RFC 2350 Badan Pangan-CSIRT

1. Information on Documents

This document contains a description of the CSIRT Badan Pangan based on RFC 2350, i.e. basic information about the CSIRT Food Agency, describing its responsibilities, services provided, and how to contact the CSIRT Badan Pangan.

1.1. Last Update Date

This is version 1.0 of the document published on February 19th 2024.

1.2. Distribution List for Notification

There is no distribution list for notification of document updates.

1.3. Where this document can be found

This document is available at:
https://csirt.badanpangan.go.id/storage/uploads/rfc2350.pdf
(Indonesian version)

https://csirt.badanpangan.go.id/storage/uploads/rfc2350-en.pdf
(English Version)

1.4. Document Authenticity

Both documents have been signed with the Badan Pangan-CSIRT PGP *Key*. For more details, please refer to Section 2.8.

1.5 Document Identification

Documents have attributes, namely:

Title	: RFC 2350 Badan Pangan-CSIRT;
Version	: 1.0;
Publication Date	: February 19, 2024
Expires	: This document is valid until the latest document is published.

2. Data/Contact Information

2.1. Team Name

Cyber Security Incident Response Team Within the National Food Agency
Abbreviated: Badan Pangan-CSIRT.

2.2. Address

Jl. Harsono RM No.3, Ragunan, Ps. Minggu, South Jakarta, Special Capital Region of Jakarta 12550

2.3. Time Zone

Jakarta (GMT+07:00)

2.4. Phone Number

(+62) 851 8787 7734

2.5. Fax Number

None

2.6. Other Telecommunications

None

2.7. *E-mail* Address

csirt[at]badanpangan[dot]go[dot]id

2.8. *Public Key* and other Encryption Information/Data

Bits : 4096
ID : 0xCADC9CDD6D6A3FAE
Fingerprint Key : 141B E4D9 683B 571A B90E F771 CADC 9CDD 6D6A 3FAE

