

RFC 2350 BALIPROV-CSIRT

1. Document's Information

This document contains the description of BALIProv-CSIRT based on RFC 2350 which is the basic information about Baliprov-CSIRT which explains the responsibilities, services provided and how to contact BALIPROV-CSIRT.

1.1. Last Updated Document

The document is 2.0 version that issued on January 26th 2022.

1.2. Distribution Notification List

There is no Distribution notification list for document updates.

1.3. Location to Access this Document

This document is available at :

<https://csirt.baliprov.go.id/RFC2350/rfc2350-id-v2.pdf> (bahasa version)

<https://csirt.baliprov.go.id/RFC2350/rfc2350-en-v2.pdf> (english version)

1.4. The Authenticity of the Document

This document has been signed using PGP Key owned by Bidang Persandian - Dinas Komunikasi, Informatika dan Statistik Provinsi Bali. See section 2.8 for more details.

1.5 Document Identification

Documents' Identity:

Title : RFC 2350 BALIPROV-CSIRT;

Version : 2.0;

Publication date : January 26th 2022;

Expired : This document is valid until the newest document is publish.

2. Data Information/ Contact

2.1. Team's Name

Bali Provincial Computer Security Incident Response Team (CSIRT) or BALIPROV-CSIRT

2.2. Address

Dinas Komunikasi, Informatika dan Statistik Provinsi Bali
D.I. Panjaitan Street No. 7, Renon, Denpasar Bali

2.3. Time Zone

Denpasar (GMT+08:00)

2.4. Phone

(0361) 225859

2.5. Fax

(0361) 227810

2.6. Another Communication Access

None

2.7. Electronic Mail Address

csirt[at]baliprov.go.id

2.8. Public Keys and Encryption Information

Bits : 4.096 bit

ID : baliprov-csirt <csirt[at]baliprov.go.id>

Key Fingerprint : 51BC 52B4 DB2C ACD4 910D 6760 C361 C2CF 92D0 579E

Blok PGP Public Key :

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

mQINBGHwta8BEACvCDkA8qBq2LCGJKno+3533ZYfgLTfR0QA0Pd2p12pwBzPQ
TAgxv1yUSjIwmLDozXqz7kU4h5qi3ph2eEvgHpsiy/P5sAqRnsSTRmyCTHF0fVHlzv
GcDvQ2TubP42W8oZu9qvLwnLsWg2dKq0ijNiEt3Yy89/DK2JrAlaEJhGty9CaRmN
VjFr7UJWCUIW3vN0ALdox3ud3EqnAjFvQrNXBqHosPYg2NfvjtmilKeYXv9xyB1cl
yVLksP6xolLxIFr6HvQ1NKoYwO6RsaQSS9cZB4oHRBHzJxGDspEUIZ3NAAHEq/
HpR5bb2nIEZ5NW1LKxt19Sv5waEXf/11m+eglx5gWG4cVOjQW80dfEa1gB25F
Q3uLrJV6WDOXMcnZQFA0TNpn/vpnis7sG6xovjufAk2o6IAVYyHX3gvX9O5WZ8w
QsGfX+svE3+2T5mUo3fm2OqErfqJmpNkfkf4pzAWjBYBO8DjmSYZ2RmPpjdvh
b/DbVdwbnhIMUN3icVHwcV8/f7QjkS7QzC0ITVE2+ikKnMLBQI5V9edP6WEzgr6o
R6ii8kTnbmcNgHVRsKLYCNewNKgFQF+UZZqx+0gJ762tmGe9Sts8rDU0cMqnUB
SVDJP/iINnkq+ptt255rjduLZAPhLnDJoWoMg/w/Lu8ZWKjq9Xhpy89IGZQARAQ
ABtCViYWxpcHJvdi1jc2lydCA8Y3NpcnRAYmFsaXByb3YuZ228uaWQ+iQJYBBMBC
ABCfIEEUbxStNssrNSRDWdgdw2HCz5LQV54FamHwta8CGwMFCQPcEJEFCwkl
BwIDlgIBBhUKCQgLAqQWAgMBAh4HAheAAoJEMNhws+S0FeemYgP/3Jm7FW
oFd5CZRSr5/bbav1MystXEMTJ63attq/it0QEUEqk6gHmY2oteOEbVNSG5GTRYh
oeMY3hcrF6JPHNaH8Ny7gwfMlsy9mo4jXtwemXIAGyglzV+trunT2w1Gm3PY91hz
1yewK6JhSQHS2dE3cPIMEIxCHxAu3ApA1DMYkr4YoqQ5y5DAjUZxt6U8OkWYAi
oNSJH5GgLHcOf7IQkox1f9O+BmOkGn40VKuSNA0ZsBOmdSQ+pVaSOYsl+8e1i
gzgXIBqQEft2OFzx5oYUjo6ATTNjNjcx+XVul2nAS28ALd90NewjBR6l4gkF6VC7
Hxqk+s5FKxH1y2iozuxFPFwaoPn5IKkLw6lNxA+KdCPmUKUU+FEiizveO7M4zHc
R86rnPf+YtQ6NjnHUXXcTUxY1+Z0EjYfG9kHX5B6qk3th2tKsC27AvJRF1dhibleFZ
3bsJjdsjm0qv65p9WkHVMdfI+kHkB5UoEGjlxpZ2os/5rICnrhXldABx4x7uCbaa+2q0
JfIRwYlHv7HJlfQkyMMhWOuleL+IHjf71z78HV4a38cd9hOKTLOS63VEIT2G/HYrgc
EfkCB9wnhal7JO2KRISpgJNMCxz57Vvx99kNZxyr6ngMx3XDxHBpX5NWBPJZ/of
R5FZHHJn43i8H3sjpQesUB6etmeLg9OVuQINBGHwta8BEADChGsj/EDmFTP2fHP
nP+K6/1kqh9BeXXgFyhXV2BdlvMNe4nH8KkMtkHJUGymt4+9gBnLICCCQ5bDGrD9

