Information Security Policies

Table of Contents

[Core Security Policies Every Organization Should Have: 2](#_Toc203391369)

[Roadmap for Developing Organizational Policies 4](#_Toc203391370)

[Checklist for Developing Policies 5](#_Toc203391371)

[CIS Controls to Security Policy Mapping 6](#_Toc203391372)

[Information Security Policy 7](#_Toc203391373)

[Acceptable Use Policy 10](#_Toc203391374)

[Access Control Policy 12](#_Toc203391375)

[Data Classification and Handling Policy 14](#_Toc203391376)

[Incident Response Policy 17](#_Toc203391377)

[Password Management Policy 19](#_Toc203391378)

[Third-Party Vendor Management Policy 21](#_Toc203391379)

[Security Awareness and Training Policy 23](#_Toc203391380)

# Core Security Policies Every Organization Should Have:

**1.** [**Information Security Policy (ISP)**](#_Information_Security_Policy)

**Purpose:** Defines the organization’s overall approach to information security.  
**Why:** Serves as the umbrella policy from which others derive.  
**Includes:** Security objectives, roles, governance, and compliance scope.

**2.** [**Acceptable Use Policy (AUP)**](#_Acceptable_Use_Policy)

**Purpose:** Outlines what users can and cannot do on organizational systems.  
**Why:** Prevents misuse of resources and protects from legal liability.  
**Includes:** Internet use, personal device use, social media, software restrictions.

**3.** [**Access Control Policy**](#_Access_Control_Policy)

**Purpose:** Defines how access to systems and data is granted, monitored, and revoked.  
**Why:** Prevents unauthorized access to sensitive information.  
**Includes:** Role-based access, least privilege, MFA, account reviews.

**4.** [**Data Classification and Handling Policy**](#_Data_Classification_and)

**Purpose:** Provides rules for classifying and securing data based on sensitivity.  
**Why:** Ensures appropriate protection and compliance (e.g., PII, PHI, CUI).  
**Includes:** Data tiers (Public, Confidential, Restricted), handling requirements.

**5.** [**Incident Response Policy**](#_Incident_Response_Policy)

**Purpose:** Defines how the organization detects, reports, and responds to security incidents.  
**Why:** Ensures rapid response to reduce damage and meet reporting obligations.  
**Includes:** Roles, communication, escalation paths, breach notification.

**6.** [**Password / Authentication Policy**](#_Password_Management_Policy)

**Purpose:** Sets requirements for secure password use and authentication methods.  
**Why:** Protects accounts from brute-force and credential attacks.  
**Includes:** Password complexity, MFA, rotation, lockout thresholds.

**7. Change Management Policy**

**Purpose:** Controls how changes to systems and applications are planned and implemented.  
**Why:** Minimizes risk of disruption and security flaws from poor change control.  
**Includes:** Approval process, testing, rollback plans, documentation.

**8.** [**Vendor / Third-Party Risk Management Policy**](#_Third-Party_Vendor_Management)

**Purpose:** Ensures third parties handling your data or systems meet your security standards.  
**Why:** Prevents breaches from insecure vendors.  
**Includes:** Due diligence, contracts, data processing agreements, audits.

**9. Encryption and Cryptographic Policy**

**Purpose:** Sets standards for encrypting sensitive data.  
**Why:** Ensures confidentiality and regulatory compliance.  
**Includes:** Approved algorithms, key management, encryption in transit/at rest.

**10. Backup and Recovery Policy**

**Purpose:** Defines how data is backed up and recovered in case of loss or disaster.  
**Why:** Supports business continuity and reduces downtime.  
**Includes:** Frequency, testing, retention, off-site storage.

**11. Remote Access / Telework Policy**

**Purpose:** Governs secure access for remote workers and devices.  
**Why:** Protects systems when accessed off-site.  
**Includes:** VPN use, device requirements, BYOD rules, monitoring.

**12. Mobile Device / BYOD Policy**

**Purpose:** Manages security of employee-owned devices accessing corporate data.  
**Why:** Reduces risk of data leakage or device compromise.  
**Includes:** MDM requirements, encryption, remote wipe, app controls.

**13.** [**Security Awareness and Training Policy**](#_Security_Awareness_and)

**Purpose:** Mandates ongoing education for employees on security threats and best practices.  
**Why:** Reduces human error, phishing risk, and policy violations.  
**Includes:** Training frequency, content areas, completion tracking.

