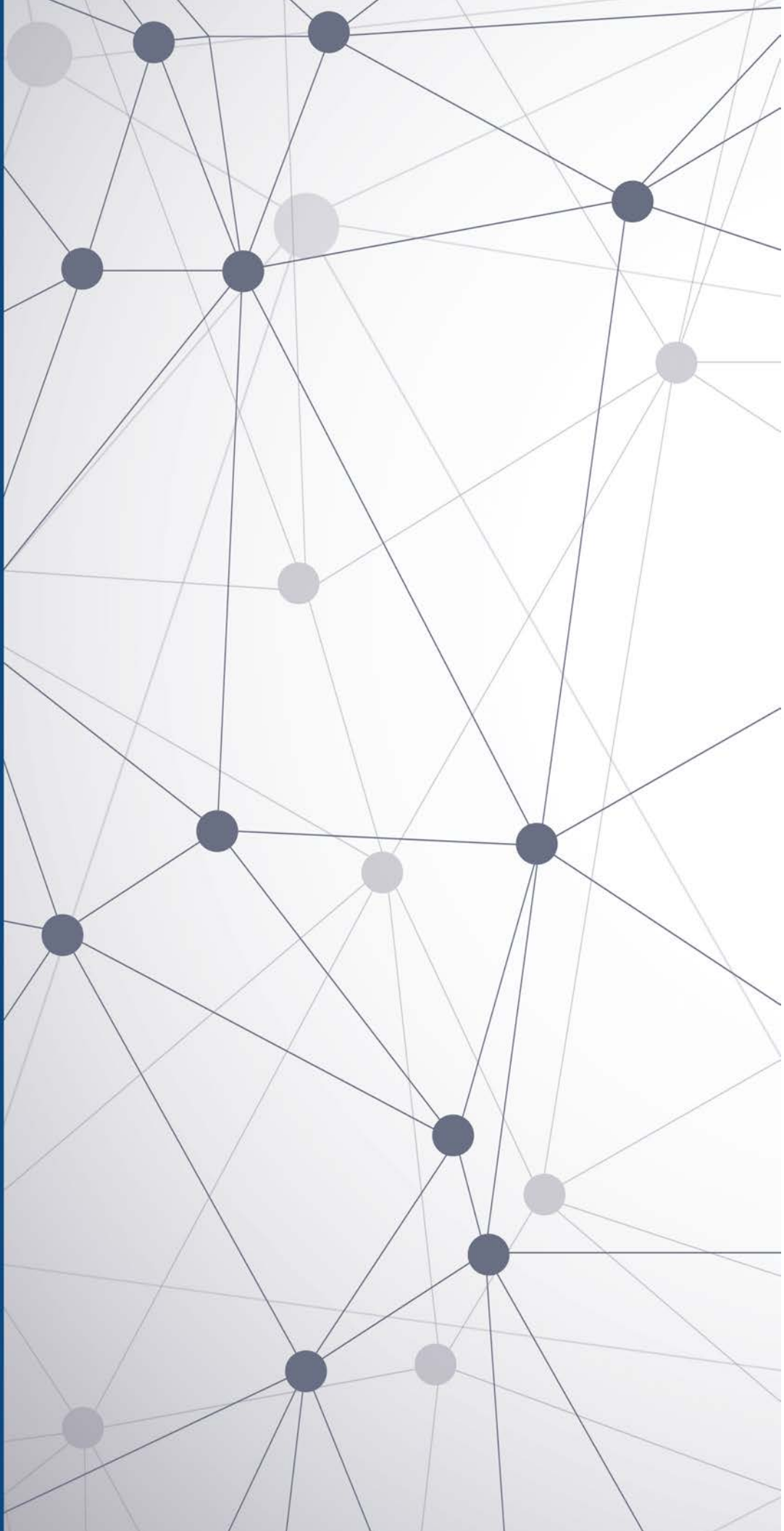
Information Security Policy

October 2026



Document Title	Information Security Policy
Version:	1.0
Dated:	
Document Author:	
Document Owner:	

