Information Security Policy

Version 1.1

Document Statistics

Type of Information	Document Data
Document Title	Information Security Policy
Date of Release	25-11-24
Document Version No	1.0
Document Name	ISMS_FIL_IS_POL_02
Security Classification	Internal
Document Status	Official release

Name	Designation	Review Date (DD-MMM-YY)
Siddharth A. Zaveri	CISO	08-July-2024
Siddharth A. Zaveri	CISO	18-Nov-2024
Reviewed By		
Name	Designation	Review Date (DD-MMM-YY)
Harish Dash	CIO	08-July-2024
Harish Dash	CIO	18-Nov-2024
Approved By		
Name	Designation	Approval Date (DD-MMM-YY)
Harish Dash	CIO	8-July-2024
Saurabh Dhanorkar	MD	21-Nov-2024

Revision History				
Ver. No.	RFC Number	Revision Date (DD-MMM-YY)	Summary of changes (Include RFC number if applicable)	Updated By
1.0	-	-	Initial Version Released	Siddharth Zaveri
1.1	-	21-Nov-2024	Approval Authority Changed	Siddharth Zaveri

Document Reference List

S. No.	Document Name
1	Asset Management Policy
2	Logging & Monitoring policy
3	Network Security Policy
4	Encryption and Cryptography Policy
5	Acceptable Usage Policy
6	Backup and Restoration Policy
7	Access Management Policy
8	Incident Management Policy
9	Internal Audit Policy
10	Physical and Environmental Security Policy
11	Vulnerability Assessment and Penetration Testing Policy
12	Change Management Policy
13	Data Privacy Policy
14	Human Resource Security Policy
15	Third Party Security Management Policy

Table of Contents

1. Introduction

The information security policy outlines commitment to the security of Finolex businesses, resources, employees, contractors, other stakeholders, and the actions they shall take to prevent any information security incidents. It also seeks to set responsibilities for functions/businesses to deliver against information security commitments as well as establish a management framework to initiate/control the implementation and operation of information security within Finolex.

2. Policy Statement

Finolex is committed to safeguarding the confidentiality, integrity, and availability of all physical and electronic information assets to ensure that regulatory, operational, and contractual requirements are met.

This Information Security Policy is designed to:

- Protect information from unauthorized access, disclosure, modification, or destruction.
- Ensure the availability of critical information to meet business objectives.
- Establish a secure framework for the management of information across all systems and processes.
- Comply with applicable legal, regulatory, and contractual obligations.
- Promote awareness of information security risks and foster a culture of security across all levels of the organization.
- Implement risk management practices to identify, assess, and mitigate information security risks effectively.

This policy applies to all employees, contractors, and third-party partners who have access to Finolex's information systems, data, and resources. Any violation of this policy may result in disciplinary actions and potential legal consequences.

This policy will be reviewed and updated regularly to adapt to emerging threats and evolving business needs.

3. Scope

This document applies to all the users in the organization, including temporary users, visitors with temporary access to services and third parties/ off roll employees/ partners with limited or unlimited access to services.

4. Objective

The overall objective of this policy shall be to provide guidance and direction for the protection of Finolex's data, information, and information systems against any kind of accidental or deliberate damage, destruction, or misuse. It shall also seek to ensure that the information systems comply with relevant standards, laws, and regulations.

5. Policy Enforcement

Any violation of this policy by a Finolex employee shall be subjected to corrective actions and or/disciplinary actions as per HR Policies.

Any violation of this policy by a Finolex partner/vendor shall be reported to their respective organizations to take appropriate action. The partner/vendor organization may be subjected to penalties and/ or legal action as per the contractual agreement between both parties.

6. Exception Management

Exceptions may be granted in cases where security risks are mitigated by compensating controls and in cases where security risks are at a low, acceptable level and compliance with minimum security requirements, not interfering with legitimate business needs. To request a security exception, approval from the respective business head and Information security head/Management representative are mandatory.

7. Terms and Definitions

- Information Asset: A piece of information which has business value. Types of Information assets include software, hardware, electronic & paper documents, services, facilities, and people.
- Information Processing Facility: Any information processing system, service or infrastructure, or the physical locations housing them.
- Information Security: All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, authenticity, and reliability, of information or Information Processing Facilities.
- Third Party: All vendors who enter a direct contract (including their employees/sub-contractors) providing services /products to Finolex.
- Data Subject: The person to whom personal data belongs.
- Security Event: A security event is an identified occurrence of a system, service or network state indicating a possible breach of Information Security policy or failure of safeguards, or a situation that may be security relevant.
- Information Security Incident: An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
- Infrastructure Elements: Generic term used for network devices, security devices, telecom devices, servers etc.
- Malware: Malware is a generic term used for viruses, worms, Trojans, spywares, and other types of malicious codes.
- Control: Means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature.
- Asset Owner: An asset owner refers to an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets.
- Storage Media: Information recorded/stored on paper and hard copy files/folders and information stored in portable hard disks, USB, CD/DVD, memory cards, tape drives, phones, mobile devices.
- Business Continuity: Continuity of Finolex' s activities irrespective of the occurrence of natural disasters, terrorist strikes, man-made disasters etc.
- Risk Assessment: To understand what actions should be taken to minimize future damage to carrier and what risks are inevitable.

8. Policy

8.1 Information Security Framework

8.1.1 Information Security Domains

- This policy addresses the domains and controls mentioned in the ISO 27001:2022 standard under the following:
    a. Organizational Controls
    b. People Controls
    c. Physical Controls
    d. Technological Controls

8.1.2 Information Security Themes and Attributes

- Control Type – This attribute views the control from the perspective of when and how the control modifies the risk about occurrence of an Information Security Incident. *Attribute Values comprise of Preventive, Detective, and Corrective.*
- Information Security Properties – This attribute views the control from the perspective of which characteristic of the information the control will contribute to preserving. *Attribute values comprise of Confidentiality, Integrity, and Availability.*
- Cybersecurity Concepts – This attribute views the control from the perspective of the association of controls to cybersecurity concepts as defined in ISO 27110. *Attribute values comprise of Identify, Protect, Detect, Respond, and Recover.*
- Operational Capabilities – This attribute views the control from the perspective of information security capabilities. *Attribute comprises of Governance, Asset management, Information Protection, Human Resource Security, Physical Security, System and Network Security, Application Security, Secure Configuration, Identity and Access Management, Threat and Vulnerability Management, Continuity, Supplier Relationship Security, Legal and Compliance, Security Event Management, and Security Assurance.*
- Security Domains – This attribute views the control from the perspective of four Information Security Domains as identified in ISO 27001:2022. *The attributes comprise of Governance and Ecosystem, Protection, Defence and Resilience.*

8.2 Organizational Controls

8.2.1 Policies for Information Security

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify	• Governance	• Governance and Ecosystem • Resilience

- This policy highlights the senior management's intention to identify and secure organization's valuable assets in a manner which complies with legislations, meets leading practices and business needs, protecting it from unauthorized use, disclosure, or destruction. To ensure continuing suitability, adequacy, and effectiveness, the information security policy and supporting documents shall be reviewed annually or earlier if a significant change occurs (e.g., technology level changes in the organization, business level changes in the organization and regulations that impact information security)

- The input to the review should include but not be limited to:
  - Change in the business
  - Change in the IT environment
  - Trends related to threat and vulnerabilities, and
  - Reported security incidents and audit findings
- Records for the management review and approval shall be maintained
- Recommendations provided by relevant authorities and/or other associated entities, both within and outside the organization, shall be part of the security policy review agenda

8.2.2 Information Security Roles and Responsibilities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify	• Governance	• Governance and Ecosystem • Resilience

- All Information Security responsibilities, with regards to the protection of Finolex' s sensitive information, Information Systems and information processing facilities shall be clearly defined through job descriptions, work allocation and delegation of tasks
- The Information security policy shall be approved by Information Security Head
- The standards, procedures, templates, and guidelines shall be approved by MD
- The defined Information Security responsibilities shall be formally allocated and accepted across the organization. Such responsibilities shall include but are not limited to: -
  - Identifying the information assets and the security processes associated with each individual asset
  - Defining and documenting the asset ownership, the level of responsibility and authorization levels
  - Classification, labelling and handling of information assets in accordance with the Finolex Data Classification and Handling Policy
- Conduct risk assessment for all the identified critical assets at the time of any major change in the business/operational environment or once in every year, whichever is earlier
- Identification and implementation of controls that shall be termed necessary to adequately protect assets
- Reviewing and approving user access privileges in accordance with the Access Management Policy
- Conduct of internal audit, and fire drill and other audit activities, to ensure that the above mentioned are being followed

(For further details please refer to Asset Management Policy and Internal Audit Policy)

8.2.3 Segregation of Duties

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains

Preventive	• Confidentiality • Integrity • Availability	• Protect	• Governance • Identity and Access Management	• Governance and Ecosystem

