprWPdUGLV60HmQ/Hyhczt0bsSy0s8e+6
WRVJqrDLjsvA8YDmAS0phiGX4fXdUPxWOAPT07+mzacLT1Gz2kXZgoRs7HsQIyeo

```
iUTfAcCBm8xnPju76cWLKtBF98M/RkhCwmJMUUjGZ/sd6HiPuuPUyZ4IgecLa4ty
3MC0W01PWESxDjjOwU0EYe/qqAEQANELVMmrqQ0YQ48a58J8h7SsPZsgWt0XFpmo
o66oiVtgP0DC8vWf6/T2uhY+9ChNJ72ZXRXn7gQ/Pf7urmOV1VDAV0seKrDrOvxt
rUcyAOuYV3Sp76FRFi7/grZIFQmn1FpujtPtRIAPT9aJ/Pa55nu7azXEASBG8FeH
+auqnyI6gdCJqHWwQZTMo0RcraePe723tnvnhuRtOMwOP60rskoVFHpyspJ5Dc7f
C4ZeaUmPEdJjDytKY6CqGItoobnaWyp5zxM03R9Q47/6cJwxTbk94ubmfxI+IfBH
nt+xI09tQf4KegA4KszKBZwb5dBlBajioXmA85IMW75h9ONRcDyR+8/uOGqWsAMw
fEYQS/gNTpSVczr0+7+K8j3ndfniahQNicxHnaBtl/Wj8PAKj0s3Hd9HIJq4c4lp
wWSwRyFryn0NywcVwCeDf35Ue0SX2whTz6YdlQyu1Ojw4aL6vI9b7mUPKMxbNUJI
llGvMNc9CWGGtClM0tkJId+NQl+lZdpIqDf1APHv4u6wHx34mAwr1BD1jUuOZjID
FaeeW55dmTF4EDvQ/vZim6CuhsJEcfjdS8X+lM7PsqR6bXNW83PuoecqZXSuZXOx
xperhk3pIokwEvKbh9Ctwq3Do1LD4IqYzsgqyAMXDEk5/IId2ZU3PiB3Pmjjmy4D
crk8LOnhABEBAAHCwXwEGAEIACYWIQR+AeP6UX4/ewafYtCb1Pb7FQF7+wUCYe/q
qQUJBaOagAIbDAAKCRCb1Pb7FQF7+1k7EADJ62AWE8TbtIuZdiI5zpQ/SKl+4H8h
uSL2wN8ND+udwZgqqQ15Ofox82JJvKEKkIu6RwVoYJV7ADd3ihhVSDto6x9Q0+nL
1mu4geoWddPa8WhlJnVuDJQhTUQErCH0hldtIpjQRZWMAJdEAAh8cuhDflQXQoNP
uKQ+d9vRPByrnzxyDYTkMG6UClXEejqED+sXSlIo19Xr1f23DMIlG1P6y64aqQpm
fzGJ26DoUG2Q+zAv8svJqb5jiq5ny/qi5Gg+Qji0XUNZFUS7AXGYCvznZNxVl/1N
36py2sNPyOfGTlQOAW462BbuTE4NLdGxWlRemyIp19s1hKq+YKwH8cCnpR0nZMzg
KuUhFyDa72PQ2ROLJzt5RcLkBbIhLszBEOsYsCu0ob/xFu8VJJd1f9Ck7rg09tK6
zVh0+F3XiDQz6sO40UwHLd1LO8xnohEkB0g5QIa68czpR+GaNmmvo1p0UoXRTeue
JrnW8Iry4AOSk4M1ZvhqJhcUH5IoLuPQTc2C26GxD5q/vRO7ha//39ZvOq18iTJa
KZ3tsRqw04zS/wegwvo+1V5+6G2gN9JgP/gbv5i/r1SO/eyag3QtlgjxG7xwA0BN
f6FNrCtKhgk5820tg6JBAz1WjcFYfL+3csAjWq0S1XdgAJq0/zV0Ld66MgxdS4YW
8ZWbqI5m0TAkFg==
=V99d
```

-----END PGP PUBLIC KEY BLOCK-----

The PGP key file can always be found at: https://csirt.JabarProv.go.id/assets/
PubKeyJabarProv-CSIRT 2022.asc

2.9. Team Members

the Director of JabarProv-CSIRT is the Regional Secretary of West Java Province, Responsible Person is the Administrative Assistant of the Regional Secretariat of West Java Province, the Chairperson of West Java Province-CSIRT is the Head of the Communication and Information Office of West Java Province, CSIRT Secretariat is the Secretary of the West Java Provincial Communication and Informatics Office, and its members are from the Employees which reports cyber / information technology incidents at each Regional Apparatus Organization in West Java Provincial Government Environment.