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

xsFNBGXSvK0BEACnx2SPzc/acGNCQlNsxn9eSbE22cUSK8l4t3cz33i0k3nAOPfZ
48RDnlKD7PueLiSTrfbP0w9ek+y2d4Og1lkK4idwWPt37daQSZg2NnLk9FlHBqiy
HZsufa99QJsHJ0MDMmwE3hW82y2H2HwgN3iyBS3OhUQymrN8EEOaFOe8wZTkDbYm
blPUlNL1pRm8FInLsuuYusQLr7Id4x0unTatnHUFNjg/Zsb5VbBuAD/+nu+X2Ukz
XHp59sUACNM8xM2YmO91ZsJPG+l+4bJFYIUPWiAOxKvt19v4EENj1mNOYUkm61Zd
aqMRAWAePZXzQa1QgQrBuQ7ZQa+RzuPVt1KaiXrymktFRcAOOawsLBpASTlF1E4i
KTYf6mcq07s+98awgi/K2supl9jrsqQ1d+y7Y8rqdsuydfSvcyXHGc1w4rncn4g
RG1fO5nuMWW0TpWRbaGzwRSdS+Afy5poilneFGQvCvR5M0ZOS0MOt4p7IKbWVBfY
AVgebpOayZ9ycGhQjPz5/OU5mnoDfH0rv8g/tzEMNbbP5RS0glsAZOC4tVJP+sup
K7sbwYfmOsnUkNTyQZJ0wILf5uEPLA9WS6GCuARCdVFvBkWP3bo32hTbsHBlYViF
5viOGRQx5vtQu/my3DeGicUZNnEg4CHi7BMgvGBCA70AiIBxncj3v/EjswARAQAB
zSNORkEgQ1NJUlQgPGNzaXJ0QGJhZGFucGFuZ2FuLmdvLmlkPsLBhwQTAQgAMRYh
BBQb5NloO1cauQ73ccrcnN1taj+uBQJl0ryuAhsDBAsJCAcFFQgJCgsFFgIDAQAA
CgkQytyc3W1qP67kJRAAjmYtG+qie/Myn2rT+9ZC4nj4469ER7q3Pa7eB3jjeRC
ePItdqAShsP3+qJ2uEfmoTg3tc8qi4TgdsWTcMHWttluy59nukyaR0ODmY0cDAFc
u651c+aEiI0R9iO8iyqsw9z2LPVLbPqKOfoOCt3WRDQ7whb0uELiw7iBurpCiWlL
VZffbTW1tO3S5/T7os71jKaOLKIZLb2Z4uRXk/QkGARCqwb/Cs/waH0SSqchl6Sa
yH/Zs2u7z1vBz/7rVRHR+hxMTmH8UV+SqBlvEVJC9tKgdDC+TIR5WrCwBBMtZtIp
MyRT/of6wMIW3Pn4cyyRDRIFbozBbXVvZyda4YAJEfD9xcK3enbgfQ8BBJgHwB6a
mN9I8ivahS8g55GvxoRzfPGzYj3oB0l/TQBv1MqdcjSoJj3ye5thqxTkmVaFJ+cV
VnaPHyY1OPWO3p5N5UiAs+0+DPNAh/EG0lujWQ/uANuA3VH1NGV2hiOz6S7M5LHG
M3DW93OhhDvunBKmVJcAsWUVTYDMxFFvqKIC+f/RMfzZXYuv2ds7jnE4DwDPdEdt
royzocgHE7OlNR1EKlHr7uGIoOyf7GkkdwQmIqNu10XDXi870lBbafwaFneliu8O
BYYAaVjSkRpEzNMjaImGknkiQVOD8265nmSLJKsqVBgvPooYVnYysemPmnhWzETO
wU0EZdK8rwEQAKRObtYKI0EelgluDLjzn2w9xrf1oplyPoT9uy9jFS6tVncsIDRy
mtKeKIJ6SejoZaL305apBDeGEQwOM2Sr4p1o5BGjrFL9cKDKjgV1RAADnbaTNWsX
UxJ3olZLlUKhqxA5gmjLwqWfyNRnEEaqB26Gsa7YAfkXWARPBfZrVSudnFkvs06
zWe4IU/478AVDM0GSyCfs5Rn0oQmYta+JS9wt8n9oQWgFcuEOMFZliHHAFhD561w
oAjci1r+Vc/2IV3J2mSVcTQyn/BTHfN94jNLdg5R+vZSIzKgv3m/3zDhgaKFLtt
BYX8fpAclmMXq1NqmCYxSoHm9c5LCSJ7AxbDz5HW8b93+WSGAwegBk04+VAFO+4j
bGyg74/+HQGgnvLi3AopkH1dLIs0LymqkNgMWTfdC76mg7DiXoT0Cxy85aI9JkXF
4usqwMqgPKPAI+5oNe2mt8yaqtsy3nE89MZx8RpwgYcc7lciQFzcwZ/YfeF0QKOn
edRKy+Cn4PGDsojbS5pGFTtDSwGV9SmsUI0cCTeebF3fW8H5A7BTAVmaFAIOtaWh
knxQhLuLdYuefiDK4aVbblntYHaRDqvXYtQBgGmZdfhP4G4UgFDx/C0Z+B48dlaI
X4qJaQcgt7CJImW3/h0RUNupe4rSLuYtaSjOsyeBPppr6WH16aVpi3BFABEBAAHC
wXYEGAEIACAWIQQUG+TZaDtXGrkO93HK3JzdbWo/rgUCZdK8sAIbDAAKCRDK3Jzd
bWo/rtoND/96gm+95xHnUf2YhUmOYJC9ET8tj0mIwcJFWeukuEMAATh/3fHY75w6
```