- Roles defined to carry out business activities must consider segregation of duties to reduce opportunities for deliberate or accidental misuse of infrastructure elements and/or software. E.g., ability to initiate, authorize, execute, and verify requests should be split so that no one person completes the entire request
- Wherever segregation of duties is not possible, appropriate compensatory controls such as activity monitoring, audit trails and management supervision shall be developed to detect misuse of access rights
- When primary personnel are not available (e.g., vacations, illness and leave of absence) and the role is filled in by another person with a different role, appropriate segregation and/or compensatory controls shall be considered
- Conflicting functions (e.g., functions with ability to initiate, authorize, execute, and verify transactions) shall be identified and formally documented

8.2.4 Management Responsibilities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify	• Governance	• Governance and Ecosystem

- Finolex Management shall enforce all personnel to adhere Information Security Policy and other relevant documents
- All the Finolex personnel shall be properly briefed on their Information Security Roles and Responsibilities

8.2.5 Contact with Authorities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive Corrective	• Confidentiality • Integrity • Availability	• Identify • Protect • Respond • Recover	• Governance	• Defence • Resilience

- Appropriate contacts shall be established with law enforcement authorities, regulatory bodies, third party vendors such as hardware vendors, software vendors, and office security providers
- The responsibilities to maintain those contacts shall be jointly fulfilled by the legal, Information Security team and IT team

8.2.6 Contact with Special Interest Groups

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive Corrective	• Confidentiality • Integrity • Availability	• Protect • Respond • Recover	• Governance	• Defence

- The Information Security Head shall maintain appropriate contacts with special interest groups, forums, and professional associations related to Information Security to:
  - Improve knowledge about best practices and keep up to date with latest developments
  - Gain access to specialist Information Security advice
- Such information security related interest groups are ISACA (Information Systems Audit and Control Association), CERT-IN (Computer Emergency Response Team) agency for respective country, and likewise

8.2.7 Threat Intelligence

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive Detective Corrective	• Confidentiality • Integrity • Availability	• Identify • Detect • Respond	• Threat and Vulnerability Management	• Defence • Resilience

- The Information Security Head shall gather threat intelligence feeds or alerts from various external sources such as Vendor (OEM) Reports, Government Agencies (CERT-IN), Subscription to publicly available Threat Intel web sources and analyse the feeds as per the existing threat vector or landscape and maintaining the feeds in a centralized manner to take appropriate mitigation actions.
- The IT Managers shall update the appropriate IOCs in their respective security devices such as Firewalls, IDS, IPS, Anti-Malware, SIEM tool to prevent the Finolex environment from any potential cyber-attack

8.2.8 Information Security in Project Management

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify • Protect	• Governance	• Governance and Ecosystem • Protection

- Information security shall be integrated into organizations project management methods to ensure that information security risks are identified and addressed as part of projects. The project management methods in use shall require that:
  - Information security objectives are included in project objectives
  - A project risk assessment is conducted at an early stage of the project to identify project risks, and
  - Information security is part of all phases of the applied project methodology

- Information security implications shall be addressed and reviewed regularly in all projects

8.2.9 Inventory of information and other associated assets

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify	• Asset management	• Governance and Ecosystem • Protection

- All Information Assets (Physical, Software, Information, Paper, People, Site and Services) shall be clearly identified along with owners and an inventory of all assets shall be drawn and maintained, and
- Each function shall be responsible for identification of Information Assets and Information Systems used for processing and storing information; they shall maintain an inventory of such assets
- Asset Owner shall be identified for each asset within the asset inventory
- The asset owner or his delegates shall be responsible for:
    - Ensuring that assets are appropriately classified
    - Defining and periodically reviewing access restrictions and classifications, considering applicable access control policies
    - Approving information-oriented access control privileges
    - Selecting special controls needed to protect information, such as additional input validation checks or more frequent backup procedures
    - Approving all new or substantially enhanced application systems that use their information before these systems are moved into production operational status
    - Reviewing reports about system intrusions and other events that are relevant to their information, and
    - Select a security classification category relevant to their information and review this classification for possible downgrading or upgrading
- Information owners shall not delegate ownership responsibilities to contractors /external consultants, or to any individual who is not a full-time employee of the company
- Software asset management: Software asset management includes maintaining software license compliance; tracking the inventory and usage of software assets and maintaining control over the deployment and use of software assets. These include:
    - Procurement details, such as number of licenses granted, expiry date of licenses, etc., of software purchased shall be recorded by the IT team.
    - Software usage and deployment shall be tracked and reconciled against purchase data on a periodic basis. Any discrepancies, if observed, shall be reported to the asset owner, fixed asset team and IT team
    - In case software license agreements are found to be violated, the fixed asset team & IT team shall initiate immediate corrective actions to be taken as applicable
    - Software purchases and related data shall be tracked and regularly monitored. IT team along with respective business owner of the applications, shall be responsible for conducting annual reviews on this data to determine, but not limited to, the following:
        - If more licenses are being used than purchased, and
        - If new software or a greater number of licenses need to be procured to meet future business requirements

- IT team shall conduct a review at least once a year, of servers, desktops & laptops to determine if any unauthorized and unlicensed software are installed

- The asset owner shall be responsible for the conducting a risk assessment as described in asset management policy

(For further details please refer to Asset Management Policy)

8.2.10 Acceptable use of information and other associated assets

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Asset management • Information Protection	• Governance and Ecosystem • Protection

- Acceptable use of assets associated with information processing facilities shall be clearly defined
- All users (employees) who use or interface with assets associated with information processing facilities shall acknowledge their awareness of acceptable use of assets
- Employees and vendors using or having access to Finolex assets shall be responsible for their use of any information processing resources and of any such use carried out under their responsibility; and
- Finolex shall ensure control against unauthorized copying of relevant information (e.g., intellectual property) by employees and vendors
- Finolex shall ensure that adequate security controls are put in place to secure the information on the employee-owned devices

(For further details please refer to Acceptable Usage Policy)

8.2.11 Return of assets

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Asset management	• Protection

- Upon termination of employment or services, the employees or third-party vendors shall return/ hand-over all Finolex' s assets that were issued to them or are under their purview

(For further details please refer to Asset Management Policy)

8.2.12 Classification of Information

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify	• Information Protection	• Protection • Defence

- Information Assets and information processing systems shall be classified based on their business value, legal requirements, sensitivity, and criticality to the organization
- Information Assets shall be classified as per established standard in the following parameters:
    - Confidential – This classification applies to data that must be available for Finolex to effectively perform its mission and meet legally assigned responsibilities, and for which special precautions are taken to ensure its accuracy, relevance, timeliness, and completeness. This data, if lost, could cause significant financial loss, inconvenience, or delay in performance of the Finolex mission
      Examples: Third Party/Vendor Contracts, Internal Audit Reports, System Design Documents, Financial Records etc.
    - Internal – This classification applies to data that is specifically meant for employees of Finolex. While its unauthorized disclosure is against the policy, it is not expected to seriously or adversely impact. The distribution of such documents shall remain with the business, employees, customers, stockholders and/or business partners
      Examples: Intranet web site content, Process documentation like policies and procedures etc.
    - Public – This classification applies to data, which has been explicitly approved by the management for open/public access
      Example: Sales brochures, Web Site *Content, Advertisements, Statutory Audit reports etc.*
- Following guidelines shall be considered for reclassification of data assets:
    - Classification of data assets should be reviewed periodically (at least once every year) to ensure adequate classification as per the business requirements
    - Whenever there is a need to reclassify the data, the data custodian should seek approval from the data owner, in consultation with Business head, prior to changing the data classification
    - In case the data owner and Business head are same individual, the approval (over email) shall be taken accordingly
    - Reclassification date for "confidential data" should be mentioned on the document statistics section of any document, and
    - After reclassification, the data custodian should ensure that all the necessary changes are incorporated in the asset register

8.2.13 Labelling of Information

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Information Protection	• Protection • Defence

- Data owners shall ensure that data either in paper form or stored in removable media like tape, laptop, desktop, USB etc. shall be externally labelled (marked) with the appropriate classification
- Data owners shall ensure that the labelling will be maintained until the paper / removable media is destroyed or data is declassified. Data owners shall ensure that in case of electronic documents, the appropriate data classification is mentioned in the footers of the document. Alternatively, the electronic documents residing on the systems shall be kept in folders marked according to the pre-defined data classification, and

- Users shall ensure that the naming of Finolex data files will be meaningful and capable of being recognized by its intended users. Every document should follow a specific naming convention for ease of understanding and to maintain the integrity of the document

  Example: Asset Management Policy

8.2.14 Information Transfer

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Asset Management • Information Protection	• Protection

- Finolex shall ensure that security is maintained at all aspects of Confidentiality, Integrity, and Availability while transferring the information within and outside the organization
- Adequate legal controls like signing of NDAs and other Information Security Controls shall be put in place while sharing the information with any third party
  - Finolex official emails shall not be forwarded to personal email account(s)
  - Finolex emails shall not be forwarded to unauthorized personnel within or outside of Finolex network
  - All information stored, transmitted, received, or contained in Finolex e-mail systems is Finolex' s sole property and may be accessed by the company at any time, and
  - Wherever possible, business functions shall use only officially appointed courier service providers for transmitting physical information

8.2.15 Access Control

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Identify and Access Management	• Protection

