RFC 2350 CSIRT Alto Network

1. **Document Information**:

This document contains a description of the CSIRT Alto Network based on RFC 2350, providing basic information about CSIRT Alto Network, explaining its responsibilities, the services offered, and how to contact CSIRT Alto Network via email at csirt@alto.id.

a. Last Update Date: This document is version 1.0.

b. Distribution List for Notifications: There is no distribution list for document update notifications.

c. Document Availability Location: https://github.com/altonetworksecurity/csirt

d. Document Authenticity: There are two original versions of the document, one in Indonesian and one in English. Both documents have been signed with the PGP Key of CSIRT Alto Network. For more details, see Subsection 2.f.

e. Document Identification with attributes, as follows:

Title	RFC 2350
Version	1.0
Document Date	1 May 2024
Expiration	This document is valid until superseded by a later version

2. Data Information/Contact

Name : Cyber Security Incident Response – Alto Network
Abbreviation : CSIRT – Alto Network
Address : Blok C4 No.5, Satrio Tower Building, Jl. Prof. DR. Satrio 12th floor, Kuningan, Jakarta, Daerah Khusus Ibukota Jakarta 12950
Timezone : Jakarta, Indonesia (GMT+7)
Phone Number : +62 21 5085 8600
Email : csirt@alto.id
Public Key Information : We use PGP as the information exchange (incident reporting, incident announcement) with partner, vendor, constitution

Bits	EdDSA (Sign only) - ed25519
Key ID	95ED2B77B69F0833
Key Fingerprint	BC19 9884 47BC DC7C 3EC2 C255 95ED 2B77 B69F 0833
Blok PGP	-----BEGIN PGP PUBLIC KEY BLOCK----- xjMEZpngvBYJKwYBBAHaRw8BAQdA+T4czaV2fb931o75fgJk5fVSF2 XeNDHyTiN2j3rTv1PNJENTSVJUIC0gQWx0byBOZXR3b3JrIDxjc2lydE BhbHRvLmlkPsKMBBAWCgA+BYJmmeC8BAsJBwgJkJXtK3e2nwgzAx UICgQWAAIBAhkBApsDAh4BFiEEvBmYhEe83Hw+wsJVle0rd7afCDM AANEeAP0TXPFfYWdq/0FRn0M6Ur9/kh31cURibKS3aLFyzfBeVgEA6 fj0n22ahiuaJc2i3r//vjKKNdnvQtkmbvxVgasmHAPOOARmmeC8Egor BgEEAZdVAQUBAQdA5JIwo+VNpCeek7p9PYYJnzZOipGE4Teo49+b0 uP+tVUDAQgHwngEGBYKACoFgmaZ4LwJkJXtK3e2nwgz ApsMFiEEvBmYhEe83Hw+wsJVle0rd7afCDMAAEC1AQDQuZfSZsHiV iJ2DuOnwoLu/TwOE3uEg5eBzJYeMpmRFAEAitys51xfLCJtUmXWS74 lGvOl63wRiXow UgVZRoK3SQQ==spRA -----END PGP PUBLIC KEY BLOCK-----

a. Team Member
CSIRT Alto Network leads by Rionaldo Palinggi and helped by 30 more staff member.

b. Additional Notes
The recomended methodology to reach out CSIRT Alto Network is by email csirt@alto.id or phone +62 21 5085 8600 (24 hours).

3. About CSIRT – Alto Network

a. Vision & Mision

Vision:

To enhance the secure digital payment experience through improved data and cybersecurity.

Mission:

- Provide secure services in the implementation of digital payment technologies aimed at building resilience and reliability in cybersecurity to support business objectives.
- Educate and raise cybersecurity awareness among employees and users of Alto's payment technology to enhance cybersecurity resilience.
- Provide information on vulnerabilities, potential attacks, and other cybersecurity intelligence to foster a cybersecurity resilience ecosystem both within and outside of Alto.

b. Constituent

Constituent CSIRT – Alto - Network includes:

- PT Nova Digital Perkasa

c. Sponsorship and/or Afiliate

The funding for CSIRT – Alto Network comes from internal sources of Alto Network.

d. Authority

- To determine the assessment of information security levels in ongoing or upcoming business processes.
- To conduct assessments of the security levels of information systems that are developed in-house or contracted/purchased from third parties.
- To supervise and actively intervene in the operations of information systems to ensure cybersecurity resilience and reliability that supports business objectives.
- To plan, create, and operate a layered cyber defense mechanism (cyber defense-in-depth).
- To implement cybersecurity awareness programs in collaboration with relevant stakeholders.
- To have full authority to coordinate and intervene internally and externally, including access to data and systems for handling cybersecurity incidents.