**14. Physical Security Policy**

**Purpose:** Protects physical access to systems, data centers, and workspaces.  
**Why:** Prevents theft, tampering, and unauthorized access.  
**Includes:** Badge access, visitor management, secure disposal.

**15. Log Management / Monitoring Policy**

**Purpose:** Sets rules for logging, monitoring, and analyzing system activity.  
**Why:** Supports incident detection, forensics, and compliance.  
**Includes:** Log retention, tools used, who monitors, alert thresholds.

**🧩 Optional / Advanced Policies (as your program matures)**

* Cloud Security Policy
* DevSecOps / Secure SDLC Policy
* Data Loss Prevention (DLP) Policy
* Privacy Policy (especially for customer-facing organizations)
* System Hardening Policy

# Roadmap for Developing Organizational Policies

1. Initial Preparation and Planning

* Understand the Need: Identify why policies are needed and what areas they should cover.
* Form a Policy Development Team: Assemble a team with representatives from different departments.
* Research Best Practices: Look into similar organizations and industry standards.
* Set Objectives: Define clear objectives for what the policies should achieve.

2. Drafting the Policies

* Outline the Structure: Establish a consistent format for all policies.
* Write Clear and Concise Policies: Avoid jargon and ensure policies are easily understandable.
* Include Key Components: Ensure each policy includes purpose, scope, responsibilities, procedures, and compliance.
* Consult Legal and Regulatory Requirements: Ensure policies comply with all relevant laws and regulations.

3. Review and Feedback

* Internal Review: Have the policy development team review the drafts.
* Seek Feedback: Circulate drafts to key stakeholders and collect feedback.
* Revise Accordingly: Make necessary adjustments based on feedback.

4. Approval and Implementation

* Executive Approval: Present the final drafts to the organization's leadership for approval.
* Communicate Policies: Clearly communicate the new policies to all employees.
* Training: Provide training sessions if necessary to ensure understanding and compliance.
* Document Distribution: Ensure policies are easily accessible to all members of the organization.
* Change Management: Implement a plan to review and communicate changes with the organization.

5. Monitoring and Review

* Regular Monitoring: Continually monitor the effectiveness of the policies.
* Periodic Review: Schedule regular reviews to update and revise policies as needed.
* Feedback Mechanism: Establish a system for ongoing feedback from employees.

# Checklist for Developing Policies

|  | Action Needed | Responsible Team | Notes |
| --- | --- | --- | --- |
|  | Identify the need for policies |  |  |
|  | Assemble a policy development team |  |  |
|  | Research best practices |  |  |
|  | Define objectives |  |  |
|  | Outline the structure of policies |  |  |
|  | Write clear and concise policies |  |  |
|  | Include key components in each policy |  |  |
|  | Ensure compliance with legal and regulatory requirements |  |  |
|  | Conduct an internal review |  |  |
|  | Seek feedback from stakeholders |  |  |
|  | Revise policies based on feedback |  |  |
|  | Obtain executive approval |  |  |
|  | Implement change management process |  |  |
|  | Communicate policies to all employees |  |  |
|  | Provide necessary training |  |  |
|  | Distribute policies to all members |  |  |
|  | Monitor policy effectiveness |  |  |
|  | Schedule regular reviews |  |  |
|  | Establish a feedback mechanism |  |  |

# CIS Controls to Security Policy Mapping

|  |  |
| --- | --- |
| Policy Name | Aligned CIS Control(s) |
| Information Security Policy | *Governance layer* — Supports all controls as the foundation of a security program |
| Acceptable Use Policy (AUP) | Control 14: Security Awareness and Skills Training  Control 17: Incident Response Management |
| Access Control Policy | Control 6: Access Control Management  Control 16: Application Software Security (for app-level access) |
| Data Classification & Handling Policy | Control 3: Data Protection  Control 13: Network Monitoring and Defense |
| Incident Response Policy | Control 8: Audit Log Management  Control 17: Incident Response Management |
| Password / Authentication Policy | Control 4: Secure Configuration of Enterprise Assets and Software  Control 5: Account Management  Control 6: Access Control Management |
| Change Management Policy | Control 4: Secure Configuration  Control 16: Application Software Security |
| Vendor Risk Management Policy | Control 2: Inventory and Control of Software Assets (if vendors provide software)  Control 15: Service Provider Management |
| Encryption / Cryptographic Policy | Control 3: Data Protection |
| Backup & Recovery Policy | Control 11: Data Recovery |
| Remote Access / Telework Policy | Control 6: Access Control Management  Control 12: Network Infrastructure Management |
| Mobile Device / BYOD Policy | Control 1: Inventory of Enterprise Assets  Control 10: Malware Defenses |
| Security Awareness & Training Policy | Control 14: Security Awareness and Skills Training |
| Physical Security Policy | Control 7: Continuous Vulnerability Management (covers physical asset risk indirectly)  Control 18: Penetration Testing *(includes physical tests and social engineering)* |
| Log Management / Monitoring Policy | Control 8: Audit Log Management  Control 13: Network Monitoring and Defense |

