Finolex Industries Limited

Information Security Policy

Contents

1. Introduction

FINOLEX INDUSTRIES LTD is committed to protecting the confidentiality, integrity, and availability of information across all business functions. The Information Security Policy outlines the company's security objectives and management framework to safeguard data, systems, and operations.

2. Commitment to Information Security

FINOLEX INDUSTRIES LTD protects information from unauthorized access, disclosure, modification, and destruction. The organization follows industry-leading security standards and regularly reviews security measures to address emerging risks.

3. Scope

This policy applies to all employees, contractors, vendors, partners, and individuals with access to FINOLEX INDUSTRIES LTD information systems and resources.

4. Objectives

• Prevent data loss, damage, or misuse.

• Maintain secure and reliable business operations.

• Protect personal and confidential information.

• Strengthen resilience against cyber threats.

5. Key Security Principles

• Organizational Controls: Governance, Policies for Information Security, defined roles and responsibilities, Acceptable use of information and other associated assets, supplier security and Risk Assessment.

• People Controls: Background checks, training, confidentiality obligations.

• Physical Controls: Access control, facility safety, CCTV monitoring.

• Technological Controls: Access control, encryption, antivirus, Patch management, Vulnerability Management, System monitoring, backups.

6. Incident Management

Security events must be reported immediately. FINOLEX INDUSTRIES LTD maintains structured procedures for investigation, containment, and corrective actions.

7. Data Protection

Sensitive data is masked, encrypted and processed per applicable privacy standards, access control, Identity Management.

8. Policy Framework

A detailed Information Security Standard will support this policy, outlining all controls needed for compliance. Each entity must maintain current documentation to prove adherence to both the policy and the standard.

9. Policy Deviations

Any deviations from the policies and standards outlined in this document—whether arising from legal or regulatory conflicts, existing internal policies, or implementation challenges—must be formally documented or have the associated risk accepted by the Head IT and / Business Head. Each entity maintains a record of such deviations along with their justification, and this log must always remain available for review.