Exide Industries Limited (EIL)

Information Security Policy

1. Purpose

The purpose of this Information Security Policy is to establish a comprehensive framework for safeguarding all IT assets, information systems, business processes supported by IT, and personnel across our organization. This policy aims to ensure the confidentiality, integrity, and availability of information, as well as the protection of IT resources against unauthorized access, disclosure, alteration, and destruction.

2. Scope

This policy applies to all employees, contractors, third-party collaborators, and any other personnel with access to the organization's IT assets, and information systems, or involved in business processes supported by IT. The scope encompasses all devices, networks, software, data, and technology resources owned or operated by the organization.

3. Responsibilities

- **Management:** Executives and management are responsible for establishing and promoting a culture of security within the organization. They must allocate resources, define roles and responsibilities, and endorse security initiatives.
- **IT Security Team:** The IT Security team is tasked with implementing and maintaining security measures, conducting risk assessments, and responding to security incidents. They are responsible for enforcing this policy.
- **Employees and Users:** All personnel must adhere to this policy, follow security guidelines, and promptly report any security incidents or concerns to the IT Security team.

4. Information Classification and Handling

4.1. Data Classification:

Define categories of information based on sensitivity and establish appropriate security controls for each category.

4.2. Access Control:

Implement access controls to ensure that personnel have access only to the information and systems necessary for their roles.

4.3. Data Encryption:

Encrypt sensitive data during transmission and storage to prevent unauthorized access.

5. Network Security

5.1. Firewalls and Intrusion Detection/Prevention Systems:

Utilize firewalls and intrusion detection/prevention systems to monitor and control network traffic.

5.2. Wireless Security:

Secure wireless networks with strong encryption, access controls, and regular monitoring.

6. System Security

6.1. Patch Management:

Regularly update and patch all software and systems to address vulnerabilities.

6.2. Antivirus and Anti-malware:

Deploy and maintain antivirus and anti-malware solutions on all IT assets.

7. Incident Response and Reporting

7.1. Incident Response Plan:
Develop and maintain an incident response plan to address and mitigate security incidents promptly.

7.2. Reporting Security Incidents:
Establish clear procedures for reporting security incidents, ensuring a timely and efficient response.

8. Physical Security

8.1. Access Control:
Implement physical access controls to restrict unauthorized entry to IT facilities.

8.2. Equipment Protection:
Safeguard IT assets and equipment from theft, damage, or unauthorized access.

9. Personnel Security

9.1. Employee Training:
Provide ongoing security awareness training for all personnel to enhance their understanding of security best practices.

9.2. User Account Management:
Implement robust user account management procedures, including onboarding and offboarding processes.

10. Compliance and Review

10.1. Compliance: Ensure compliance with relevant laws, regulations, and industry standards about information security.

10.2. Regular Audits and Reviews: - Conduct regular security audits and reviews to assess the effectiveness of security controls and identify areas for improvement.

11. Document Control
This policy will be reviewed annually and updated as necessary to address emerging security threats or changes in the organization's structure. The IT Security team is responsible for maintaining and communicating any changes to all relevant stakeholders.

Version History

Version Number	Date of Enforcement
V1.0 – V5.0	2018 – 2022
V6.0	30th October, 2023
V7.0	1st April, 2024