# Information Security Policy

Introduction

This Information Security Policy is designed to protect the information assets of [Organization Name] from all threats, whether internal or external, deliberate or accidental. The policy outlines the responsibilities and expected behaviors of all employees, contractors, and third-party users to ensure the safe and secure use of the organization’s information resources.

Purpose

The purpose of this policy is to:

* Ensure the confidentiality, integrity, and availability of information.
* Protect against unauthorized access, use, disclosure, disruption, modification, or destruction of information.
* Promote compliance with legal, regulatory, and contractual requirements.
* Establish a framework for the management of security risks.

Responsibilities

To ensure the effectiveness of this policy, the following roles and responsibilities are established:

* Chief Information Security Officer (CISO): Responsible for the overall implementation, enforcement, and review of this policy.
* Information Security Team: Supports the CISO in the day-to-day management of information security and compliance with this policy.
* Department Heads: Ensure that their respective areas comply with the information security policy and procedures.
* Employees and Contractors: Adhere to the information security policy and report any security incidents or concerns to the Information Security Team.

Commitment of Management

* The Chief Information Security Officer (CISO) is responsible for the overall implementation, enforcement, and review of this policy.
* The CISO will establish security committees and working groups as necessary to support the information security program. This includes overseeing the entire security program to ensure effectiveness.
* Regular security audits and risk assessments will be conducted to identify and mitigate potential security threats.

Policy

1. Access Control

* Access to information systems and data will be granted based on the principle of least privilege and need-to-know.
* Users must use strong, unique passwords and change them regularly.
* Multi-factor authentication will be implemented where necessary.
* Access rights will be reviewed periodically to ensure appropriate access levels.
* Mechanisms for ensuring that only authorized users can access systems will be maintained.

2. Awareness and Training

* All employees will receive regular training on information security policies, procedures, and best practices.
* Security awareness programs will be conducted to keep employees informed about emerging threats and security trends.
* Ensuring that all personnel are aware of security risks and are trained to follow security procedures.

3. Audit and Accountability

* Actions on information systems must be traceable to individuals, and records must be maintained for accountability.

4. Security Assessment and Authorization

* Policies and processes for assessing security controls and authorizing systems for operation will be established and enforced.

5. Configuration Management

* Controls for managing system configurations and changes will be implemented and maintained.

6. Contingency Planning

* Preparing for and recovering from unexpected events that disrupt operations will be ensured through established contingency plans.

7. Data Protection

* All sensitive and confidential data must be encrypted during transmission and storage.
* Data classification schemes will be used to categorize data based on its sensitivity and criticality.
* Regular backups of critical data will be performed and stored securely offsite.
* Ensuring that systems and information are accurate, complete, and protected from unauthorized changes.

8. Incident Response

* An incident response plan will be established to address security breaches and incidents. This plan must include identification, containment, eradication, recovery, and lessons learned phases.
* All employees must report suspected security incidents immediately to the CISO or designated contact.

9. Maintenance

* Ensuring that systems are properly maintained and secure during repairs and updates.

10. Media Protection

* Controls for protecting information stored on various media types will be implemented and maintained.

11. Physical and Environmental Protection

* Access to the organization’s physical premises and information systems will be controlled and monitored.
* Visitors must be escorted at all times and must sign in and out at reception.
* Physical security controls such as locks, alarms, and surveillance cameras will be used to protect information assets.
* Safeguards for physical access and environmental conditions of systems and facilities will be maintained.

12. Planning

* Policies for establishing security plans and procedures will be developed and maintained.

13. Personnel Security

* Ensuring that personnel are reliable and trustworthy for their roles through proper vetting and clearances.

14. Risk Assessment

* Identifying and evaluating risks to information systems through regular risk assessments.