- An access control policy shall be established, documented, and reviewed regularly considering the requirements of the business for the assets in scope. The policy should consider below mentioned points:
  - o Access to different business applications
  - o Management of assigned level of access, and
  - o Formal procedures/policies for defined roles and responsibilities
- As per the principle of least access, every Finolex employee should only get access to Finolex network and network services as per their designated job's roles and responsibilities. The following points should be taken into consideration:
  - o The networks and network services in scope for access
  - o Finolex employees shall only have direct access to the network services that they have been specifically authorized to use
  - o Users should not establish any external network connections that could permit third party users to gain access to Finolex systems and information, and

- When using Finolex systems, users shall not deliberately conceal or misrepresent their network identity

- A formal user registration and de-registration process shall be implemented to enable assignment of required access rights. The below mentioned points should be taken into consideration
  - All user IDs on Finolex systems shall be assigned according to the Finolex standard user ID creation
  - Every user shall have a unique user ID and password for access to Finolex systems and networks
  - There shall be a formal process for user id creation and deletion process
  - User id creation/ modification/deactivation request shall be required to be authorized by respective Business head and submitted to application owner/IT team before user access is created, and
  - IT team should follow formal de-registration process for revocation of access to all Finolex systems and network services
- A formal user access provisioning process shall be implemented to assign or revoke rights for all user types to all systems and services. The provisioning and revoking process should include the following points:
  - The respective Business head of the user shall be authorised to approve the access to Finolex domain, applications, and infrastructure components
  - Post obtaining the required approval from Business head, access shall be provisioned/ granted to the user by the IT team, and
  - For any privileged access to Finolex systems/networks/applications the approval shall be obtained from Information Security Head in consultation with Business head
- Process shall be defined to ensure that access rights associated with the employees, and third-party personnel are revoked upon termination of their employment, contract, or agreement.
  - The defined processes must also outline steps to be taken in case of management-initiated terminations based on disciplinary grounds
  - If there is a change of role, necessary changes/adjustments shall be made so that the user does not have more rights than required to carry out the new job function and
  - The removal or modification of access rights for terminated Finolex employees or contract employee shall be carried out by the IT team

8.2.16 Identity Management

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Identify and Access Management	• Protection

- A formal user registration and de-registration process shall be implemented to enable assignment of required access rights. The below mentioned points should be taken into consideration:
  - All user IDs on Finolex systems shall be assigned according to the Finolex standard user ID creation
  - Every user shall have a unique user ID and password for access to Finolex systems and networks

- There shall be a formal process for user id creation and deletion process
- User id creation/ modification/deactivation request shall be required to be authorized by respective Business head and submitted to application owner/IT team before user access is created, and
- IT team should follow formal de-registration process for revocation of access to all Finolex systems and network services

8.2.17 Authentication Information

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Identify and Access Management	• Protection

- Secret authentication information is a gateway to access valuable assets. It typically includes passwords, encryption keys etc. the allocation of secret authentication information shall be controlled through a formal management process.
  - Passwords used by the Finolex employees and those set/provisioned on systems, network devices shall meet complexity requirements
  - Users shall be educated to keep the passwords allocated to them confidential
  - When granting access to infrastructure or software(s), users shall be provided with a temporary or one-time password that meets the password complexity requirements. Users need to change this password at first login and shall be unique for each user; and
  - Temporary passwords should be given to users in a secure manner such as through restricted emails to intended user

8.2.18 Access Rights

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Identify and Access Management	• Protection

- Asset owners in coordination with Business heads must review users' access rights at regular intervals. The below mentioned points should be taken into considerations:
  - The user's access level, access logs shall be reconciled on a monthly frequency
  - Redundant and unused user accounts shall be removed within 90 days
  - Authorisation for privileged access rights should be reviewed at frequent intervals by IT team

(For further details please refer to Access Management Policy)

8.2.19 Information Security in Supplier Relationship

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains

Preventive	• Confidentiality • Integrity • Availability	• Protect	• Supplier Relationships Security	• Governance and Ecosystem • Protection

- Information security requirements for mitigating the risks associated with supplier's access to Finolex' s assets shall be agreed with the supplier and documented in the form of agreements or contracts
- Finolex shall identify the critical vendors based on confidential, integrity and availability of the services associated with the vendor

8.2.20 Addressing information within Supplier Relationship

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify	• Supplier Relationships Security	• Governance and Ecosystem • Protection

- All agreements with suppliers that access, process, communicate or manage organizations information or information processing facilities, or provide products or services shall have relevant security requirements embedded in them
- The information security clauses in the supplier agreements shall be followed in adherence to the Finolex Third Party Management Security Policy

(For further details please refer to Third Party Security Management Policy)

8.2.21 Managing Information Security in the ICT supply chain

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify	• Supplier Relationships Security	• Governance and Ecosystem • Protection

- Finolex shall maintain security in line with Confidentiality, Integrity, and Availability for its ICT systems
- Agreement with suppliers shall include requirements to address the information security risks associated with information and information processing facilities and product supply chain
- A Business Continuity strategy shall be developed for all ICT systems
- Periodic risk assessments or security assessments shall be performed to ensure the assurance of the security

8.2.22 Monitoring, review and change management of supplier services

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify	• Supplier Relationships Security	• Governance and Ecosystem • Protection • Defence • Information Security Assurance

- Significant changes to supplier services (e.g., enhancement to networks, new technologies, new products, or newer versions, change of vendors, change of physical location etc.) shall be informed to the Information Security team
- Such changes shall:
  - Consider criticality of business systems and processes involved, and
  - Be accompanied by re-assessment of risks
- All the changes in the supplier services shall be performed in line with Finolex Change Management Policy

8.2.23 Information security for use of cloud services

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify	• Supplier Relationships Security	• Governance and Ecosystem • Protection

- Finolex shall define Information Security requirements associated with the use of Cloud Services for all SaaS, IaaS, and PaaS platforms.
  - All the cloud infrastructure shall be hardened
  - There shall be adequate security controls to manage the access to the cloud infrastructure
  - The cloud infrastructure shall be integrated with the SIEM solution
  - A Vulnerability Assessment and Penetration Testing of the cloud infrastructure shall be performed, and the findings shall be mitigated. In case of SaaS platforms, the vendor shall be asked to share the VAPT reports
  - Finolex should follow secure coding guidelines for the applications which are going to be deployed on cloud

8.2.24 Information security incident management planning and preparation

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Corrective	• Confidentiality • Integrity • Availability	• Respond • Recover	• Governance • Information Security Event Management	• Defence

- An incident management approach should document how Finolex shall establish responsibilities and procedures to ensure timely, effective, and orderly response to address weaknesses, events, and security incidents
- The procedures for incident, event and weakness response planning shall need to be clearly defined in advance of an incident occurring and been approved by Finolex
- Information Security weaknesses, both actual and suspected, shall be reported through different channels such as email, phone line, and intranet. In addition, users shall not test the existence of vulnerability in any information facility, system, or application
- Centralized tracker shall be maintained of all reported Information Security weakness

8.2.25 Assessment and decision on information security events

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Detective	• Confidentiality • Integrity • Availability	• Detect • Respond	• Information Security Event Management	• Defence

- The reported events shall be analyzed and classified as information security incidents, as per the defined criteria, on basis of their potential impact
- If required, the Information Security team shall have the necessary rights to access the systems and applications for forensic purposes

8.2.26 Response to Information security incidents

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Corrective	• Confidentiality • Integrity • Availability	• Respond • Recover	• Information Security Event Management	• Defence

- The overall response to reported incidents shall include identification of corrective actions
- Where a follow-up action against a person or organization after an Information Security Incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s)

8.2.27 Learning from Information security incidents

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify • Protect	• Information Security Event Management	• Defence

- Incident Response Team (IRT) in consultation with IT Team shall establish a Known Error Database (KEDB) for the information gained from the evaluation of all incidents. The KEDB shall be referred to for incident handling and as a learning source of incidents

8.2.28 Collection of evidence

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Corrective	• Confidentiality • Integrity • Availability	• Detect • Respond	• Information Security Event Management	• Defence

- As per the legal/contractual requirements, the evidence shall be collected during incident analysis, retained, and presented for relevant authorities for the high and medium incidents for which Root Cause Analysis (RCA) shall be conducted. The evidence shall be collected in a manner that does not destroy its evidentiary value. While collecting the evidence, the following shall be considered but not limited to:
  - Applicability of evidence: Whether the evidence can be used in a court of law, and
  - Weight of evidence: The quality and completeness of the evidence

  (For further details please refer to Incident Management Policy)

8.2.29 Information Security during disruption

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive Corrective	• Confidentiality • Integrity • Availability	• Protect • Respond	• Continuity	• Protection • Resilience

- The organization-wide Information security processes shall include Information Security requirements to help ensure that confidentiality, integrity, and availability of critical information assets shall be preserved even in the event of a business disruption or disaster
- Finolex shall identify recovery guidelines that can be taken as baseline reference to classify critical systems and develop recovery and restoration plans
- A strategy plan, based on appropriate risk assessment, shall be developed for the overall approach to information security, and
- In the absence of formal business continuity and disaster recovery planning, information security management shall assume that information security requirements remain the same in adverse situations, compared to normal operational conditions