2.10. Other Information

None available

2.11. Points of Customer Contact

The preferred method to contact JabarProv-CSIRT is to send an e-mail to csirt[at]JabarProv.go.id or call +6222 2502898 to Bidang Persandian dan Keamanan Informasi.

2.12. Vision Statement

JabarProv-CSIRT's vision is the realization of cyber resilience in the environment of the reliable and professional West Java Provincial Government.

2.13. Mission Statement

The mission of the West Java Province-CSIRT are:

a. developing, coordinating, collaborating and operating a system of mitigation, crisis management, prevention and recovery of cyber security incidents in the West Java Provincial Government environment;

b. building cooperation in the framework of overcoming and recovering cyber security incidents within the Government of the Province of West Java;

c. building the capacity of resources to handle and recover cyber security incidents in the West Java Provincial Government.

2.14. Constituency

JabarProv-CSIRT constituents include the Regional Apparatus within the Regional Government of West Java Province that uses the West Java Province Data Center services.

2.15. Sponsorship and/or Affiliation

JabarProv-CSIRT is part of the Regional Government of West Java Province so that all funding comes from the West Java Province Regional Budget.

2.16. Authority

JabarProv-CSIRT has the authority to carry out incident mitigation, incident mitigation, investigation and analysis of the impact of incidents, and recovery after cyber security incidents in the Regional Government of West Java Province.

JabarProv-CSIRT undertakes countermeasures and remedies at the request of its constituents and can coordinate with BSSN / other parties for incidents that cannot be handled.

3. Policies

3.1. Types of Incidents and Level of Support

JabarProv-CSIRT has the authority to handle incidents namely:

a. Web Defacement;

b. DDOS;

c. Malware;

d. Phising.

The support provided by JabarProv-CSIRT to constituents can vary depending on the type and impact of the incident.

3.2. Co-operations, Interaction and Disclosure of Information

JabarProv-CSIRT will collaborate and share information with CSIRT or other organizations within the scope of cyber security.

All information received by West Java Province-CSIRT will be kept confidential.

3.3. Communications and Authentication

For regular communication JabarProv-CSIRT can use email addresses without data encryption (conventional email) and telephone. However, for communications that contain sensitive / limited / confidential information you can use PGP encryption on e-mail.

4. Services

4.1. Reactive Services

The reactive services from JabarProv-CSIRT are the main and priority services, namely:

5.1.1 Alert service related to cyber incident reports

This service is carried out in the form of providing warnings of cyber incidents to electronic system owners and statistical information related to the service.

5.1.2 Incident relief and recovery services

This service is provided in the form of coordination, analysis, technical recommendations and on-site assistance in the context of mitigating and recovering cyber incidents

5.1.3 Vulnerability management services

This service is provided in the form of coordination, analysis, and technical recommendations in order to strengthen security (hardening). However, this service only applies if the following conditions are met:

a. Reporting of vulnerability is the owner of the electronic system. If the reporter is not the owner of the system, the report on vulnerability cannot be handled;

b. vulnerability handling service can also be a follow up to the Vulnerability Assessment activity.

5.1.4 Artifact handling services

This service is provided in the form of handling artifacts in the context of

recovering affected electronic systems or investigative support.

4.2. Proactive Service

JabarProv-CSIRT is actively building capacity of cyber security resources through activities:

5.2.1 Notification of observations related to new threats

This service is provided in the form of the results of the Honeynet BSSN early detection system. JabarProv-CSIRT provides statistical information related to this service.

5.2.2 Security assessment service

This service is in the form of vulnerability identification and risk assessment for discovered vulnerabilities. JabarProv-CSIRT provides statistical information related to this service.

5.2.3 Security audit services

This service is in the form of information security assessment. JabarProv-CSIRT Indonesia provides statistical information related to this service.

4.3. Cyber Handling Readiness Improvement Service

JabarProv-CSIRT improves the quality of security through activities:

5.3.1 Consultation related to preparedness and recovery of incidents

This service is provided by JabarProv-CSIRT in the form of providing technical recommendations based on the results of the analysis related to incident response and recovery.

5.3.2 Development of awareness and concern for cyber security

In this service JabarProv-CSIRT documents and publishes various activities carried out in the framework of building awareness and concern for cyber security.

5.3.3 Guidance related to preparedness for the response and recovery of incidents

JabarProv-CSIRT prepares a training program in the context of supporting incident response and recovery.

6. Reporting of Incidents

Cyber security incident reports can be sent to csirt [at] JabarProv.go.id by attaching at

least:

    a. Photo / Scan of identity cards;

    b. Evidence of incidents in the form of photos or screenshoots or log files found.

7.   Disclaimer

None available