Document History

version	**Dated**	**Prepared by**	**Changes**
1.0			Initial Document

Document Review/Approval

	Name	**Designation**	**Signature**	**Date**
Reviewed by				
Approved by		Directors/CEO		

Contents

1. **Introduction** 3
2. **Asset Management** 5
3. **Personnel Management** 6
4. **Cybersecurity Awareness and Training** 7
5. **Acceptable Use Policy** 8
6. **Access Control** 9
7. **Operations Security** 11
8. **Communications Security** 12
9. **System Acquisition, Development, and Maintenance** 12
10. **Supplier and Third-Party Relationships** 13
11. **Physical and Environmental Security** 14
12. **Risk Management** 15
13. **Information Security Incident Management** 16
14. **Business Continuity and Disaster Recovery** 17
15. **Data Protection and Privacy** 18

1. Introduction

Notice: [The organization should adjust this chapter or add details that apply to or reflect its specific requirements, the sector and/or industry in which it operates.]

1.1. Policy Statement

Institutional Background info that is linked with the following paragraph

The [***organization Name****]* is committed to protecting its information assets against unauthorized access, loss, or damage. Information security is critical for maintaining customer and stakeholder trust, complying with applicable laws and regulations, and supporting business continuity.

This Information Security Policy outlines the framework for ensuring the confidentiality, integrity, and availability of information assets within [***Organization Name***]. Compliance with this policy is mandatory for anyone accessing organizational information assets.

1.2. Purpose

The purpose of this policy is to ensure that there are appropriate security measures in place to protect the ***organization name***'s corporate information assets and prepare the business to withstand security threats or incidents.

1.3. Information Security Objectives

The Information Security Objectives of [***Organization Name***] are to:

- Protect information assets from unauthorized access, disclosure, alteration, or destruction;
- Ensure the availability and reliability of information systems supporting organizational operations;
- Comply with applicable laws, regulations, and contractual obligations;
- Manage information security risks to an acceptable level
- Promote security awareness and accountability across the organization;
- Support business continuity and resilience;
- Support continuous monitoring, detection, and response to cybersecurity threats and incidents.

1.4. Scope

This policy applies to:

- All employees, contractors, vendors, consultants, and temporary staff.
- All systems, networks, software, hardware, and data owned or managed by the ***organization name*.**
- All forms of information: paper, digital, verbal, and cloud-hosted.
- All organization's work performed or accessed both onsite and remotely.

1.5. Governance and Responsibility

Roles and Responsibilities

Clear accountability ensures security is part of everyone's job. Leadership must set the tone, and responsibilities must be distributed across different levels of the *organization*.

- **Board of Directors / Executive Management:** Provide oversight and approve the Information Security Policy.
- **Chief Information Security Officer (CISO):** Accountable for the strategy, implementation, and enforcement of information security program.
- **Information Security Team:** Monitor, assess risks, respond to incidents, and provide training and awareness to the users.
- **Department Heads:** Ensure compliance and effective implementation of security controls within their departments and the organization.
- **All Users:** Must comply with the policy and report violations or incidents immediately.
- **Third Parties:** Must comply with contractual security requirements when accessing organizational information.

Security Committee

A security committee can be established to enhance oversight and promote continuous improvement of information security within the *organization*

- Establish an Information Security Steering Committee with representation from different units such as, but not limited to, Information Technology, Human Resources, Legal, and Business Operations.
- Review internal audit findings, external threats, and risk assessments regularly.
- Recommend updates to security policies and practices.
- Report findings and recommendations to senior management.
- Oversee the continuous improvement of the Information Security Management System (ISMS).