8.2.30 ICT readiness for business continuity

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Corrective	• Availability	• Respond	• Continuity	• Resilience

- Finolex shall ensure that an adequate framework is in place to prepare for, mitigate and respond to a disruptive event using personnel with necessary authority, experience, and competence
- Finolex shall identify personnel with necessary responsibility, authority, and competence to manage an incident and maintain information security
- Finolex shall ensure that documented plans, response, and recovery procedures are developed and approved, describing how Finolex will manage a disruptive event and maintain its information security at a predetermined management approved information security continuity objective

- Information security controls for all systems shall be reviewed and verified. Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective
- Each calendar quarter, emergency contact information shall be validated and revised
- The roles and responsibilities for both information systems contingency planning and information systems recovery shall be reviewed and updated annually

8.2.31 Legal, statutory, regulatory, and contractual requirements

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify	• Legal and Compliance	• Governance and Ecosystem • Protection

- Information Security Head at Finolex shall be responsible for communicating changes to any of the above areas and additional security requirements
- Necessary measures shall be taken to prevent the following types of content from being carried over the Finolex network in any form:
    - Objectionable, obscene, unauthorized content
    - Content, messages, or communications infringing copyright, intellectual property etc. and
    - If instances of such infringement are reported by the enforcement agencies, it shall be ensured that carriage of such material on the network is prevented immediately
- Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations

8.2.32 Intellectual Property Rights

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify	• Legal and Compliance	• Governance and Ecosystem

- Software used must be acquired from legitimate (known and reputable sources) to ensure copyright is not violated
- Proof and evidence of ownership of licenses, master disks, manuals etc. shall be maintained
- Controls shall be implemented to ensure maximum number of users permitted to use the software is not exceeded
- Only authorized software and licensed products shall be installed, and
- Copying, storage, duplicating, converting to another format, extracting of electronic content (eBooks, media files, articles, reports etc.) must not violate copyright laws

8.2.33 Protection of Records

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains

Preventive	• Confidentiality • Integrity • Availability	• Identify • Protect	• Legal and Compliance • Asset Management • Information Protection •	• Defence

- Important records required for meeting statutory and regulatory requirements shall be identified and their retention periods defined, and
- Each department having ownership of such records shall ensure that these records are protected from loss, destruction, unauthorized disclosure, and falsification

(For more details, please refer to Document Control and Record Policy)

8.2.34 Privacy and Protection of PII

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify • Protect	• Information and Protection • Legal and Compliance •	• Protection

- Finolex shall ensure Privacy and protection of personally identifiable information as required by the relevant legislation and regulations
- The customer data shall be masked on all the application
- The employee PII (Personally Identifiable Information) shall be masked on all the platforms
- Access to customer database shall be restricted and shall only be accessed from intranet

(For more details, please refer to Data Privacy Policy)

8.2.35 Independent Review of Information Security

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive Corrective	• Confidentiality • Integrity • Availability	• Identify • Protect	• Information Security Assurance	• Governance and Ecosystem

- Audits of operational Information Systems shall be planned and performed at periodic intervals with the agreement of the Information Systems' owner to minimize the risk of disruption to business processes
- Independent audits of information security management system shall be performed as per the planned intervals or when significant changes occur

(For more details, please refer to ISMS Monitoring and Measurement Procedure)

8.2.36 Compliance with policies, rules, and standards for information security

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify • Protect	• Legal and Compliance • Information Security Assurance	• Governance and Ecosystem

- Continued compliance with Finolex' s information security policies and procedures shall be maintained
- Any detected non-compliances with the information security policies shall be investigated and corrective action shall be taken and reviewed
- Such non-compliances as well as their preventive actions shall be further reported at the time of independent reviews

8.2.37 Documented operating procedures

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive Corrective	• Confidentiality • Integrity • Availability	• Protect • Recover	• Asset Management • Physical Security • System And Network Security • Application Security • Secure Configuration • Identity And Access Management • Threat And Vulnerability Management • Continuity • Information Security Event Management	• Governance and Ecosystem • Protection • Defence

- Operations shall ensure that all relevant documentation including software details is obtained from manufacturer/vendor/supplier
- Following documents will be made available to the relevant people manning the operations:
  - Operations and Maintenance procedure or standard operating procedure (SOP) for all operational activities including security requirements
  - Network diagrams to be maintained, and
  - Product and user manuals

8.3 People Controls

8.3.1 Screening

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Human Resource Security	• Governance and Ecosystem

- Background verification checks shall be performed on all candidates considered for employment, in accordance with relevant laws, regulations and ethics
    - The background verification checks process should ensure that all personal information is kept confidential, and the privacy of the prospective employees' data is maintained in line with the Section 7.2.34 "Privacy and Protection of PII"
    - The organisation shall ensure that competent personnel are employed for performing duties assigned to them

8.3.2 Terms and Conditions of employment

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Human Resource Security	• Governance and Ecosystem

- The terms and conditions of employment, signed by Finolex' s employees shall include the employee's responsibilities for information security and related obligations, both during and after employment
- All employees handling or accessing organizations information assets shall be liable for protecting the asset against unauthorized disclosure, modification and/ or destruction of information

8.3.3 Information security awareness, education, and training

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Human Resource Security	• Governance and Ecosystem

- All employees shall be provided appropriate awareness training and regular updates in organizational policies and procedures
- The initial security training and awareness program shall be conducted as part of the induction process, and
- The learning and development function shall conduct information security sessions for all the employees joining Finolex. Further, a refresher training shall be conducted for all employees

8.3.4 Disciplinary Process

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains

Preventive Corrective	• Confidentiality • Integrity • Availability	• Protect • Respond	• Human Resource Security	• Governance and Ecosystem

- The organization shall ensure that a comprehensive disciplinary process is in place to handle all kind of security breaches and cases of misconduct. The disciplinary procedure shall be applicable to all employees and be enforced in event of an information security breach

8.3.5 Responsibilities after termination or change of employment

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Human Resource Security • Asset Management	• Governance and Ecosystem

- The responsibilities for performing employment termination and/or change of employment shall be defined, documented, and clearly communicated. The respective Function Head shall sign off the exit letter for the employee exiting the organization
- Employment agreement shall include the duties and responsibilities that shall be valid after the termination of such contract or agreement
- Upon termination, all assets issued by Finolex to the employee shall be taken back and access rights on Finolex' s information assets be removed
- In the case of change of employment, the access rights and/or privileges granted to employees shall be formally reviewed and accordingly adjusted, and
- The academic or professional qualification certificates/records from the employee will be retained for a period of three years post the last working date

8.3.6 Confidentiality or Non-Disclosure Agreements

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality	• Protect	• Human Resource Security • Information Protection • Supplier Relationship	• Governance and Ecosystem

- Non-disclosure agreements shall be defined, implemented, and maintained to address organization's information confidentiality/ non-disclosure requirements
- All employees shall sign and comply with the non-disclosure agreement maintained by the Human Resource Team
- All external consultants or the entity providing these services shall sign and comply with a non-disclosure agreement prior to any access to critical assets

8.3.7 Remote Working

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Asset Management • Information Protection • Physical Security • System and Network Security	• Protection

- Employees shall be allowed to remotely connect to the organisation's network/application using mobile devices (such as organisation issued laptops) to access the business information, only after successful identification and authentication.
- A secure communication channel between the remote user and the networks/Application of the organisation shall be provided

8.3.8 Information security event reporting

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Detective	• Confidentiality • Integrity • Availability	• Detect	• Information Security Event Management	• Defence

- Information Security events shall be reported through appropriate management channels as quickly as possible
- Different channels such as email and phone line shall be implemented to facilitate reporting of Information Security event. All information security events will be logged in an information security incident tracker
- Facility for monitoring (like Security Operations Centre) shall be setup for proactive monitoring of intrusions, attacks, and frauds
- Users/Employees shall be educated on how to identify and report Information Security events

(For more details, please refer to Human Resource Security Policy)

8.4 Physical Controls

8.4.1 Physical Security Perimeters

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Physical Security	• Protection

- Security controls, such as perimeter fencing, entry control and manned reception desk, shall be used to protect areas that contain information and information processing facilities. The facility department should carry out the following activities to ensure physical security of the facility:

- Identify and define perimeter of the facility
- Ensure that doors to public zones are equipped with the locking devices
- Deploy security personnel on round-the-clock basis

- Combustible materials should be stored safely at a safe distance from secure areas
- The Finolex offices shall be logically divided into different zones. Each zone shall have appropriate level of access restrictions and access authorization requirements. Areas containing critical IT equipment (such as the network room and the data centres) shall be designated as high security zones

8.4.2 Physical entry

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Physical Security • Identity and Access Management	• Protection

- Offices, buildings, and facilities should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Following controls should be implemented to ensure access to authorized personnel:
  - The facility department should issue badges for employees of Finolex and visitors. The badges issued should help in clear identification and differentiation between employee and visitor
  - Deploying security guards round the clock
  - Maintenance of entry / exit register for visitors
  - Requirement for personnel to wear visible identification badge
  - Declaration of belongings such as Laptop, personal devices like pen drive, hard disk, etc. at entry gate
- All floor and office premises shall be accessed by using valid electronic card/access card which is issued by security team/IT team
- Visitor or other third-party access to Finolex facility containing sensitive information shall be controlled by proper access controls, guards, receptionists, or other front office staff
- Inventory of all types of visitor passes / badges should be maintained at security gate and all visitor passes / badges shall be verified on the daily basis against the inventory issued and received. Any discrepancy needs to be communicated to respective Business head