+YvEYsOB7kguhfiHSjDPr3zdFHuljYCwbha+ZP3HEHOdtAn8xbAAb99fUy8RjjbasV
G/R14P/XPjz4sLfHcFdxgV9Kb8t2PpEuokHAHgaulloAzKqxrUO2KE98ZVa0hTs7YL
TN28knK52JuB5NnCCQvPtgiw4mCeNHaCerHPGuLF1fHeutUPLhIqFo/MCt6nUaJs2
e8iZczgjb4yWVW6+iw6Jm/49Fs3S0oTXuz4bD7hscE9e1dptKs5AnUuj1aPvCs+7O
E1+X5LKGpGu5fDmhAnm5RQjN3E1OV3O8qng4PoXccspXNq2KBlbfaGo3U7kAJX
OZ+mj2yLQrkwg+Z8USRfx2CQ3maFodbL2Hu+ThDpbzWHjKwtk8cmzplqQvWU/zk
3y7Lem7E7iHqAP107+GeLkeUPjPQpiK16BNSJxeQiaXu8KmFfbmEMDoX6QZWjn
0CkJWQ61till2pFyWkliF3v7iT6hTch3BOESGR+QTPCWIVb3Cb/2nkKP09ZMc9W
aDQV0ruggLEoKa69LrXQwBn9ZeAX2JxQshsuooXIEYkQWqGbkUqRIYLIZyqSU3p
noovHxO+09ZkwYforIFPnc5fVzJDwARAQABiQI8BBgBCAAmFiEEUbxStNssrNSR
DWdgw2HCz5LQV54FAMHwta8CGwwFCQPCeJEACgkQw2HCz5LQV56dlg/9Hwi
yevmFvN+jf9ICAYB2BH22kkGmfd2kpvWH5JyiZRcig36VnGKpaU7zpYMrlXPW2tcK
CRTR9HCneVrEfF5zaVtgCrXlpYSCfGY9g8CNBePHt4GnETLGrdRPNAL+q5/Q4b8
l63aD33M7HYGFzuK9atqQzON8pXpjJDhM5YI+2C1riEacCo3k5kZ9rhNNH5WkTG
4Qaz/7XilRBwLQ/ILLVfnymkG0ZkuT/KdMej4oDm0t0dDtRFcDmwF5mqbj4fZCPb3s
744dfEeY33jAQ+2b2nQoYTpsrXCJ3N1bWv7G7XiskLMCKls7iN4sOz24iLYMYJTbR
Lj3wLDPD+Qj3+tL6bK1O8yNY8Ep6RSu+T5h1wxJRBQ9OrFDamW81ghBpc2d8tF
RZ5yBC7iufgD9drsmZUrRrYFqKDtZf5vIA8kf58QoBGP7qQW9khF7PW2xikkoR5mk
+XeQfEOPnMgJvbD1jRPwZwuJEar6gAs3nf8ox1m56CxCzCRMk9z51fJEVHt2VFInk
OkegDxtGL2olRHylHlrmkBFk2P2V8w9/EswUqU4JIWS4Q+YGrjU1TiJ+Gyv9XB6u
Y/V9srtg8DnXI/8D1WerUPodUUfsiTvz/EsWIFE4MkiVC2LIUYzH+3kJGMGCair/snA
xlvx/gOyb6KiRMyEYMK82TzjF4rwmU2l/cA=
=FeJQ
-----END PGP PUBLIC KEY BLOCK-----

The PGP key file can always be found at:

<https://csirt.baliprov.go.id/RFC2350/publickey-v2.asc>

2.9. Team Members

The chief of BALIPROV-CSIRT is the Head of Bali Communication, Information and Statistic Department. The team members include all the staff of Bali Communication, Information and Statistic Department and other Bali Provincial's Offices as Cyber Agents in Bali Provincial Government.