1.6. Policy review

This policy must remain current to address evolving risks. It shall be reviewed at least once a year and updated whenever there are major organizational, operational, or regulatory changes. All reviews and updates must be formally documented and approved by Senior Management to ensure continued relevance, accountability, and effectiveness.

1.7. Compliance and Enforcement

Compliance with this policy is mandatory. The organization shall establish, maintain, and continuously improve an Information Security Management System (ISMS) aligned with

recognized standards (e.g., ISO/IEC 27001) to protect information assets from internal and external threats, whether intentional or accidental.

Violations may result in disciplinary action, revocation of access, contractual remedies, or legal action, in accordance with the organization's policies and applicable laws and regulations.

2. Asset Management

Notice: [The organization should adjust this chapter or add details that apply to or reflect its specific requirements, the sector and/or industry in which it operates.]

Asset Management ensures that organizational assets are identified, have clear ownership, and are protected based on criticality level to the organization's operations.

2.1. Asset Inventory

Controls:

- An inventory of information and associated assets shall be established and maintained for all organizational assets by the IT unit or designated Personnel.
- Every asset shall have a designated business owner who is responsible for its classification and security enforcement.
- The asset inventory will be regularly reviewed and updated, coordinated by the IT unit or other designated staff or unit.

2.2. Information Classification

Controls:

- The organization creates or adopts a data classification matrix and communicates to all staff to identify and apply appropriate protection measures.
- The organization shall categorize and label all the organization's information according to the applicable classification type. For example: Public, Internal, Confidential, or Restricted.
- The asset owner or Security personnel will ensure the application of strong protection controls (e.g., encryption, access control) based on classification categories.
- Assets shall also be classified based on business criticality to support prioritization in risk management and business continuity planning.

2.3. Media Handling

Controls:

- Security personnel shall protect and encrypt corporate portable devices and storage (including obsolete media) to prevent information leaks in case of theft or loss. (Example: Implement Data Loss Prevention).

- Media in transit shall be protected at all times using approved physical and technical controls to prevent loss, theft, damage, or unauthorized access.

2.4. Secure Disposal

Controls:

- The organization shall establish secure disposal procedures for all assets.
- The asset owner must ensure shredding or incineration for paper records containing sensitive data.
- The organization shall ensure secure technology is used to erase data on electronic storage. (Example: wipe tools or degaussing). Data remains recoverable unless destroyed properly.
- The organization shall partner with certified service providers for the destruction and disposal of old hardware or other electronic waste items.
- The IT unit and designated personnel document and verify all IT assets' disposal activities.

3. Personnel Management

Notice: [The organization should adjust this chapter or add details that applies to or reflect its specific requirements, the sector and/or industry in which it operates.]

Background checks reduce insider risks and ensure only trustworthy people gain access to organization assets.

3.1. Pre-Employment Screening

Controls:

- The organization shall apply screening measures to ensure the careful selection of employees, vendors, and contractors.
- Background checks and due diligence shall be conducted to reduce the risk of system failure, internal sabotage, fraud, or misuse of systems.
- Screening processes shall be documented, consistent, and effective, and applied before granting access to organizational systems or information.

3.2. Staff Management

Controls:

- Staff shall be informed and acknowledge the Acceptable Use and Information Security policies.
- The organization has to ensure third-party contracts contain similar security obligations.
- The organization shall include security responsibilities in all job descriptions.

- Staff will be required to sign non-disclosure agreements (NDAs) with their employment contracts, or other documents like access request forms, for cases where the organization handles sensitive information such as intellectual property items, or other critical work or partners' information.
- The organization and/or business units will establish processes to identify and/or authenticate each staff member (physical ID/electronic ID).
- Segregation of duties shall be implemented to reduce the risk of fraud, error, or unauthorized activities.

3.3. Termination and offboarding

Controls:

- Upon departure, the employee shall return all devices, system access, and organizational information in accordance with internal processes, including BYOD procedures.
- HR shall coordinate with system admins to revoke logical and physical access on or before the final day.
- HR or a dedicated committee shall remind the departing employee of confidentiality obligations and conduct exit interviews when appropriate.