8.4.3 Securing offices, rooms, and facilities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Physical Security • Asset Management	• Protection

- Security personnel should check all Finolex required rooms and facilities are locked after office hours

- Facility department should ensure that photocopiers, printers, fax machines are located outside the secure area
- Employees should ensure that they lock their cabins before they leave office
- IT team shall ensure that any network switches and cabling racks/ distribution points in the office area are not physically accessible to people other than IT team
- CCTV surveillance system shall store recordings as per regulatory and legal requirement in secure areas entry and exit points
- Fire drill / earthquake drills and training shall be provided to employees on periodic intervals
- Fire drill record shall be maintained with the respective business departments. The records shall include time taken in evacuations of the building, learnings, etc. from the drill

8.4.4 Physical Security Monitoring

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive Detective	• Confidentiality • Integrity • Availability	• Protect • Detect	• Physical Security	• Protection • Defence

- CCTV Cameras shall be installed to view and record access to the sensitive areas within and outside Finolex premises
- Monitoring systems should be protected from unauthorized access to prevent surveillance information, such as video feeds, from being accessed by unauthorized persons or systems being disabled remotely
- Any monitoring and recording mechanism should be used taking into consideration local laws and regulations including data protection and PII protection legislation, especially regarding the monitoring of personnel and recorded video retention periods

8.4.5 Protecting against physical and environmental threats

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Physical Security	• Protection

- Finolex shall ensure that critical information processing facilities are appropriately equipped and maintained with security controls to safeguard against external and environmental threats
- Data center/ Hub room/ server room shall have proper/enough illumination to restrict any unauthorized access
- Doors/ windows of server room/hub room/data center shall not be transparent
- No water line/pipeline shall be through adjoining server room/ hub room/ data cater

8.4.6 Working in secure areas

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity	• Protect	• Physical Security	• Protection

	• Availability			

Finolex shall ensure that:

- Employees and third-party resources shall be aware of the existence of, or activities within a secure area on a need to- know basis
- All areas within its facilities shall be supervised to avoid safety breaches and to prevent opportunities for malicious activities
- Vacant secure areas shall be physically locked and periodically reviewed

8.4.7 Clear desk and clear screen

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality	• Protect	• Physical Security	• Protection

- A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted
- All confidential information shall be kept in a secure office or other location e.g., storage in a locked drawer, file cabinet etc.
- All incoming and outgoing mail points and unattended facsimile machines shall be protected from unauthorized physical and logical access
- Personal computers, laptops and printers shall be left logged off or protected by a password, token, or similar user authentication mechanism when unattended
- Application sessions shall be locked after 30 minutes of inactivity until a user's password is re-entered
- Users shall log off or lock their systems when leaving it unattended for any period

8.4.8 Equipment siting and protection

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Physical Security • Asset Management	• Protection

Equipment needs to be sited and protected to reduce the risks from environmental threats and hazards, and against unauthorized access. The siting of equipment will be determined by several factors including the size and nature of the equipment, it's proposed use and accessibility and environmental requirements.

- All elements of systems including but not limited to servers, firewalls, hubs, routers etc. shall be physically located within a secure area
- All equipment shall be sited to reduce the risk and opportunities for unnecessary and unauthorized access into work areas
- Information processing facilities (laptops, desktops etc.) handling sensitive data should be protected using screen protectors to reduce the risk of information being viewed by unauthorized persons during their use

- Information processing facilities like laptops are sited so they are securely stored when not in use and easily accessed when required

8.4.9 Security of assets off-premises

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Physical Security • Asset Management	• Protection

Security controls need to be applied to off-site assets, considering the different risks involved while working outside the Finolex' s premises.

Finolex shall ensure that:

- Any use of equipment or assets for information processing outside Finolex premises shall require authorization by Business head in consultation with Information Security Head. Authorization for issue of mobile computing devices (includes laptops & smart phones) shall be considered as an authorization for use of equipment and assets for information processing outside Finolex premises
- Employees shall store mobile and other hardware devices sensibly and securely when storing outside Finolex' s premises e.g., hotels, airports, etc. Equipment shall not be left unlocked, logged in or powered up without the employee being with the equipment
- While traveling on road via taxi/ own car the employees are requested to secure office belongings, laptop etc. in car boot space

8.4.10 Storage Media

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Physical Security • Asset Management	• Protection

- Finolex shall ensure authorized disclosure, modification, removal, or destruction of information on storage media
- Procedures for the secure reuse or disposal of storage media shall be established to minimize the risk of confidential information leakage to unauthorized persons. The procedures for secure reuse or disposal of storage media containing confidential information should be proportional to the sensitivity of that information
- When confidential information on storage media is not encrypted, additional physical protection of the storage media should be considered

8.4.11 Supporting Utilities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains

Preventive Detective	• Integrity • Availability	• Protect • Detect	• Physical Security	• Protection

Equipment needs to be protected from power failures and other disruptions caused by failures in supporting utilities. For example, risks related to failing or faulty power supplies should be assessed and considered. This might include dual power supplies from different sub-stations; backup power generation facilities; regular testing of power provision and management, etc.

Finolex shall ensure that:

- All servers and network equipment shall be fitted with uninterruptible power supply systems, electrical power filters or surge suppressors that have been approved
- All Finolex multi-user systems and communications facilities shall have alternative source of power, such a generator sets etc., so that normal business operations are sustainable even during extended period of unavailability of main power supply

8.4.12 Cabling Security

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Availability	• Protect	• Physical Security	• Protection

Finolex shall ensure that:

- Power and telecommunications cabling carrying data supporting information services shall be protected from interception or damage
- Cabling shall be physically protected from unauthorized interception or damage, for example by using a conduit or by avoiding routes through public areas
- Power cables should be segregated from communications cables to prevent interference
- Cables should be protected using electromagnetic shield
- Clearly identifiable cable and equipment markings should be used to minimize handling errors, such as accidental patching of wrong network cables
- Installation of cables should be in such a way that it is not easily accessible
- Shielded twisted pair (STP) cables should be used instead of unshielded twisted pair (UTP)

8.4.13 Equipment Maintenance

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Physical Security • Asset Management	• Protection • Resilience

Finolex shall ensure that:

- All information systems equipment used for production processing shall be maintained in accordance with the supplier's recommended service intervals and specifications, with any repairs and servicing performed only by qualified and authorized maintenance personnel
- All hardware and software products shall be registered with the appropriate vendors for maintenance after Finolex staff takes delivery of new or upgraded information systems products

- The annual maintenance contracts for all hardware and software products, if applicable, shall be monitored and reviewed after every year
- Preventive maintenance shall be done and reviewed by relevant Business heads or Information Security Head on predefined periods

8.4.14 Secure disposal or re-use of equipment

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality	• Protect	• Physical Security • Asset Management	• Protection

All items of equipment including storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Finolex shall ensure that:

- Equipment shall be disposed (transferred or scrapped) if:
  - The equipment has reached end of life
  - The equipment does not suit the computing environment requirement and cannot be upgraded further to meet the same
  - Equipment has gone faulty and cannot be repaired
- Critical infrastructure equipment which needs to be disposed, such as servers, network, security equipment etc. shall be approved with valid justification by Information Security Head. Exceptions to the same can be implemented based on the management approval
- Any information that resides in the asset shall be removed from the equipment before disposal/transfer/scrapping
- The list of equipment, which are being disposed, shall be removed, or deleted from asset list as well as from register books, if any
- List of equipment disposed/ transferred/ scrapped shall be maintained separately by the IT team
- Controls implemented to wipe information shall be commensurate with the classification of information on the storage media / systems
- Media containing confidential or sensitive data that should no longer be retained must be disposed of in a secure and safe manner as noted below:
  - Hard disks: physical destroy, disk sanitization or shred platter
  - Floppy disks: disintegrate, shred or melt, etc.
  - Tape media: demagnetize, shred, melt, etc.
  - USB drives and digital media: crush, melt, shred, etc.
  - Optical disks (CDs and DVDs): destroy optical surface, crush, shred, or melt, etc.