```
aY1Qm9ch/t29PWJvkFX5PDAufxISKqxomcw4ppZ5useg8/JsKMPkG5gexfakO/gu
Pub4drVK+cascTPD5NyTNMtcDJaTy0gPww9J/VyYvivBVyzWEBabCEspQpTXhYfr
XWUfepFnOwtErtxLCu3R2r2/BEJtkAoG1mCzzceE4wUTLjViy4CuaovYxX0j+jUE
SIoM8rKpe6ORkDi2MeNFAheJAwIBOIFZw/GfrQicDEmaL5k+MTs+g5UFwnXrjn5j
sf5tZ58XqsWHsuoGFqIZQen8+eFOLa60lEHtMg/2Rl/HlvTFPrhbKstuoQYzy+kG
xig3Vf3rauicwdldMSHGNthFOLjv3deJmMdk9fuqC5qtHq9w/p5TUneFtGLGQifh
w07S9ojsL0pD4QmKBwGXMHtPKMPmwJgixPAscx1knJanir0ROM25XRd4RV0tcrVo
lS/5P3qVSOHuGkytl++BM+jsCmdBgNtCZoAr6oy13DxI7beHFIaXwCKI/qolGJxV
WsSJneiFqzg4GZm6u/sCELTxr+cp5WIRStO+I4pt+BIJR67zaEvoMrl5dcClvCl
f8Lb5QZAT0xxf+5uheMtumzCuEGYAh86YhjUgV38XwgzRZpL6IztEA==
=E0dW
-----END PGP PUBLIC KEY BLOCK-----
```


This PGP *key* file is available at:
https://dev-csirt.badanpangan.go.id/storage/public-key/BadanPangan_CSIRT_public.asc

2.9. Team Member

The Head of the Badan Pangan-CSIRT is the Head of the Food Data and Information Center, National Food Agency. Team members include personnel within the Food Data and Information Center, and echelon1 work units within the National Food Agency.

2.10. Other information/data

None.

2.11. Notes on Badan Pangan-CSIRT Contacts

The recommended method to contact the Badan Pangan-CSIRT is via e-mail at csirt[at]badanpangan[dot]go[dot]id or via telephone number (+62) 851 8787 7734 which is available from 08:00 - 15:30 WIB on Monday - Friday.

3. About the Badan Pangan-CSIRT

3.1. Vision

The vision of the Badan Pangan-CSIRT is

a. The creation of a reliable information security system within the National Food Agency.
b. Creating cybersecurity awareness in Human Resources within the National Food Agency

3.2. Mission

The mission of the Badan Pangan-CSIRT, viz:

a. Establish a center for recording, reporting, and responding to cybersecurity incidents within the National Food Agency;
b. Building cooperation in the framework of cyber security for IT services within the National Food Agency;
c. Increase the capacity of human resources against cybersecurity threats in the aspects of prevention, mitigation and recovery of cybersecurity incidents within the National Food Agency.

3.3. Constituents

Badan Pangan-CSIRT constituents include:
Users of Electronic-Based Government System within the National Food Agency.

3.4. Sponsorship and/or Affiliation

Funding for the Badan Pangan-CSIRT comes from the state budget.

3.5. Authority

The Badan Pangan-CSIRT has the authority to carry out incident management, incident mitigation, incident impact investigation and analysis, and post-incident recovery of cybersecurity at the National Food Agency and can coordinate and cooperate with BSSN / IT Security Academics / IT Security Principals / Security Experts for incidents that cannot be handled.

Badan Pangan-CSIRT conducts countermeasures and remediation upon request from its constituents

4. Policy - Policy

4.1. Incident Types and *Levels* of Support

The Badan Pangan-CSIRT caters to the following types of cyber incidents:

a. *Web Defacement;*
b. *Distributed Denial of Service (DDoS);*
c. *Malware;*
d. *Phishing.*

The support provided by the Badan Pangan-CSIRT to constituents may vary depending on the type and impact of the incident. The support provided is limited to the official tools of the National Food Agency.

4.2. Cooperation, Interaction and Disclosure of Information/data

The Badan Pangan-CSIRT will cooperate and share information with CSIRT or other organizations within the scope of cybersecurity.

All information received by the Badan Pangan-CSIRT will be kept confidential.

4.3. Communication and Authentication

For ordinary communication, the Badan Pangan-CSIRT can use e-mail addresses without data encryption (conventional e-mail) and telephone. However, for communications containing sensitive/restricted/confidential information, PGP encryption of e-mail may be used.

5. Services

5.1. Reactive Service

The reactive services of the Badan Pangan-CSIRT are primary and priority services, namely:

5.1.1. Providing alerts related to cyber incident reports

This service is carried out in the form of providing cyber incident alerts and also service-related statistical information to electronic system owners.

5.1.2. Incident response and recovery services

This service is provided in the form of coordination, analysis, technical recommendations, and on-site assistance in the context of cyber incident response and recovery.

5.1.3. Insecurity management service

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. The reporter of the vulnerability is the owner of the electronic system. If the reporter is not the system owner, the vulnerability report will be coordinated with the system owner;

b. *The vulnerability* management service in question may also be a follow-up to the *vulnerability assessment* activities.

5.1.4. Artifact handling service

This service is provided in the form of artifact handling in order to recover affected electronic systems or investigative support.

5.2. Proactive Service

a. Organizing cybersecurity workshops for constituents;
b. Organizing cybersecurity socialization to constituents

6. Incident Reporting

Cybersecurity incident reports can be sent to csirt[at]badanpangan[dot]go[dot]id by attaching at least :

a. *Photo/scan* of identity card
b. Evidence of incidents in the form of photos or *screenshots* or *log files* found

7. *Disclaimer*

None.