Every suspended, resigning or dismissed staff member must not retain access to or sensitive information. Internal processes and applicable laws shall be followed.

4. Cybersecurity Awareness and Training

Notice: [The organization should adjust this chapter or add details that applies to or reflect its specific requirements, the sector and/or industry in which it operates.]

Awareness and training enable employees to recognize risks, act responsibly, and respond effectively when incidents occur.

4.1. Security Awareness Program

Controls:

- ***[Organization Name]*** shall implement and maintain a formal Information Security Awareness Program for all employees and relevant third parties.
- Security awareness training shall be provided to all staff upon hire as part of the onboarding process and refreshed periodically for all employees.
- Additional awareness training shall be conducted whenever significant policy, regulatory, or work environment changes occur.

4.2. Training Topics

Controls:

- Training shall cover all essential cybersecurity areas so employees know how to act in different situations. It includes, but not limited to:
  - ❖ Password and authentication security, including safe credential use.
  - ❖ Phishing and social engineering awareness.
  - ❖ Secure use of devices, internet, cloud, applications, remote work and BYOD
  - ❖ Incident and security issue reporting procedures.
  - ❖ Best practices for enforcement of the protection of personal data and privacy in the data they access.

4.3. Specialized Training

Controls:

- Additional advanced training must be provided for:
  - ❖ IT Administrators: Secure system configuration, patching, and vulnerability management, among others.
  - ❖ Developers: Secure coding practices, threat modeling, among others.
  - ❖ HR and Legal: Privacy compliance, data management, retention requirements, and other relevant areas.
  - ❖ Executives: Cyber risk governance, risk oversight, decision-making, and other relevant areas.

4.4. Evaluation and Metrics

Controls:

- Organization shall establish training evaluation metrics.
- Training effectiveness shall be evaluated through assessments, phishing simulations, and analysis of incident trends.
- Training participation shall be tracked, and failure to complete required training may result in disciplinary action.
- Periodic phishing simulation exercises shall be conducted, in coordination with the Information Security/IT team, to assess and improve user awareness.

5. Acceptable Use Policy

Notice: [The organization should adjust this chapter or add details that applies to or reflect its specific requirements, the sector and/or industry in which it operates.]

Misuse of company resources can cause security breaches, legal issues, or reputational harm. This section sets the ground rules.

5.1. General Use

Controls:

- Organization resources must be used only for work-related purposes.

- Illegal, malicious, or inappropriate use of organizational resources is strictly prohibited and constitutes a policy violation.
- Employees shall protect organizational information when working remotely or in public locations.
- Any accidental or intentional misuse of organizational resources shall be reported immediately to security personnel.

5.2. Software and Hardware Use

Controls:

- Only licensed and IT-approved software shall be installed on company systems. Unapproved installations are strictly prohibited.
- Users must not disable, bypass, or modify any system security configurations, including firewalls, antivirus, or endpoint protection.
- Where applicable, all personal devices (BYOD) must be formally registered and approved by the IT Department before connecting to the organization's network.
- Personal devices must comply with minimum security standards, including up-to-date antivirus protection, full disk encryption, and automatic screen locking.
- IT and Security personnel shall conduct periodic audits to detect and remove unauthorized software or devices.

5.3. Internet and Email

Controls:

- Internet and email services shall be used for authorized business purposes only.
- Employees shall not use corporate email for personal financial, political, or sensitive communication.
- Users are strictly prohibited from accessing or distributing illegal, offensive, discriminatory, or inappropriate content through the *organization*'s systems.
- Do not open unknown email attachments or click unverified links unless confirmed by IT.
- Phishing or suspicious messages must be reported immediately to the IT or Security team using the designated reporting channel.

