Standard Operating Procedure (SOP) - Information Security Governance

Document ID: ISG-SOP-002
Effective Date: [22nd Jan 2024]
Version: 1.0
Prepared By: Information Technology Department
Approved By: Senior IT Manager – Sagar Pardeshi

---

1. Purpose

This SOP defines the governance structure and responsibilities for managing information security within the organization. It ensures that security initiatives align with business objectives, legal and regulatory requirements, and risk tolerance levels.

---

2. Scope

This SOP applies to all business units, departments, employees, contractors, vendors, and third parties who access or manage the organization's information assets.

---

3. Objectives

- Establish an effective security governance model.

- Define clear roles and responsibilities for information security.

- Ensure compliance and promote a security-aware culture across the organization and regularly assess and improve the security posture.

---

4. Roles & Responsibilities

Role	Responsibility
Senior IT Manager	Approve information security policies and allocate resources.
IT Manager	Lead security strategy and governance implementation.
	Enforce security controls in their functions.

Role	Responsibility
Employees / Users	Comply with security policies and report incidents.

---

6. Governance Framework

6.1 Policy Management

- Develop, review, and maintain an Information Security Policy and supporting standards.

- Ensure policy approval by senior IT manager.

- Communicate policies across the organization.

6.2 Risk Management

- Conduct periodic Information Security Risk Assessments.

- Identify, analyse, and mitigate security risks.

6.3 Compliance & Audits

- Ensure compliance with applicable standards.

- Conduct internal audits annually.

6.4 Security Awareness & Training

- Run mandatory security awareness sessions for all employees.

- Provide targeted training for high-risk roles (e.g., IT, HR, Finance).

- Maintain attendance and training logs.

6.5 Incident Management

- Investigate and respond to security incidents.

- Report major incidents to senior management and regulators as needed.

6.6 Monitoring & Metrics

- Use security dashboards to monitor:

    o Number of incidents

    o Training completion rate

---

7. Review & Updates

- This SOP will be reviewed annually or upon significant changes to the security landscape or business requirements.

- IT Manager is responsible for initiating the review process.

---END---