(For more details, please refer to Physical Security and Environmental Security Policy)

- Information or data shall be erased from equipment prior to disposal or re-use
- Equipment shall be disposed in an environmentally sensitive manner, taking account of any recycling facilities provided by manufacturers, local authorities, or commercial organizations

8.5 Technological Controls

8.5.1 User endpoint devices

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Asset Management • Information Protection	• Protection

- Finolex shall establish secure configuration and handling of user endpoint devices
- All users should be made aware of the security requirements and procedures for protecting user endpoint devices, as well as of their responsibilities for implementing such security measures
- A specific procedure considering legal, statutory, regulatory, contractual (including insurance) and other security requirements of Finolex should be established for cases of theft or loss of user endpoint devices
- For the use of personal devices (BYOD) the personal usage and business use of the devices shall be segregated using end point device management tools to protect Finolex data on a private device
- All software and operating systems on endpoints shall be updated with the latest security patches to address known vulnerabilities
- A list of approved and unapproved applications should be maintained to control which applications can run on endpoints, thereby preventing the execution of malicious software
- Finolex should enforce policies to regulate the use of external devices (e.g., USB drives, external hard drives) to prevent data leakage and the introduction of malware
- Data stored on endpoints shall be encrypted to protect sensitive information from unauthorized access, especially in case of theft or loss of the device
- Strong authentication mechanisms (e.g., multi-factor authentication) and granular access controls should be implemented to ensure that only authorized users can access endpoints and sensitive data
- Regular backup shall be maintained to ensure that critical data can be recovered in case of a security incident or system failure

8.5.2 Privileged Access Rights

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Identity and Access Management • Information Protection	• Protection

The allocation and use of privileged access rights shall be restricted and controlled over Finolex systems and networks. The below mentioned points should be taken into considerations:

- Respective Business head shall approve privilege access rights for Finolex employees and notify the same to IT team

- The Finolex system privileges of all users, systems, etc will be restricted based on the need to know
- By default, all users shall be granted basic information systems services such as electronic mail, etc.
- All other system capabilities shall be provided through job profiles or by special request approved by the IT team in consultation with Business head, and
- The privileges for non Finolex employees shall be revoked immediately by the IT team when the requirement or the contract is over

8.5.3 Information Access restrictions

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Identity and Access Management • Information Protection	• Protection

Access to Finolex information shall be tied to access control policy. Key considerations should include:

- Role-based access control
- Levels of access
- Read, write, delete, and execute permissions
- Limiting output of information, and
- Physical and/or logical access controls to sensitive applications, data, and systems

8.5.4 Access to source code

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Identity and Access Management • Application Security • Secure Configuration	• Protection

- Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) shall be controlled, to prevent the introduction of unauthorized functionality and to avoid unintentional changes
- Where possible, program source libraries should not be kept in production systems
- Support personnel should not have unrestricted access to program source libraries, and
- Relevant audit trails shall be maintained for accesses and changes to program source libraries

8.5.5 Secure Authentication

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains

Preventive	• Confidentiality • Integrity • Availability	• Protect	• Identity and Access Management	• Protection

Secret authentication information is a gateway to access valuable assets. It typically includes passwords, encryption keys etc. the allocation of secret authentication information shall be controlled through a formal management process.

- Passwords used by the Finolex employees and those set/provisioned on systems, network devices shall meet complexity requirements
- Users shall be educated to keep the passwords allocated to them confidential
- When granting access to infrastructure or software(s), users shall be provided with a temporary or one-time password that meets the password complexity requirements. Users need to change this password at first login and shall be unique for each user, and
- Temporary passwords should be given to users in a secure manner such as through restricted emails to intended user

8.5.6 Capacity Management

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive Detective	• Integrity • Availability	• Identify • Protect • Detect	• Continuity	• Governance and Ecosystem • Protection

- Capacity management shall help identify and reduce inefficiencies associated with either under-utilized resources or customer demands not fulfilled and shall provide satisfactory service levels in a cost-efficient manner. This shall help ensure that all infrastructure components can perform all required functions, those components shall perform as efficiently as possible, and accommodate reasonable growth without being overly wasteful
- Critical IT resources related to each of the business processes, which need to be provided with maximum availability, shall be identified by Management Committee. These can be:
  - Business Critical application(s)
  - Operating systems
  - Databases
  - Hardware (servers, PCs, storage devices)
  - Networking components (routers, switches, firewalls)
  - Data files
  - Network Connectivity
- Critical parameters and their thresholds shall be monitored for all critical infrastructure elements and software(s) at periodic intervals to ensure required performance levels and availability
- Capacity planning shall take account of new business and system requirements and current and projected trends in the organization's information processing capabilities
- The periodicity of capacity review shall be defined taking into consideration the criticality of the infrastructure element, lead time / costs to procure replacement, and the parameter being monitored

- System tuning and monitoring shall be applied to ensure and, where necessary, improve the availability and efficiency of systems. Detective controls should be put in place to indicate problems in due time
- Outcome of the monitoring activity shall:
  - Be used to take corrective actions (if required)
  - Help in root cause analysis (if required)
  - Be used to make projections of future capacity requirements to reduce the risk of system overload

8.5.7 Protection against malware

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive Detective	• Integrity • Availability	• Identify • Protect • Detect	• Continuity	• Governance and Ecosystem • Protection

- Anti-malware tools shall be implemented to efficiently detect, prevent, and recover against Malwares
- Appropriate protection shall be enforced so that the users cannot disable the Anti-virus check
- Anti-virus software installed on gateway antivirus server and associated signature files and virus definitions shall be kept up to date
- Use of unauthorized software shall be prohibited
- E-mails, attachments, system files, download, and all removable media such as USB drives, or CD-ROMs shall be scanned and quarantined for malicious code before use
- The auto run feature of CD, DVD or any other removable media shall be disabled on all systems
- Updated and approved versions of anti-virus on windows systems, system firewalls, host Intrusion Prevention system/ intrusion detection system, scanning engines and other software shall be deployed. Signatures and virus-definitions of all such deployments shall be kept appropriately current
- Controls shall be implemented to prevent malware files from being introduced into the organization's infrastructure from external networks like Internet
- Appropriate incident management process shall be put in place to recover from malicious code attacks
- Malicious code incidents shall be reported and be dealt as per the Incident Management Procedure
- Users shall report the results of virus scanning and removal activity to the system administrators
- Any machine discovered to be infected by a virus shall immediately be disconnected from all networks. The machine shall not be reconnected to the network until IT system administration staff can verify that the virus has been removed, and
- Users and staff shall be educated and made aware of the dangers of malicious code and protection measures to be adhered

8.5.8 Management of Technical Vulnerabilities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify • Protect	• Threat and Vulnerability Management	• Governance and Ecosystem • Protection • Defence

- There shall be documented procedure for technical vulnerability management
- Timely information about technical vulnerabilities in infrastructure elements and software(s) being used shall be obtained from trusted sources (e.g., through subscription to vendor security advisories)
- Timelines shall be defined for responding to identified / reported technical vulnerabilities
- Information obtained regarding vulnerability shall be evaluated to assess risk to Finolex' s infrastructure. The evaluation shall take into consideration:
  - Vendor reported criticality (e.g., high, medium, and low)
  - Likelihood of the vulnerability being exploited (e.g., existence of a known exploit or other malicious code that uses the vulnerability as an attack vector)
  - System criticality (e.g., the relative importance of the applications and data the system supports at Finolex), and
  - System exposure (e.g., proxy server vs. internal file server vs. application servers)
- The identified risk shall be categorized as per the severity of the risk (e.g., High, Medium, and Low)
- Appropriate measures shall be taken to address the associated risks. If the vulnerability cannot be addressed, controls shall be considered to reduce the impact of risk
- If the vulnerability closure requires patch deployment, the patch must be tested in a test environment before deployment to production environment. The test environment should closely simulate the production environment and if possible, the test should verify the patch does not conflict with other software(s). The patch deployment must go through change management process with a rollback plan
- The system should be checked to verify if the patch has not affected any of the existing functionality
- For high-risk vulnerabilities, after applying the patch/solution, a check shall be performed to ensure that the vulnerability has been closed, and
- To assist with technical vulnerability management, inventory of Infrastructure elements and software assets shall be maintained

(For more details, please refer to Vulnerability Assessment and Penetration Testing Policy)

8.5.9 Configuration Management

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Secure Configuration	• Protection

- Finolex shall define and implement processes and tools to enforce the defined configurations (including security configurations) for hardware, software, services (e.g., cloud services) and networks, for newly installed systems as well as for operational systems over their lifetime

- Roles, responsibilities, and procedures should be in place to ensure satisfactory control of all configuration changes
- Established configurations of hardware, software, services, and networks should be recorded and a log should be maintained of all configuration changes
- Changes to configurations should follow the change management process

8.5.10 Information Deletion

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality	• Protect	• Information Protection • Legal and Compliance	• Protection

- Sensitive information should not be kept for longer than it is required to reduce the risk of undesirable disclosure
- A secure deletion method like degaussing or physical destruction shall be selected in accordance with the business requirements and taking into consideration relevant laws and regulations
- A secure data destruction mechanism shall be implemented for the deletion of sensitive information, including chat logs.
- Where cloud services are used, Information Security Head should verify if the deletion method provided by the cloud service provider is acceptable, and if it is the case, Finolex should use it, or request that the cloud service provider delete the information

8.5.11 Data Masking

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality	• Protect	• Information Protection	• Protection

- While dealing with sensitive data or Personally Identifiable Data Finolex shall hide such data by using techniques such as data masking, pseudonymization or anonymization
- Hash functions can be used to anonymize PII. To prevent enumeration attacks, they should always be combined with a salt function

8.5.12 Data Leakage Prevention

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive Detective	• Confidentiality	• Protect • Detect	• Information Protection	• Protection • Defence

- Finolex shall:
  - identify and classify information to protect against leakage (e.g., personal information, pricing models and shoe designs)
  - monitor channels of data leakage (e.g., email, file transfers, mobile devices, and portable storage devices)