6. Access Control

Notice: [The organization should adjust this chapter or add details that applies to or reflect its specific requirements, the sector and/or industry in which it operates.]

Access management defines the requirements for granting, reviewing, and revoking access to the organization's assets. It ensures access is based on business need, managed securely, and monitored to prevent unauthorized use.

6.1. User Access Management

Controls:

- Each staff member will be assigned a unique user ID to ensure accountability. Shared accounts are strictly prohibited.
- Access rights will be granted based on the principle of least privilege and need-to-know.
- Any request to grant or modify access must be formally approved by the asset owner and submitted to the IT unit for implementation.

6.2. Authentication Mechanisms

Controls:

- Enforce strong password policies (length, complexity, update rotation).
- To access all digital applications or systems of the organization, multi-factor authentication (MFA) shall be implemented. The IT or security units will provide guidance on what authentication methods are used internally.
- Restrict administrative accounts to authorized IT staff only, or system managers where applicable.
- Privileged access shall be strictly controlled, monitored, and limited to authorized personnel only.

6.3. Digital signatures

Controls:

- Digital signatures shall be used where applicable to verify the authenticity and integrity of critical documents, contracts, and system communications.
- Private keys used for digital signatures shall be securely stored and protected against unauthorized access or misuse.
- Users shall be trained on the proper use and verification of digital signatures.

6.4. Review and Revocation

Controls:

Security personnel and asset owner shall:

- Conduct periodic access reviews to validate user privileges and detect anomalies.
- Implement logging and monitoring of all internal and remote access sessions.
- Configure account lockout after a defined number of failed login attempts.
- Maintain a formal access request process through the designated unit.
- Enforce role-based access updates when staff change roles.
- Apply immediate account disablement upon termination.

7. Operations Security

Notice: [The organization should adjust this chapter or add details that applies to or reflect its specific requirements, the sector and/or industry in which it operates.]

The Operations Security outlines how the organization protects its systems and information during daily activities. It focuses on maintaining secure operations, detecting issues early, and reducing risks that could disrupt business or compromise data.

7.1. Malware Protection

Controls:

- The IT team must install approved antivirus software on all company devices and ensure it is always updated.
- Users must not disable, pause, or remove any security or antivirus software on their devices.
- Full system scans must be done regularly based on the IT schedule or after any suspected security issue.
- Any malware found or suspected must be reported immediately to the IT or Security personnel for further action.
- Monitoring and logging must be maintained to detect and respond to malware threats across the organization's network.

7.2. Logging and Monitoring

Controls:

- Logging shall be enabled on servers, network devices (including firewalls), and all critical applications.
- Security logs shall be regularly reviewed and monitored to identify suspicious activity, anomalies, or violations of security policies.
- Logs shall be retained for a period required by applicable legal, regulatory, or contractual obligations.
- Access to logs shall be restricted to authorized personnel.

7.3. Patch Management

Controls:

- Critical security patches shall be applied promptly, based on risk and operational impact.
- A formal patch management process and schedule shall be established and followed.
- Automated tools shall be used to identify missing, outdated, or failed patches across systems.
- Patches shall be tested and validated before deployment to minimize the risk of service disruption.

8. Communications Security

Notice: [The organization should adjust this chapter or add details that applies to or reflect its specific requirements, the sector and/or industry in which it operates.]

Communications Security protects information exchanged over networks, email, and wireless systems by defining controls for secure communication.

8.1. Network Security

Controls:

- Networks shall be separated into appropriate zones to protect critical systems.
- Security measures such as IDS/IPS shall be used to protect the network and detect suspicious activity.
- Only authorized users and approved devices are permitted to access corporate networks.
- All Network changes (configuration, rules, ...) shall be approved and documented.
- Regular network vulnerability scans and penetration tests must be performed to identify weaknesses and ensure timely remediation.
- Network logs must be collected, retained, and analyzed to detect suspicious activity or security policy violations.