15. System and Services Acquisition

* Ensuring that security is built into systems and services from the beginning through stringent acquisition processes.

16. System and Communications Protection

* Protecting system and data communications from unauthorized access and manipulation at all times.

17. Supply Chain Risk Management

* Managing risks from external vendors and supply chains to protect organizational information assets.

18. System and Information Management

* Ensuring proper management of information systems and data throughout their lifecycle.

Compliance

All employees, contractors, and third-party users must comply with this policy. Non-compliance may result in disciplinary action up to and including termination of employment or contract, as well as possible legal action.

Review

This policy will be reviewed annually by the CISO and updated as necessary to reflect changes in the organization’s information security requirements, regulatory environment, and emerging threats.

Approval

This Information Security Policy has been approved by the senior management of [Organization Name] and is effective as of [Effective Date].

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | [Date] | Initial creation | [Name] |

# Acceptable Use Policy

Scope

This policy applies to all employees, contractors, consultants, temporary, and other workers at Company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Company.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Company. These rules are in place to protect the employee and Company. Inappropriate use exposes Company to risks including virus attacks, compromise of network systems and services, and legal issues.

Roles and Responsibilities

* Employees: Ensure compliance with this policy and report any identified security breaches.
* IT Department: Provide guidance regarding acceptable use, monitor compliance, and address security concerns.
* Management: Enforce policy adherence and address violations appropriately.

Acceptable Use

* Use company resources for business-related purposes only.
* Protect sensitive information at all times.
* Comply with all applicable laws and regulations.
* Respect the privacy and personal rights of others.
* Limited personal use that doesn’t interfere with work or violate policy.
* Access only data the user is authorized to access.
* Use licensed software and respect copyright laws.

Unacceptable Use

* Engaging in illegal activities.
* Using company resources for personal gain or activities not related to company business.
* Accessing, downloading, or distributing offensive materials.
* Introducing malicious software into the network.
* Unauthorized access to systems or data (hacking).
* Sharing login credentials or using someone else's credentials.
* Downloading or distributing pirated software or media.
* Connecting unapproved devices to the corporate network.
* Bypassing security controls (e.g., VPNs, firewalls).
* Excessive personal use of internet or email during work hours.

Internet Use

* Use the internet for business purposes in alignment with company goals.
* Avoid accessing websites that contain illegal, offensive, or inappropriate material.
* Do not download or install unauthorized software.

Personal Device Use and BYOD (Bring Your Own Device)

* Personal devices should be used for business purposes only during work hours.
* Ensure personal devices comply with company security policies.
* Report any lost or stolen personal devices immediately.
* Install company-approved software to manage and secure the device.

Social Media

* Do not post confidential or proprietary company information.
* Represent the company professionally and respectfully at all times.
* Do not engage in social media activities during work hours unless it is part of your job duties.

Software Restrictions

* Only use software that is approved and provided by the IT department.
* Do not download or install unauthorized software on company devices.
* Ensure all software is kept up to date with the latest security patches.

Security Requirements

* Lock your computer when leaving your desk.
* Do not leave sensitive information unattended.
* Use encryption for transmitting sensitive data.
* Use strong, unique passwords and multi-factor authentication (MFA).
* Report any suspicious activity or security violations.
* Prohibiting the use of public Wi-Fi for sensitive work without a VPN.

Data Handling

* Classify data according to its sensitivity level.
* Store sensitive data securely and restrict access to authorized personnel only.
* Dispose of sensitive data in a secure manner.
* Do not share sensitive data via unsecured channels.

Compliance

Adherence to this policy is mandatory. Non-compliance may result in disciplinary action, up to and including termination. Regular audits will be conducted to ensure compliance.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | [Date] | Initial creation | [Name] |

# Access Control Policy

Scope

This Access Control Policy applies to all employees, contractors, consultants, temporary staff, and other workers at [Organization's Name], including all personnel affiliated with third parties. This policy covers all systems, applications, and data owned or managed by [Organization's Name].

Purpose

The purpose of this Access Control Policy is to define the procedures and guidelines for granting, managing, and revoking access to [Organization's Name]'s systems and data. This policy ensures alignment with security best practices and compliance with relevant regulations and standards.

Roles and Responsibilities

* Chief Information Security Officer (ISO): Responsible for the overall implementation and enforcement of this policy.
* System Administrators: Tasked with managing user accounts, access permissions, and monitoring activities.
* Department Managers: Approve access requests and ensure employees' access rights match their job responsibilities.
* Employees and Contractors: Responsible for using their access privileges in accordance with this policy and reporting any security incidents.