- act to prevent information from leaking (e.g., quarantine emails containing sensitive information)

- Where data is backed up, care should be taken to ensure sensitive information is protected using measures such as encryption, access control and physical protection of the storage media holding the backup

8.5.13 Information Backup

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Corrective	• Integrity • Availability	• Recover	• Continuity	• Protection

- Backup solution shall be used to meet the business requirements and ensure availability of business-critical information, software(s), device configurations in case of emergencies
- Relevant processes / procedures shall be created and followed to meet the business requirements. The process / procedures will cover:
  - Frequency for taking backup and testing of backup through a restoration process.
  - Data to be backed up
  - Type of backup (incremental, differential, full)
  - Root Cause Analysis for such failure would be carried out as per the incident management procedure
  - Instructions to restore in case of an actual disaster, and
  - Retention period for backup
- Adequate controls shall be put in place to ensure protection of backup media. The environmental conditions for storing the backup media shall be in line with the specifications on environmental conditions for the backup media
- The backup media shall be labelled to a consistent standard
- Adequate controls shall be put in place to protect the information contained on back up media
- Restoration testing shall be performed on regular basis to ensure effectiveness of backup tools, and
- The restored contents shall be verified against the tape for an exact match

(For more details, please refer to Backup and Restoration Policy)

8.5.14 Redundancy of information processing facilities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Availability	• Protect	• Continuity • Asset Management	• Protection • Resilience

- Finolex shall identify business requirements for availability of information systems
- Redundant components or architectures shall be considered wherever availability cannot be guaranteed using the existing systems architecture
- Redundant information systems shall be tested to ensure the successful failover from one component to another, and
- Adequate redundancy has been provided for network links and network devices

8.5.15 Logging

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Detective	• Confidentiality • Integrity • Availability	• Detect	• Information Security Event Management	• Protection • Defence

- Event logging activity affects information system performance, therefore, decision shall be made upon a risk assessment, to, which events require logging on a continuous basis and which events require logging in response to specific situations. Following minimum events shall be considered but not limited to:
  - Logins and logouts to systems and applications
  - Unsuccessful usage of user identification or authentication mechanisms
  - Access violation and unsuccessful logon attempts
  - Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing high impact file permissions, changing database object permissions and user password changes
  - All system or application administrator actions
  - Application process start-up, shutdown, or restart
  - Application process abort, failure, or abnormal end, faults, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, disk space, or other resources) or hardware fault for critical applications
  - Use of privileged accounts
  - Administrator logons, changes to the administrator group, and account lockouts; and
  - System faults shall be logged in near real-time and corrective action shall be taken immediately by the IT Administrator/IT Team
- IT Team shall ensure that systems are configured in such a way that the system administrator and system operator activities are logged. Event logs shall be captured and stored for administrator activities. It shall also be ensured that system administrator and operator do not edit /delete their logs. Logs shall include but not limited to:
  - The time at which an event (success or failure) occurred
  - Information about the event or failure
  - The user/service account involved

8.5.16 Monitoring activities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Detective	• Confidentiality • Integrity • Availability	• Detect	• Information Security Event Management	• Protection • Defence

- The monitoring scope and level should be determined in accordance with business and information security requirements and taking into consideration relevant laws and regulations. Monitoring records should be maintained for defined retention periods
- The monitoring system should be configured against the established baseline to identify anomalous behavior

8.5.17 Clock Synchronisation

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Detective	• Integrity	• Protect • Detect	• Information Security Event Management	• Protection • Defence

- All systems, application and database servers shall have appropriate time and clock synchronization, wherever feasible. This shall be achieved by configuring a Network Time Protocol (NTP) environment to which all critical component like servers, network etc., shall synchronize time. To secure logs following shall be followed:
  - Access to logs shall be limited to authorized people, for review and analysis
  - Backup of logs shall be taken on periodic basis; for critical system, database, and application the backup shall be taken at least on daily/weekly basis, and
  - Backup tapes or drives on which logs are getting backed up shall be secured against any unauthorized access

(For further details please refer to Logging & Monitoring policy)

8.5.18 Use of privileged utility programs

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• System and network security • Secure configuration • Application security	• Protection

- Access to Finolex' s local system control utilities shall be restricted and controlled
- These system utilities shall be installed on local systems and shall be intended for use by IT to assist in resolving problems, and
- Remote control utilities for IT team personnel shall only be used after the IT team has informed the user of this capability and has received permission from the user to use them

8.5.19 Installation of software on operational systems

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Secure configuration • Application security	• Protection

- Installation of new software and changes to existing software on production systems shall be in line with change management policy to ensure:
  - Changes are authorized and made by authorized personnel only
  - Production systems hold only approved code and not development code

- Implementation happens only after required level of testing
- System documentation is updated, and
- Roll back plan is available

- The risks of relying on unsupported software (software for which support has been ceased by the vendor) for business-critical applications shall be considered

8.5.20 Network security

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive Detective	• Confidentiality • Integrity • Availability	• Protect • Detect	• System and network security	• Protection

- Networks shall be adequately managed and controlled, to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit
- Network based intrusion prevention/detection system shall be deployed to cover critical network segments within IT infrastructure as per the risks identified
- Infrastructure elements and software(s) exposed to un-trusted or semi trusted networks/users (e.g., Internet facing systems, distributors, call centers, s etc.) shall be adequately protected by firewalls, intrusion prevention systems (IPSs), and limited connectivity
- All internet facing systems shall be treated as semi-trusted systems
- Any system deployed on the Internet must go through a thorough vulnerability check. All identified vulnerabilities must be closed or mitigated before the system is deployed on the Internet
- All end user systems connecting to the Finolex' s infrastructure must be hardened, patched, and installed with updated anti-malware software
- Every connection to an external network terminated at a firewall
- Firewalls do not have any rules that permit 'any' network, sub network, host, protocol, or port on any of the firewall
- The firewall rule base treated as a sensitive information and is knowledge of the same restricted only to authorized officials in the IT team

8.5.21 Security of Network services

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• System and network security	• Protection

- The servers shall be implemented for a single primary function, wherever possible. This shall simplify configuration, thereby reducing the risk of configuration errors. In some cases, however, it may be appropriate to offer more than one service on a single host computer (e.g., database, DNS (Domain Name System), FTP (File Transfer Protocol) and HTTP (Hyper Text Transfer Protocol) services)

- All network servers shall be protected using strong passwords, and the passwords shall be managed as defined in the password policy of Finolex
- The appropriate authority shall assess the security risks associated with enabling a network service to arrive at the security requirements
- Any unused or unwanted network services shall be removed or disabled as per the relevant hardening documents
- A documented list of services and ports required for the business purpose shall be maintained and updated regularly
- If the business requires any services or ports to be enabled, they shall be enabled only after authorization and testing and implementation of mitigating controls to avoid misuse

8.5.22 Segregation of Networks

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• System and network security	• Protection

- Group of users, systems, applications shall be adequately segregated through creation of Virtual LANs, Zones based to prevent unauthorized access, and
- Appropriate logical segregation shall be done and Physical Security infrastructures through creation of zones. Traffic flows between different zones shall be documented

8.5.23 Web filtering

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• System and network security	• Protection

- Finolex shall reduce the risks of its personnel accessing websites that contain illegal information or are known to contain viruses or phishing material
- Finolex shall identify the types of websites to which personnel should or should not have access. Finolex shall block access to the following types of websites:
  - websites that have an information upload function unless permitted for valid business reasons
  - known or suspected malicious websites (e.g., those distributing malware or phishing contents)
  - command and control servers
  - malicious website acquired from threat intelligence
  - websites sharing illegal content
- The IP addresses or domains of such malicious websites shall be blocked by the anti-malware

(For further details please refer to Network Security policy)

8.5.24 Use of cryptography

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Secure configuration	• Protection

- Encryption shall be adopted for information assets based on the criticality of information. Standard encryption technology would be deployed for encryption unless required by regulatory requirements
- Users shall not employ encryption, digital signatures, or digital certificates for any business activity or business information without the written authorization of their department manager in consultation with Information Security Head, the completion of proper training and having their systems configured by authorized personnel
- Cryptographic algorithms shall be patched against any known technical vulnerabilities
- Encryption shall be used for transportation of information by mobile devices and removable media devices or across communication lines
- Key strength used shall be enough to prevent attacks targeted to breaking the cryptographic key (e.g., brute force attack on the cryptographic key)
- Roles and responsibilities shall be defined for key management and implementation of policy

Key management that involves the generation, creation, protection, storage, exchange, replacement and use of keys deals with many types of security liabilities beyond encryption, such as people and flawed policies. To mitigate such scenarios, the following standards need to be kept in mind when working with keys (wherever applicable):

- The secret key shall be secured by logically and physically securing the device on which the key is stored. Wherever possible, a Hardware Security Module (HSM) should be used to store the key
- The shared secret key shall be accessible only by authorized personnel on a need-to-know basis
- Keys shall be revoked and generated afresh in case of suspected compromise
- Audit trails of key management activities shall be stored and protected
- Internal Certification Authority systems shall be managed securely with appropriate physical and logical controls
- Backed up keys shall be protected from physical and environmental threats
- Cryptographic keys shall be destroyed in a secure manner when they are no longer required for both hardware and software keys
  (For further details please refer to Encryption and Cryptography Policy)

