Langslide

Threat Intelligence Policy

Version 1.0

PURPOSE

This policy aims to establish guidelines for the collection, analysis, and use of threat intelligence to protect the information assets of the Rudramsa Systems Pvt. Ltd. (herein referred to as Organization).

SCOPE

This policy applies to all employees, related departments, and functions facing information security threats.

DEFINITION

Threat Intelligence: Information used to identify and analyze potential threats and vulnerabilities to the organization's information assets.

Information Assets: All information owned, used, processed, or stored by the organization.

POLICY

Collection of Threat Intelligence

- The organization shall collect threat intelligence from various sources, including, but not limited to, open-source intelligence, commercial intelligence feeds, and internal data sources.
- The threat intelligence collection shall comply with all applicable laws and regulations.
- The organization shall establish a process for reviewing and validating the accuracy and reliability of the threat intelligence collected.

Analysis of Threat Intelligence

- The organization shall analyze the collected threat intelligence to identify potential threats and vulnerabilities to its information assets.
- The analysis shall be performed regularly or as necessary to address specific threats or vulnerabilities.
- The analysis shall be conducted by qualified personnel trained in threat intelligence analysis.

Use of Threat Intelligence

- The organization shall use the threat intelligence analysis to develop and implement appropriate measures to mitigate identified threats and vulnerabilities.
- The organization shall establish procedures for promptly disseminating threat intelligence to appropriate personnel.
- The organization shall maintain a record of the use of threat intelligence and the actions taken to mitigate identified threats and vulnerabilities.
- Threat intelligence should be analyzed and later used. By implementing processes to include information gathered from threat intelligence sources in the organization's information security risk management processes;
    - as additional input to technical preventive and detective controls like firewalls, intrusion detection systems, or anti-malware solutions;
    - as input to the information security test processes and techniques.

Management of Threat Intelligence

- The organization shall establish a process for managing the threat intelligence program on an ongoing basis, including periodic review and assessment of its effectiveness.
- The organization shall maintain appropriate documentation to support the threat intelligence program.
- The organization shall establish a process for disposing of threat intelligence that is no longer relevant or necessary.

Training and Awareness

- The organization shall train personnel with access to information assets on the importance of threat intelligence and how to use it.
- The organization shall provide all personnel with awareness training on potential threats and vulnerabilities to its information assets.

Conclusion

- This policy establishes the guidelines for collecting, analyzing, and using threat intelligence to protect the organization's information assets.
- Compliance with this policy is mandatory for all personnel with access to information assets.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Mar 14 2026	Initial Release	Pronoy	Kartikeya	Kartikeya