Policy

User Authentication Methods

All users must be authenticated through a combination of username and password. Multi-factor authentication (MFA) is required for accessing sensitive systems and data. Authentication credentials must be kept confidential and not shared.

Role-Based Access Permissions

Access permissions are granted based on the user's role within the organization. Role definitions must be documented and maintained to reflect current job responsibilities. Access rights will be reviewed and reassigned when roles change.

Principle of Least Privilege

Users are granted the minimum level of access necessary to perform their job functions. This principle minimizes the risk of unauthorized access to sensitive information.

Access Request and Approval Procedures

* Access requests must be submitted through [Organization's Name]'s access management system.
* Requests must include the reason for access, duration, and systems/data required.
* Department Managers must review and approve all access requests.
* The ISO must review and approve access to highly sensitive systems and data.

Account Management and Provisioning

* New user accounts are created following the approval of access requests.
* Accounts must be provisioned with the appropriate access rights based on their role.
* Temporary accounts must have an expiration date and be deactivated after the specified period.
* Accounts must be reviewed regularly to ensure compliance with the least privilege principle.

Monitoring and Auditing Requirements

* All access to systems and data must be logged and monitored for suspicious activities.
* Audit logs must be retained for a minimum of [specify duration] to comply with regulatory requirements.
* Regular audits must be conducted to ensure compliance with this policy and detect potential security breaches.

Access Revocation and Review Guidelines

* Access must be revoked immediately upon termination or change in job responsibilities.
* Departments must notify the IT department of any changes requiring access adjustments.
* Regular access reviews must be conducted to ensure that access rights are current and appropriate.
* The ISO must review and approve the results of access reviews.

Compliance

Non-compliance with this policy may result in disciplinary actions, up to and including termination of employment. Compliance with this policy is mandatory for all employees and affiliated personnel. The Chief Information Security Officer is responsible for ensuring compliance through regular audits and reviews.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | [Date] | Initial creation | [Name] |

# Data Classification and Handling Policy

Purpose

This policy outlines the processes and measures for data handling and classification to ensure the protection and confidentiality of information. It is essential to safeguard data throughout its lifecycle and comply with regulatory requirements.

Scope

This policy applies to all employees, contractors, and third-party service providers who handle, manage, or access the organization's data. It covers all data types, including but not limited to electronic records, paper records, and verbal communications.

Roles and Responsibilities

Data Protection Committee

Oversees the implementation and enforcement of this policy, conducts regular reviews, and updates the policy as necessary.

IT Department

Responsible for implementing encryption, access controls, logging, monitoring, and other technical measures outlined in this policy.

Data Owners

Ensure that data is classified appropriately and that protection measures are applied according to the classification.

Employees

Adhere to this policy, complete required training, and report any incidents or breaches.

Data Classification

Data will be classified based on its sensitivity and criticality. The classifications (examples) are as follows:

* Confidential: Data that unauthorized disclosure could cause significant harm. (High)
* Internal: Data meant for internal use within the organization. (Moderate)
* Public: Data that can be freely shared without harm. (Low)
* Example: NDIT Data Classification Policy
  + <https://www.ndit.nd.gov/governance/data-classification-policy>

Protection Measures

Encryption

All sensitive data must be encrypted both in transit and at rest using industry-standard encryption protocols.

Data Access Control

Access to data will be based on the principle of least privilege, ensuring only authorized personnel can access specific data based on their role.

Storage Requirements

Data must be stored in a secure environment with physical and logical access controls in place to safeguard it from unauthorized access and breaches.

Transmission Requirements

All data transmissions must be encrypted using secure protocols to ensure data integrity and confidentiality during transit.

Access Controls

Access to data will be restricted based on role-based access control (RBAC) policies, ensuring that employees only have access to data necessary for their job functions.

Logging

All access to sensitive data must be logged, including user identity, time and date of access, and type of access. Logs must be protected against unauthorized modifications.

Monitoring

Continuous monitoring of data access and usage will be conducted to detect and respond to unauthorized or suspicious activity in real-time.

Retention

Data must be retained only for as long as necessary to fulfill its intended purpose and comply with legal and regulatory requirements. Once no longer needed, data must be securely deleted or archived.

