Document ID:	Owner:	Document Type:	Language:	Version:
POL-001	Vaishnavi Deshpande	Policy	EN	<1.0>

Title:

INFORMATION SECURITY POLICY

Status:	Name:	Function:	Date:	Signature:
Created	Vaishnavi Deshpande	Policy	10-01-2025	vdeshpande
Reviewed				
Approved				

Table of Contents

1. PURPOSE

The purpose of this Information Security Policy is to establish rules for protecting the confidentiality, integrity, and availability of the organization's information assets. This policy provides the highest level of authority in guiding the establishment, implementation, maintenance, and continuous improvement of the Information Security Management System (ISMS).

2. SCOPE

This policy applies to all members of the organization as defined in the scope of the ISMS. If applicable, add external entities, such as suppliers, service providers, etc.

3. TERMS AND DEFINITIONS

Information Security
The preservation of confidentiality, integrity, and availability of information.

Confidentiality
The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity
The property of accuracy and completeness.

Availability
The property of being accessible and usable upon demand by an authorized entity.

ISMS
Information security management system

CISO
Chief Information Security Officer

4. RELATED DOCUMENTS

The following documents support the purpose of this policy:

- Scope of the ISMS
- Statement of Applicability (SoA)

5. ROLES & RESPONSIBILITIES

5.1 Top Management

CISO is committed to ensure the protection of all information assets in the scope of the ISMS from unauthorized disclosure, alteration and loss of availability. For that reason, the provisioning of sufficient resources to support these efforts is guaranteed.

Information Security Officer (ISO) is aware of the ever-evolving threat landscape and recognizes the need to constantly adapt to arising challenges to keep information assets secure. This circumstance requires the continual improvement of all activities within the scope of the ISMS.

5.2 Chief Information Security Officer

The **Chief Information Security Officer (CISO)** is responsible for overseeing and ensuring the organization's information security management systems delivers its intended results.

The CISO's primary duties include:

- Strategic Leadership: Develop and maintain the organization's information security strategy, aligning it with business goals and regulatory requirements.
- Policy Development: Establish, review, and enforce information security policies and procedures to protect the organization's information assets and ensure compliance with relevant laws and regulations.
- Risk Management: Identify, assess, and mitigate information security risks across the organization. This includes performing regular risk assessments and maintaining a risk management framework.
- Incident Response: Lead the development and implementation of incident response plans. Oversee investigations into security breaches and ensure proper response and recovery procedures are followed.

- Compliance Oversight: Ensure adherence to relevant legal, regulatory, and industry standards. Facilitate audits and assessments to demonstrate compliance with internal and external requirements.
- Security Awareness: Promote information security awareness and training programs to ensure all employees understand their role in protecting the organization's information assets.
- Stakeholder Communication: Serve as the primary point of contact for information security matters. Communicate security issues and status to the executive team, board of directors, and other stakeholders as appropriate.
- Resource Management: Allocate resources effectively to support the information security program. Manage the information security team and collaborate with other departments to integrate security practices throughout the organization.

The **CISO** has the authority to:

- Access Information: Obtain access to all necessary information and resources required to perform information security functions.
- Enforce Policies: Implement and enforce information security policies and procedures across the organization.
- Allocate Resources: Make recommendations for the allocation of budget and resources necessary for the information security program.
- Engage Third Parties: Engage with third-party vendors, consultants, and other external entities as needed to support information security initiatives.

5.3 Information Security Officer

The **Information Security Officer (ISO)** is supporting the **Chief Information Security Officer (CISO)** in fulfilling its duties.

Key responsibilities include:

Please pick the appropriate responsibilities and authority of the Information Security Officer

- Policy Implementation: Assist in the development and enforcement of information security policies and procedures.
- Risk Assessments: Conduct regular risk assessments to identify and mitigate security vulnerabilities.

- Incident Response: Coordinate and support the response to security incidents and breaches.
- Compliance: Ensure adherence to relevant security standards and regulations.
- Awareness Training: Promote information security awareness and training programs across the organization.
- Collaboration: Work with various departments to integrate security practices into organizational processes.

The **ISO** is granted the authority to:

- Access Information: Obtain access to all necessary information and resources required to perform security functions.
- Enforce Security Measures: Implement and enforce information security controls and measures.
- Engage with External Entities: Collaborate with third-party vendors, consultants, and external entities to support the information security program.
- Recommend Resources: Make recommendations for the allocation of resources and budget necessary to maintain the security program.

6. POLICY

6.1 Commitment

Our organization is committed to maintaining the highest standards of information security by complying with all applicable legal, regulatory, and contractual requirements related to the protection of information assets. We pledge to continuously monitor and review our security practices to ensure they meet or exceed the requirements set forth by relevant standards and regulations. This commitment extends to all employees, partners, and stakeholders, who are expected to adhere to our information security policies and procedures, ensuring the confidentiality, integrity, and availability of our information assets are always protected.

