Policy on

Cybersecurity

For
Kansai Nerolac Paints Ltd.

Table of Contents

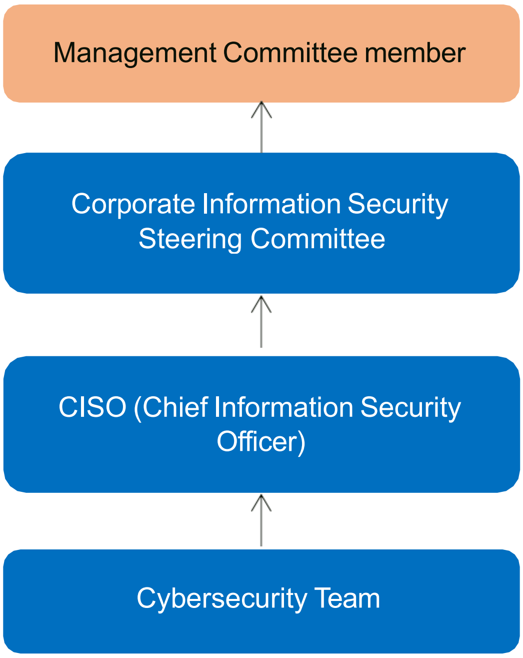
1.0 Objective 3
2.0 Structure **3**
3.0 Roles and Responsibilities 3
4.0 Policy Framework 4
5.0 Reporting Mechanism 4
6.0 Review Mechanism 4
7.0 Organizational Awareness 4
8.0 Information to External Parties 4

1.0 Objective

The objective of this policy is to safeguard, respond, resolve, and recover KNPL critical infrastructure and business application from cyber security incidence and attack by implementing, developing, collaborating, and cultivating cyber security capabilities and culture.

2.0 Structure

The responsibility for Cybersecurity rest with the Corporate Information Security Steering Committee and the cybersecurity operations head. The Corporate Information Security Steering reports to Management Committee member(s). The Cybersecurity team consists of Operations Team and report to the cybersecurity operations head.


Management Committee member
Corporate Information Security Steering Committee
CISO (Chief Information Security Officer)
Cybersecurity Team

3.0 Roles and Responsibilities

- Management Committee member(s): Responsible for providing oversight and governance and recommending best practices on cybersecurity for implementation.
- Corporate Information Security Steering Committee: Providing recommendations to the management on security tools and practices and guides the organization's security policies and ensures compliance. The committee also monitors threats and incidents and provides guidance for incident response and recovery.
- CISO (Chief Information Security Officer): Maintains awareness of emerging threats and safeguards organizations information assets and reports security incidents and impacts. CISO is also responsible for implementing the recommendation by the Steering Committee.
- Cybersecurity Team: Responsible for monitoring and mitigation of IT security risks and improve uptime and ensuring that the company's IT Infrastructure is

secure, investigating security incidences and working with other members of the organization to ensure that the IT Department and all employees are following best practices. The Team implements and monitors security policies, resolves, and recovers from cyber security incidents.

4.0 Policy Framework

The cyber security policy encompasses a series of sub policies which covers access control, data backup and recovery, incident management, human resources, vendor management, network and internet security, critical infrastructure security and end device protection.

The cybersecurity incidents are classified based on their impact and potential harm to the organization. It involves assessing factors such as the extent of data compromise, system downtime, financial losses, and reputational damage. By categorizing incidents into severity levels (low, medium, high), the response efforts are prioritized, and appropriate resources allocated for mitigation and recovery.

5.0 Reporting Mechanism

The Cybersecurity Team reports all security incidences via a ticket to the operations head daily. It is escalated depending upon the impact of security incidence.

6.0 Review Mechanism

The CISO (Chief Information Security Officer) submits monthly report to the Steering Committee. Steering Committee meets at-least once quarterly to review the cybersecurity operations.

7.0 Organizational Awareness

Training and awareness sessions are conducted / published periodically to ensure that everyone in the organization is updated on the cybersecurity issues. Learnings from advisories and tickets are incorporated in the training and awareness material periodically. Once a year all employees give an undertaking of being aware of the security protocols and policies in the HR Portal. At the time of joining the organization a security undertaking is taken from all the employees.

8.0 Information to External Parties

Indian Computer Emergency Response Team (CERT-In). CERT-In is the national nodal agency for responding to computer security incidents as and when they occur. As per guideline issued by CERT-In Organization to report cyber security incident within 6 hours of first information based on the guidance by Cyber Security Partner.

Securities and Exchange Board of India (SEBI) to be notified within 6 hours of first information of Cyber Attack based on the guidance by Cyber Security Partner.

Cyber Crime Portal – Raise the grievance on portal https://cybercrime.gov.in within 24 hours of first information of Cyber Attack based on the guidance by Cyber Security Partner. An acknowledgement number will be issued and retained for all future communication.

Affected Stake Holders to be informed where appropriate as informed by Security Committee.

Logs as per CERT-In

As per CERT-In all systems logs to be maintained securely for a rolling period of 180 days.

Last Reviewed February 2024

Jason Gonsalves
Director – IT, Corporate Planning, Materials