Data Lifecycle Management

Data will be managed throughout its lifecycle from creation to destruction. The stages include:

* Creation: Identifying and classifying data at the point of creation.
* Storage: Securely storing data in compliance with classification standards.
* Usage: Ensuring data is accessed and used appropriately based on classification.
* Archival: Archiving data securely when it is no longer actively used but must be retained.
* Destruction: Securely destroying data that is no longer required.

Compliance Requirements

The organization must comply with all applicable data protection laws and regulations, such as GDPR, CCPA, and HIPAA. Regular audits will be conducted to ensure compliance.

Training and Awareness

All employees will undergo regular training on data handling and classification policies to ensure awareness and adherence to best practices.

Incident Response

In the event of a data breach or incident, the following steps must be taken:

* Immediate containment and assessment of the breach.
* Notification to the relevant authorities and affected parties as required by law.
* Investigation to determine the cause of the breach and take corrective actions.
* Review and update policies to prevent future incidents.

Governance, Review, and Approval

This policy will be governed by the Data Protection Committee. It will be reviewed annually and updated as necessary to ensure continued relevance and compliance with evolving regulations.

Conclusion

Adhering to this data handling and classification policy will ensure the protection of sensitive information, compliance with legal requirements, and the institution of a culture of data security within the organization.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | [Date] | Initial creation | [Name] |

# Incident Response Policy

Purpose

This policy outlines the procedures for identifying, classifying, responding to, and managing security incidents. The goal is to minimize the impact of incidents on the organization and ensure a timely and coordinated response.

Scope

This policy applies to all employees, contractors, and third-party users of the organization's information systems and networks. It covers all types of security incidents including, but not limited to, data breaches, malware infections, unauthorized access, and denial-of-service attacks.

Roles and Responsibilities

Incident Response Team (IRT)

* Lead the incident response efforts.
* Coordinate with internal and external stakeholders.
* Ensure compliance with legal and regulatory requirements.

IT Department

* Identify and report incidents.
* Assist with containment, eradication, and recovery efforts.

Legal and Compliance

* Advise on legal and regulatory implications.
* Ensure evidence preservation and chain of custody.

Communications Team

* Manage internal and external communications.
* Ensure timely updates to all stakeholders.

Policy

Incident Identification and Classification

* Define and categorize types of incidents (e.g., data breaches, malware).
* Establish criteria for classifying the severity of incidents.

Communication and Escalation Procedures

* Define communication channels and escalation paths.
* Ensure timely notification to appropriate stakeholders.

Containment and Eradication Strategies

* Outline steps to contain the incident and prevent further damage.
* Detail eradication procedures to remove the root cause of the incident.

Evidence Preservation

* Ensure proper collection and preservation of evidence.
* Maintain chain of custody for forensic analysis.

Recovery Steps

* Detail processes for restoring affected systems and data.
* Verify the integrity of restored systems.

Post-Incident Review

* Conduct a thorough review of the incident and response actions.
* Identify lessons learned and areas for improvement.

Compliance with Legal and Regulatory Requirements

* Ensure all actions comply with relevant laws and regulations.
* Document compliance efforts and report to regulatory bodies as required.

Compliance

All employees, contractors, and third-party users must adhere to this policy. Non-compliance may result in disciplinary action, up to and including termination of employment or contracts.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | [Date] | Initial creation | [Name] |

# Password Management Policy

Scope

This policy applies to all employees, contractors, consultants, temporary and other workers at [Organization Name], including all personnel affiliated with third parties.

Purpose

The purpose of this policy is to establish a standard for the creation, protection, and management of passwords to ensure the security of [Organization Name]'s information systems.

Roles and Responsibilities

* Users: Responsible for creating and maintaining secure passwords and adhering to this policy.
* IT Department: Responsible for enforcing this policy, providing support, and ensuring systems comply with password security standards.
* Managers: Responsible for ensuring their team members understand and comply with this policy.
* Security Team: Responsible for monitoring and responding to security incidents related to password breaches.

Policy

Password Creation

* Passwords must be at least [minimum length] characters long.
* Passwords must contain a mix of uppercase letters, lowercase letters, numbers, and special characters.
* Passwords must not contain easily guessable information such as usernames, birthdates, or common words.
* Passwords must be unique and not reused across different systems or accounts.