4. Policies

a. Types of Incidents and Levels of Support
CSIRT – Alto Network handles cybersecurity incidents of the following types:

Core Service:

- Providing alerts related to cybersecurity
- Handling cybersecurity incidents

Additional Service :

- Addressing vulnerabilities in electronic payment systems
- Managing digital artifacts
- Notifying about potential threat observations
- Detecting attacks
- Conducting cybersecurity risk analysis
- Consulting on incident response readiness
- Building awareness and concern for cybersecurity

b. Cooperation, Interaction, and Information/Data Disclosure

CSIRT – Alto Network will collaborate and share information with CSIRT or other organizations within the cybersecurity domain. All information received by CSIRT – Alto Network will be kept confidential.

c. Communication and Authentication

For regular communication or non-sensitive/limited/confidential data to CSIRT – Alto Network, conventional email (without special data encryption) and phone calls may be used. However, for communication containing sensitive/limited/confidential information, PGP/RSA encryption (PGP Alto - sub-chapter 2.f) should be used for emails or email attachments.

5. Services

Core Services of CSIRT Alto – network:

a. Providing Alerts Related to Cybersecurity
This service will be carried out by CSIRT – Alto Network, consisting of alerts regarding cybersecurity threats to the owners/providers of financial services, including but not limited to PIP and PJP.

b. Handling Cybersecurity Incident
The cybersecurity incident handling service encompasses the full incident management cycle. Handling can be conducted on-site directly or by providing handling recommendations for follow-up.

c. Additional Services from CSIRT Alto - Network
Handling Vulnerabilities in Electronic Systems
This service includes coordination, analysis, and technical recommendations aimed at strengthening security control aspects, both in technical and non-technical scopes (Policy/Governance). In general, this handling is divided into:
- Reporting vulnerabilities on an as-needed basis by the owners/providers of the electronic systems belonging to constituents.
- Handling vulnerabilities as a follow-up to audit activities or vulnerability assessments.

d. Handling Digital Artefact
The service for handling digital artifacts is conducted to maintain the integrity of the chain of custody that may be required for investigations by law enforcement or as a means for technical incident investigations.

e. Notification of Potential Threat Observation Results
This service is provided based on observations by the cybersecurity intelligence function of CSIRT Alto Network regarding the digital assets of constituents.

f. Attack Detection
This service is offered when CSIRT Alto Network has visibility over the security systems implemented by constituents; attacks on constituents will be correlated to strengthen the overall security posture.

g. Cybersecurity Risk Analysis
This service is provided to estimate the attack surface of constituents, delivered periodically in accordance with compliance audit periods.

h. Consultation on Incident Response Readiness
This consultation service is aimed at helping constituents achieve sufficient preparedness for addressing cybersecurity incidents.

i. Building Awareness and Concern for Cybersecurity
This service is offered to constituents to develop a people-process-technology approach that supports ongoing information security awareness education programs.

j. Incident Reporting
Cybersecurity incident reports can be sent to csirt@alto.id , including at least the following attachments:

- Information: Full Name, Position, Phone Number, and originating Constituent.
- Evidence of the incident in the form of photos, screenshots, or log files found.
- Additional evidence or information as needed for incident handling according to applicable regulations.
- If the incident evidence is confidential, PGP encryption using the public key as outlined in point 2.f should be applied.

6. Disclaimer

a. C CSIRT Alto-Network conducts incident response activities by applying confidentiality as a working principle, and information sharing with parties will be conducted based on the principle of need-to-know.

b. b. CSIRT Alto-Network provides consultation services with a limited scope aimed at enhancing cybersecurity. Despite our best efforts, we cannot guarantee the definitive outcome of the services listed.

c. c. We are not responsible for the accuracy and/or timeliness of reports related to threat information dissemination.

d. d. CSIRT Alto-Network only provides communication channels as specified in RFC2350; we are not responsible for communications claiming to be from CSIRT Alto-Network through other channels.