2.10. Other information

None

2.11. Notes at BALIPROV-CSIRT

The method that recommended for contacting BALIPROV-CSIRT is via e-mail at [csirt\[at\]baliprov.go.id](mailto:csirt[at]baliprov.go.id) or via phone number (0361) 225859 to Bali Communication, Information and Statistic Department.

3. Regarding BALIPROV-CSIRT

3.1. Vision

The vision of BALIPROV-CSIRT is to create cyber resilience in Bali Provincial Government that is reliable and professional to actualize Nangun Sat Kerthi Loka Bali toward a New Bali Era.

3.2. Mission

The missions of BALIPROV-CSIRT, are:

- a. Coordinates and collaborates on cyber security services on Bali Provincial Government
- b. Build cyber security resources in Bali Provincial Government

3.3. Constituents

BALIPROV-CSIRT's constituents are government organizations within Bali Provincial Government.

3.4. Sponsorship and Affiliation

BALIPROV-CSIRT FUNDING come from Bali Province Regional Revenue and Expenditure Budget.

3.5. Authority

BALIPROV-CSIRT has authority to carry out countermeasures incident, incident mitigation, investigation and analysis of incident impact and recovery process after cybersecurity incident at Bali Provincial Government. BALIPROV-CSIRT carry out the responses and recoveries of constituents requests.

4. Policies

4.1. Types of Incident and Support Level

Types of incidents that supported by BALIPROV-CSIRT are:

- a. Web Defacement;
- b. Distributed Denial of Service (DDOS);
- c. Malware;
- d. Ransomware.

Support provided by BALIPROV-CSIRT to constituents can be varies depending on the type and impact of the incident.

4.2. Collaboration, Interaction and Disclosure of Information

BALIPROV-CSIRT will collaborate and share information with another CSIRT organization or another cybersecurity organization. All information received by BALIPROV-CSIRT will be kept confidentially.

4.3. Communication and Autentication

As regular communication BALIPROV-CSIRT use e-mail address without data encryption (conventional e-mail) and telephone. But if it's contains sensitive/limited or confidential information, BALIPROV-CSIRT will use PGP encryption on e-mail

5. Service

5.1. Main Service

BALIPROV-CSIRT's main service are:

5.1.1. Cyber Security Warnings

This service is provided by BALIPROV-CSIRT in form of Cyber security warning to the users of the electronic system and statistical information.

5.1.2. Cyber Incident Handling

This service is provided by BALIPROV-CSIRT in the form of coordination, analysis, technical recommendation and on-site assistance in the context of countermeasure and cyber incident recovety.

5.2. Additional Services

Additional Services that provided by BALIPROV-CSIRT are:

5.2.1. Electronic System Vulnerability Handling

This service is provided by BALIPROV-CSIRT in the form of coordination, analysis and technical recommendations in order to strengten (hardening). This service is only valid in thr following condition.

- a. The reporter of vulnerability is the user of the electronic system, the vulnerability report cannot service;
- b. The vulnerability management service referred, can also be follow up to vulnerability Assesement activities.

5.2.2. Digital Artifacts Handling

This service is provided by BALIPROV-CSIRT in the form handling artifacts in order to restoring affected electronic system or investigative support. BALIPROV-CSIRT provide ralated statistical information service.

5.2.3. Security Audits and Assessments

This service is provided by BALIPROV-CSIRT in the form of audits and assessments of the electronic system service.

5.2.4. Risk Analysis

This service is provided by BALIPROV-CSIRT in the form of a risk analysis of cyber security incidents as well as providing technical recommendation based on the results of the analysis.

5.2.5. Build Cyber Security Awareness and Concern

BALIPROV-CSIRT save and publish various activities doing by bali Communication, Information and Statistic Department in order to develop awareness and concern of cybersecurity.

6. Incident Report

Cybersecurity incident reports can be sent to [csirt\[at\]baliprov.go.id](mailto:csirt[at]baliprov.go.id) with attach at lease:

- a. Photo/ scan of ID card
- b. Evidence of the incident such as photos, screenshot or log files found

7. Disclaimer

Regarding the handling of malware types depending on the availability of tools that are owned.