8.2. Email and Messaging Security

Controls:

- Protective measures, such as filtering and quarantine of suspicious messages, shall be used to reduce the risk of malicious or unauthorized communications.
- Sensitive information shall be protected with encryption when shared through email or messaging.
- Employees shall be trained to recognize and report suspicious messages.
- Encryption shall be applied to sensitive information using approved standards (e.g., TLS 1.3 or latest, AES-256).

8.3. Wireless Security

Controls:

- Wireless networks shall use secure configurations and encryption to protect data in transit.
- Default system settings and credentials shall be changed before wireless services are enabled.
- Wireless access shall be restricted to authorized users and approved devices.

9. System Acquisition, Development, and Maintenance

Notice: [The organization should adjust this chapter or add details that applies to or reflect its specific requirements, the sector and/or industry in which it operates.]

The organization ensures that security is considered throughout the lifecycle of systems and applications, from acquisition to maintenance. The IT and Security team and System administrators are responsible for guiding, reviewing, and validating security practices at each stage.

9.1. Secure Development Lifecycle (SDLC)

Controls:

- Security requirements shall be included in all phases of system and software development.
- IT and Security teams shall review and approve development plans, coding standards, and testing practices.
- Developers shall follow approved secure coding standards and perform peer code reviews.
- Developers shall receive regular training in secure design and coding principles.

9.2. Vulnerability Testing

Controls:

- IT and Security teams shall conduct regular vulnerability scans and IT audits, at least on quarterly basis or after major changes.
- Findings shall be prioritized and remediated based on their risk level, severity, and impact on operations.
- Remediation actions and progress shall be documented and monitored by the Security team.
- Where applicable, the organization can hire an external certified third-party to conduct VA/PT at least once a year.

9.3. Change Management

Controls:

- All system changes shall be documented, tested, and formally approved by senior management.
- All changes shall be tracked in a centralized system.
- Perform a security risk assessment before deployment.
- Rollback plans shall be prepared and tested to ensure continuity in case of failure.

10. Supplier and Third-Party Relationships

Notice: [The organization should adjust this chapter or add details that applies to or reflect its specific requirements, the sector and/or industry in which it operates.]

The organization ensures that all third parties with access to its systems, networks, applications, or sensitive data follow strong security practices. The IT and Security teams are

responsible for evaluating, approving, and monitoring these relationships to protect organizational operations and information.

10.1. Third-Party Risk Management

Controls:

- IT and Security teams shall assess the security practices of any third party before granting access to the organization's information assets.
- Contracts and Service Level Agreements (SLAs) shall include security requirements and clearly define responsibilities for protecting organizational information.
- The organization shall not engage third parties for services involving system or data access unless minimum security requirements are met and verified.

10.2. Ongoing monitoring

Controls:

- IT and Security teams shall periodically review third-party security compliance, and after any significant incidents.
- Third parties shall provide evidence of meeting contractual security requirements upon request.
- Third-party access to systems and data shall be limited, monitored, and promptly revoked when no longer required.
- Shared information shall be securely destroyed at the end of the contract.

11. Physical and Environmental Security

Notice: [The organization should adjust this chapter or add details that applies to or reflect its specific requirements, the sector and/or industry in which it operates.]

Physical protection is just as important as digital protection. Unauthorized entry into buildings or server rooms could lead to theft, sabotage, or data breaches.

11.1. Facility Access Control

Controls:

- All facilities will be secured with access badges, locks, and visitor logs.
- Entry to data centers and critical rooms will be restricted to authorized staff only.
- Sensitive work areas will be monitored using CCTV and alarms.
- Visitors to the workplace shall be escorted at all times.

11.2. IT devices Security

Controls:

- Use cable locks or secure racks for IT devices in public or shared areas.
- Unauthorized removal or relocation of equipment is strictly prohibited without written approval from the IT Department.