8.5.25 Secure Development Lifecycle

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Application Security • System and Network Security	• Protection

- Secure development Policy shall be documented

- Secure development environment for development of software and systems
- Access to this environment shall be restricted and monitored
- The devices shall be hardened to protect against exploitation
- A secure development environment consists of people, process, and technology associated with system development and integration efforts that cover the entire secure development lifecycle. Finolex shall assess the risk considering the following but not limited to:
    - The sensitivity of the data to be processed, stored, and transmitted by the system
    - Applicable external and internal requirements
    - Security policies already implemented by Finolex that support system development
    - The trustworthiness of the personnel working in the environment
    - The degree of outsourcing associated with system development
    - The need for segregation between different development environments
    - Control of access to the development environment
    - Monitoring of the change to the environment and the code stored within
    - Backups are stored at secure offsite locations, and
    - Control over the movement of data from development to the production environment

8.5.26 Application Security Requirements

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Application Security • System and Network Security	• Protection

- Finolex shall ensure all information security requirements are identified and addressed when developing or acquiring applications
- Application security requirements should be identified and specified
- These requirements shall be determined through a risk assessment
- Application security requirements should include, as applicable:
    - level of trust in identity of entities [e.g., through authentication]
    - identifying the type of information and classification level to be processed by the application
    - need for segregation of access and level of access to data and functions in the application
    - resilience against malicious attacks or unintentional disruptions [e.g., protection against buffer overflow or structured query language (SQL) injections]
    - legal, statutory, and regulatory requirements in the jurisdiction where the transaction is generated, processed, completed, or stored
    - need for privacy associated with all parties involved
    - the protection requirements of any confidential information
    - protection of data while being processed, in transit and at rest
    - need to securely encrypt communications between all involved parties
    - input controls, including integrity checks and input validation
    - automated controls (e.g., approval limits or dual approvals)
    - output controls, also considering who can access outputs and its authorization
    - restrictions around content of "free text" fields, as these can lead to uncontrolled storage of confidential data (e.g., personal data)

- requirements derived from the business process, such as transaction logging and monitoring, nonrepudiation requirements
- requirements mandated by other security controls (e.g., interfaces to logging and monitoring or data leakage detection systems)
- error message handling

8.5.27 Secure system architecture and engineering principles

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Application Security • System and Network Security	• Protection

- Secure information system engineering principles shall be designed into all architecture layers:
  - Business layer – e.g., based on user authentication level; only particular users can see personal data
  - Data layer – e.g., only logging in with a strong database password for database maintenance activities is allowed
  - Applications – e.g., application encryption is used for data export and import, and
  - Technology – e.g., open-source software and state-of-the-art hardware and network infrastructure provided by selected vendors are used

8.5.28 Secure coding

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Application Security • System and Network Security	• Protection

- Finolex shall establish organization-wide processes to provide good governance for secure coding. A minimum secure baseline should be established and applied
- Such processes and governance should be extended to cover software components from third parties and open-source software
- Secure coding principles should be used both for new developments and in reuse scenarios
- These principles should be applied to development activities both within the organization and for products and services supplied by the organization to others

8.5.29 Security testing in development and acceptance

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Identify	• Application Security • Information Security Assurance	• Protection

			• System and Network Security	

- Acceptance criteria for new information systems and information processing facilities, upgrades and new versions shall be defined. Appropriate testing of the systems shall be carried out during development before moving to production and
- Security clearance shall be obtained from the application owner and IT Team. Information Security Head shall sign off before any new information systems, upgrades or new versions are accepted

8.5.30 Outsourced development

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive Detective	• Confidentiality • Integrity • Availability	• Identify • Protect • Detect	• Application Security • Information Security Assurance • System and Network Security	• Governance and Ecosystem • Protection

- For the customized software developed by third parties, arrangements pertaining to licensing, legal and regulatory requirements, including data protection, ownership of the entire source code by Finolex, intellectual property rights and copyright, and compliances shall be documented in the contract between Finolex and the third parties
- The contract shall include the right to audit the quality and accuracy of software development and testing. Such software code shall have arrangements in the event of failure of the third party not complying with information security requirements, and
- A Non-Disclosure Agreement (NDA) with Finolex shall be signed by all third-party employees (i.e., third parties, contractors, application developers, testers etc.) having access to Finolex' s resources. The NDA shall mandate that the third-party resources should not disclose any information related to Finolex. The third-party shall ensure that they read, accept, and sign the Non-Disclosure Agreement provided by Finolex

8.5.31 Separation of development, test, and production environments

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Application Security • System and Network Security	• Protection

- Development, test and operational (production) environments shall be separated to reduce the risks of unauthorized access or changes to the operational system
- Test environment should emulate the production environment wherever applicable or as closely or possible; and

- Development tools like compilers, editors shall not be available on production servers

8.5.32 Change Management

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• Application Security • System and Network Security	• Protection

- The scope of change shall be clearly articulated and documented. Changes shall be classified, recorded, validated, approved, and prioritized
- All change requests shall include business benefits, risk assessment, impact analysis and roll back plan details. All accepted change requests shall be tested, verified, and approved before the release
- The change request shall be analyzed by internal IT team or external agency and a detail timeline with cost will be projected for approval. Any major cash outflow for the change request must be approved by the Senior Management Team. Any scheduled change request may be deferred for an indefinite period for reasons of non- availability of adequate resources or if the change impacts any other business process
- Depending upon the nature of the change request, periodic reviews shall be conducted to ensure that the impact of the change is adequately understood and addressed. This will also ensure successful completion of the change request
- A change management log must be maintained for all changes. The log must contain, but is not limited to:
  - Date of submission and date of change
  - Owner contact information
  - Nature of the change
  - Indication of success or failure, and
  - Fall Back Plan (If failure)
- All changes shall be planned, scheduled, and communicated to all respective stakeholders. A review board shall review the changes periodically to assess the trends and improvement areas. The findings of the review board meetings shall be documented and published.
- All procedures and activities will be planned and executed in accordance with the local and/or national regulatory requirements, with appropriate approvals wherever deemed necessary; and
- Wherever external agencies are involved, the relevant Change Request (CR) document shall be raised by the agency will be treated as the final CR document.

(For more details, please refer to Change Management Policy)

8.5.33 Test Information

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity	• Protect	• Information Protection	• Protection

- Test data used shall be treated like the operational data. Operational data shall be sanitized before being used for test purposes. It shall be always ensured that 'Confidential' information is not utilized during testing (if possible).
- Operational information shall be erased from a test environment immediately after the testing is complete.
- Access to test environment shall be given to only those personnel who are involved in testing the entire application only.
- Segregation of duties shall be applied where the knowledge and/or privileges are needed to complete a process and divided among multiple users so that no single one can perform or controlling. The principles that shall be applicable to segregation of duties are but not limited to:
  - Sequential separation, when an activity is broken into steps performed by different persons e.g., development (by development team) and testing (by testers) of an application
  - Individual separation, when at least two persons must approve an activity before it is done e.g., functional lead/ business module lead approval followed by development lead for the finalization of application development feasibility
  - Spatial separation, when different activities are performed in different locations e.g., Teams at various locations working on a common application, and
  - Factorial separation, when several factors contribute to activity completion e.g., two-factor access authentication
- System integration testing shall be carried out to verify the behavior of the complete system. It shall be tested to conduct on a complete, integrated system to evaluate the system's compliance with its specified requirement
- System integration testing (SIT) shall be performed to verify the interactions between the modules of a software system. It shall deal with the verification of the high and low-level software requirements specified in the Software Requirements Specification/Data and the Software Design Document
- User acceptance testing (UAT) shall be performed by the end user to verify/accept the software system before moving the software application to the production environment. UAT shall be done in the final phase of testing after functional, integration and system testing are done, and
- This testing shall play an important role in validating if all the business requirements are fulfilled before releasing the final software product. The use of live data and real use cases shall make this testing an important part of the release cycle

8.5.34 Protection of Information Systems during audit testing

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	• Confidentiality • Integrity • Availability	• Protect	• System and network security • Information Protection	• Governance and Ecosystem • Protection

- Relevant precautions shall be taken to protect the Information Systems and data from damage or disruptions because of the audit. The following guidelines shall be observed:
  - Agreeing audit requests for access to systems and data with appropriate management

- agreeing and controlling the scope of technical audit tests
- Limiting audit tests to read-only access to software and data. If read-only access is not available to obtain the necessary information, executing the test by an experienced administrator who has the necessary access rights on behalf of the auditor
- If access is granted, establishing, and verifying the security requirements (e.g., antivirus and patching) of the devices used for accessing the systems (e.g., laptops or tablets) before allowing the access
- only allowing access other than read-only for isolated copies of system files, deleting them when the audit is completed, or giving them appropriate protection if there is an obligation to keep such files under audit documentation requirements
- identifying and agreeing on requests for special or additional processing, such as running audit tools
- running audit tests that can affect system availability outside business hours
- monitoring and logging all access for audit and test purposes