Our organization is committed to supporting and continuously improving our Information Security Management System (ISMS). This commitment includes:

In support of these commitments, our organization will:

- **Establish and Maintain a Comprehensive Information Security Policy:** We will develop, implement, and continually update a set of policies that aligns with industry standards, regulatory requirements, and the organization's strategic objectives.
- **Define and Communicate Security Objectives:** Measurable security objectives will be set to support our strategic goals, with clear communication to all relevant stakeholders to ensure alignment and understanding.
- **Allocate Necessary Resources:** We will provide the financial, technological, and human resources required to effectively implement and sustain our Information Security Management System (ISMS).
- **Enhance Employee Awareness and Training:** All employees will receive ongoing support and training to understand their information security responsibilities and to contribute to a secure working environment.
- **Foster a Culture of Security:** A proactive security culture will be promoted throughout the organization, encouraging all individuals to prioritize and actively participate in the protection of information assets.
- **Commit to Continuous Improvement:** We will regularly review and refine our information security policies, procedures, and controls to ensure their effectiveness and relevance, staying responsive to emerging threats and changes in the regulatory landscape.
- **Implement Robust Risk Management:** A comprehensive risk management framework will be employed to identify, assess, and mitigate information security risks. Appropriate controls will be applied based on regular risk assessments.
- **Ensure Effective Communication:** Open and effective communication channels will be maintained to keep all stakeholders informed about our information security policies, procedures, and any updates or changes.
- **Support Information Security Management Roles:** We will empower relevant management roles by providing the necessary authority, resources, and guidance to ensure they can effectively fulfil their responsibilities in maintaining the security of our information assets.

6.2 Information security objectives

Our organization is committed to maintaining a strong ISMS that supports our business objectives through the following information security objectives.

Reduce Information Security Incidents:

- **Objective**: Decrease the number of information security incidents by 20% within the next 12 months.
- **Measure**: Track the number of reported security incidents and compare them to the previous year's data.
- **Responsible**: Information Security Role
- **Resources**: Incident management tools, training programs.

Improve Employee Awareness and Training:

- **Objective**: Ensure 100% of employees complete mandatory information security awareness training within 6 months.
- **Measure**: Monitor training completion rates and conduct post-training assessments to gauge understanding.
- **Responsible**: HR Role, Information Security Role
- **Resources**: E-learning platforms, training materials.

Enhance Data Protection Measures:

- **Objective**: Implement encryption for all sensitive data at rest and in transit within 12 months.
- **Measure**: Verify encryption implementation through internal audits and technical assessments.
- **Responsible**: IT Role
- **Resources**: Encryption tools, technical support.

Strengthen Access Control Mechanisms:

- **Objective**: Achieve 100% compliance with multi-factor authentication (MFA) for all critical systems within 9 months.
- **Measure**: Audit system access logs and MFA implementation reports.
- **Responsible**: IT Role
- **Resources**: MFA solutions, integration support.

Enhance Vendor Security Management:

- **Objective**: Conduct security assessments for 100% of critical third-party vendors within the next year.
- **Measure**: Track the completion and results of vendor security assessments.
- **Responsible**: Procurement Role, Information Security Role
- **Resources**: Vendor assessment tools, assessment criteria documentation.

Achieve Compliance with Regulatory Requirements:

- **Objective**: Ensure compliance with GDPR (General Data Protection Regulation) requirements within 6 months.
- **Measure**: Conduct GDPR compliance audits and track remediation of identified gaps.
- **Responsible**: Legal Role, Compliance Role
- **Resources**: Legal expertise, compliance checklists.

Improve Incident Response Time:

- **Objective**: Reduce the average incident response time by 30% within 12 months.
- **Measure**: Track and analyze incident response times from detection to resolution.
- **Responsible**: Incident Response Team
- **Resources**: Incident response plans, monitoring tools.

Enhance Security Monitoring and Detection Capabilities:

- **Objective**: Implement advanced threat detection systems across all networks within 6 months.
- **Measure**: Evaluate the effectiveness of detection systems through regular testing and incident tracking.
- **Responsible**: IT Security Role
- **Resources**: SIEM (Security Information and Event Management) tools, monitoring infrastructure.

Increase Backup and Recovery Efficiency:

- **Objective**: Achieve a recovery point objective (RPO) of less than 24 hours for all critical systems within 12 months.
- **Measure**: Test and document backup and recovery procedures to ensure RPO targets are met.
- **Responsible**: IT Role
- **Resources**: Backup solutions, disaster recovery plans.

Enhance Security Culture:

- **Objective**: Foster a culture of security by integrating security practices into daily operations and decision-making processes.
- **Measure**: Conduct regular employee surveys to measure security awareness and engagement.
- **Responsible**: Information Security Role, Management Role
- **Resources**: Security awareness programs, regular communications.

6.3 Communication

The information security policy shall be communicated to all persons within the scope of the ISMS by email and document portal bi-annually, during employee onboarding and during awareness campaigns or Security week.
This policy may not be shared and communicated with external interested parties. If necessary, non-sensitive version of the document can be shared once approval from ISO is granted.

7 COMPLIANCE

7.1 Measurement

The organization will ensure compliance with this policy through various methods, including management reviews, internal and external audits, and feedback from employees and stakeholders.

7.2 Exceptions

Any exception to this policy must be approved by **ISO** in advance. The process for requesting an exception involves submitting a detailed justification, including the reasons for the exception, the potential risks, and the proposed mitigation measures. The **ISO** will thoroughly evaluate the request to ensure that it does not compromise the overall security posture of the organization. Only upon receiving explicit approval from **ISO** will the exception be considered valid and enforceable

7.3 Violations

Members of the organization found to have violated this policy may be subject to disciplinary action. Depending on the severity of the violation, consequences may include mandatory retraining on information security policies, formal reprimands, or suspension.

The organization will thoroughly investigate any suspected policy violations to ensure fairness and accuracy in the disciplinary process.