- Critical systems shall be connected to uninterruptible power supply (UPS) sources or backup generators to ensure continued operation during power failures.
- Environmental monitoring systems must be implemented in server rooms and data centers to track temperature, humidity, and air quality.
- Fire suppression and flood prevention controls shall be installed, tested, and maintained according to safety and building regulations.
- Damaged or malfunctioning equipment must be reported immediately to IT or Facilities for inspection and repair.
- Regular physical inspections shall be conducted to verify compliance with equipment security requirements.
- A clean desk and clear screen policy shall be enforced in all work environments.

12. Risk Management

Notice: [The organization should adjust this chapter or add details that applies to or reflect its specific requirements, the sector and/or industry in which it operates.]

The organization shall implement a structured risk management process to identify, assess, and manage information security risks. Senior Managers, Asset owners, and the Security Team share responsibility for ensuring risks are understood, treated, and monitored.

12.1. Risk Assessment

Controls:

- The organization shall develop cyber risk matrix/levels in line with the institution's internal/ sector, national, or industry requirements.
- Risk assessments shall be performed at least annually and following significant changes.
- Asset owners and Security personnel shall identify risks related to their systems, processes, and information.
- Risks shall be assessed based on likelihood and business impact.
- Record all identified risks in the risk register. Maintain and update it.

12.2. Risk Treatment

Controls:

- Risks shall be treated using approved options, including acceptance, avoidance, mitigation, or transfer.
- Risk treatment decisions shall be documented in a centralized risk register.
- Asset owners shall be accountable for managing assigned risks, with oversight from the Security personnel.
- Risk acceptance or unacceptable risks shall be escalated to senior management for review and decision.

12.3. Continuous Improvement

Controls:

- The risk register shall be reviewed periodically to ensure risks remain current.
- Identified risks shall be considered in projects and business planning.
- Security policies and procedures shall be updated as new risks are identified.

13. Information Security Incident Management

Notice: [The organization should adjust this chapter or add details that applies to or reflect its specific requirements, the sector and/or industry in which it operates.]

Early detection and prompt reporting of security incidents help minimize damage and reduce recovery time. All employees shall be able to identify potential threats and report them without delay to the designated team.

13.1. Incident Identification

Controls:

- Implement an incident detection solution, such as SIEM, for the network and systems to ensure early incident detection.
- Staff must be trained regularly to identify common signs of phishing attempts, ransomware, data breaches, and unusual system behavior.
- All employees are required to report any suspicious activity or security anomaly immediately to the IT or Security Department.
- Designated reporting channels (e.g., hotline, security email, or ticketing system) must be clearly communicated and always available.
- Failure to report known or suspected incidents may result in disciplinary action.

13.2. Response and Escalation

Controls:

- An approved Incident Response Plan (IRP) shall be developed, maintained and followed for all security events.
- Incidents must be classified by severity and escalated immediately to the appropriate management and technical teams.
- Containment, eradication, and recovery steps must be executed without delay according to the IRP.
- All incident actions, timelines, and communications shall be documented for accountability and post-incident analysis.
- Critical cyber incidents must be reported to executive management and, where required, to regulators and/or affected parties.
- Only authorized personnel may communicate externally about incidents to prevent misinformation.

13.3. Post-Incident Review

Controls:

- Conduct root cause analysis for every major incident.
- Document lessons learned and corrective actions.
- Share results with management and relevant teams.
- Update security policies and controls based on findings.

14. Business Continuity and Disaster Recovery

Notice: [The organization should adjust this chapter or add details that applies to or reflect its specific requirements, the sector and/or industry in which it operates.]

The organization shall maintain business continuity and disaster recovery plans to ensure continuity of business operations and timely recovery from disruptions. Responsibility is shared between Senior Management, IT, Security Personnel, and business units.

14.1. Backup Management

Controls:

- Backups of all critical systems, applications, data, and configurations shall be performed regularly based on business and risk requirements.
- Backups shall be securely stored in approved offsite or cloud locations.
- Backup data shall be protected against unauthorized access using approved security controls.
- IT shall manage backup operations, while system and data owners shall define and confirm recovery requirements.
- Backup restoration shall be tested periodically to confirm data integrity and recovery effectiveness.

14.2. Business Continuity Planning(BCP)

Controls:

- Business Continuity Plans shall be developed for critical business and operational functions**.**
- A Business Impact Analysis shall be conducted periodically to identify critical functions and recovery priorities.
- Roles, responsibilities, key contacts, and recovery strategies shall be clearly defined.
- Alternate work locations and communication methods shall be identified.
- Continuity plans shall be tested periodically through exercises involving relevant staff and stakeholders.

14.3. Disaster Recovery (DR)

Controls:

- Recovery objectives, including Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), shall be defined for critical systems.
- Disaster Recovery Plans shall be maintained and tested at least annually, involving relevant staff and stakeholders.
- Appropriate recovery capabilities, including redundant systems, cloud backups, and recovery solutions, shall be in place for critical systems.
- Staff shall be aware of their roles during a disruption or disaster.

15. Data Protection and Privacy[1]

Notice: [The organization should adjust this chapter or add details that applies to or reflect its specific requirements, the sector and/or industry in which it operates.]

Notice: [Although it can be integrated into the information security policy, it is recommended to have a separate data protection and privacy policy, and it has to be in line with Rwanda's Law relating to the protection of personal data and privacy.]

This Data Protection and Privacy Policy defines the organization's commitment to complying with Rwanda's Personal Data Protection and Privacy Law and ensuring that personal data is processed lawfully, transparently, and securely.

15.1. Processing of personal data[2]

Controls:

Personal data shall be:

- Processed lawfully, fairly, and for specific purposes
- Limited to what is necessary for business and operational needs
- Accurate and kept up to date
- Retained only for approved and lawful periods.

15.2. Personal Data Handling

Controls:

The organization shall:

- Collect only the minimum personal data required for defined purposes
- Restrict access to personal data to authorized personnel on a need-to-know basis
- Apply enhanced protections for sensitive personal data

15.3. Data Subject Rights[3]

Controls:

[1] In accordance with Law N° 058/2021 of 13/10/2021 relating to the protection of personal data and privacy
[2] Chapter II, Section 1, Art. 4 to Art. 14
[3] Chapter III, Art. 18 to Art. 26

The organization shall respect the rights of data subjects, such as the right to access, rectification, and erasure, etc., in line with Rwanda's Personal Data Protection and Privacy Law.

15.4. Data Sharing and Third Parties

Controls:

Personal data shall only be shared with third parties where:

- There is a lawful basis for sharing.
- Data protection obligations are defined contractually.
- Access is limited to what is necessary for the agreed purpose.

15.5. Data Protection Compliance and Security Controls

Controls:

The organization shall establish governance and technical controls to protect personal data:

- **Data Protection Officer (DPO):** Appoint a DPO to oversee legal compliance, guide DPIAs, serve as the regulatory and data subject liaison, conduct training, and advise on data breach management.
- **Data Protection Impact Assessment (DPIA):** Conduct a DPIA prior to launching new or high-risk data processing projects to identify privacy risks and establish appropriate mitigation measures.
- **Technical Safeguards:** Deploy technical measures including, but not limited to, Data Loss Prevention (DLP), encryption, access controls, and secure backup controls, to prevent unauthorized access, leakage, loss, or compromise of personal data across endpoints, networks, on-premise and cloud systems.
- **Privacy Training and Awareness:** Conduct regular, role-based privacy training and awareness activities for employees.

15.6. Personal Data Breach Notification

Controls:

Personal data breaches shall be identified, reported, investigated, and documented without delay. Notifications to the competent authority and affected individuals shall be made in accordance with Rwanda's Personal Data Protection and Privacy Law.