Password Protection

* Passwords must not be shared with anyone, including supervisors and IT staff.
* Passwords must not be written down or stored in an unsecured manner.
* Passwords must be changed immediately if they are suspected to be compromised.
* Multi-factor authentication (MFA) must be enabled where possible.

Password Management

* Passwords must be changed every [number] days.
* Users will be notified [number] days before their password expires.
* Accounts will be locked after [number] failed login attempts.
* Users must not use the same password for [number] previous password cycles.

Password Storage

* Passwords must be stored using strong encryption methods.
* Passwords must not be stored in plain text.

Compliance

* All employees, contractors, and third-party users must comply with this policy.
* Non-compliance may result in disciplinary action, up to and including termination of employment.
* Regular audits will be conducted to ensure compliance with this policy.

Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment.

Review and Update

This policy will be reviewed annually and updated as necessary to ensure its effectiveness.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | [Date] | Initial creation | [Name] |

# Third-Party Vendor Management Policy

Purpose

The purpose of this policy is to establish guidelines for managing and monitoring third-party vendor relationships to ensure that all vendors meet the organization’s standards for security, compliance, and performance. This policy aims to mitigate risks associated with third-party services and ensure the protection of organizational data and assets.

Scope

This policy applies to all employees, contractors, and third-party vendors who engage in business activities with the organization. It covers all stages of vendor management, including selection, onboarding, monitoring, and offboarding.

Roles and Responsibilities

* Senior Management: Approve and oversee the implementation of the vendor management policy.
* Vendor Management Team: Conduct risk assessments, due diligence, and ongoing monitoring of vendors.
* Procurement Department: Ensure that contracts and service level agreements (SLAs) meet organizational standards.
* IT Department: Ensure data security and confidentiality standards are met by vendors.
* Compliance Officer: Monitor compliance with regulatory requirements and organizational policies.
* Business Units: Identify and communicate vendor performance issues.

Policy

Vendor Risk Assessment Procedures

* Conduct a risk assessment for each vendor to identify potential risks and determine risk levels.
* Document and review risks annually or when significant changes occur.

Due Diligence Requirements

* Perform due diligence to evaluate the vendor's financial stability, reputation, and operational capabilities.
* Verify vendor compliance with relevant laws and regulations.

Data Security and Confidentiality Standards

* Ensure that vendors have adequate security measures to protect organizational data.
* Require vendors to sign confidentiality agreements and adhere to data protection policies.

Contract and SLA Management

* Include specific performance metrics, security requirements, and compliance obligations in all contracts and SLAs.
* Review and update contracts and SLAs regularly to reflect changes in organizational needs and regulatory requirements.

Ongoing Monitoring and Performance Reviews

* Conduct regular performance reviews to evaluate vendor performance against agreed-upon metrics.
* Implement corrective actions if vendors fail to meet performance standards.

Compliance with Regulatory Requirements

* Ensure that all vendor activities comply with applicable laws and regulations.
* Monitor changes in regulations and update vendor management practices accordingly.

Termination or Offboarding Protocols

* Develop a termination plan for ending vendor relationships, including data return or destruction requirements.
* Conduct an exit review to ensure all contractual obligations are fulfilled.

Compliance

All employees and contractors must adhere to this policy. Non-compliance may result in disciplinary action, up to and including termination.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | [Date] | Initial creation | [Name] |

# Security Awareness and Training Policy

Purpose

The purpose of this policy is to establish guidelines for the security awareness and training programs within the organization. These programs are designed to ensure all employees understand the importance of information security and are equipped with the knowledge and skills to protect the organization's information assets.

Scope

This policy applies to all employees, contractors, and third-party personnel who have access to the organization’s information systems and data. It covers all information assets, whether electronic, physical, or intellectual, and includes all forms of communication and data transfer.

Roles and Responsibilities

Chief Information Security Officer (ISO)

* Develops and maintains the security awareness and training program.
* Monitors compliance with the policy.
* Ensures regular updates to the training materials.

Department Managers

* Ensure their teams complete mandatory training requirements.
* Promote security awareness activities within their departments.

Employees

* Complete all mandatory security training sessions.
* Participate in ongoing security awareness activities.
* Report any security incidents or concerns immediately.

Policy

Mandatory Training Requirements

* All new employees must complete initial security training within the first 30 days of employment.
* Annual refresher courses are required for all employees.
* Specialized training sessions for employees in high-risk roles.

Awareness Activities

* Monthly security newsletters.
* Regular phishing simulation exercises.
* Workshops and webinars on emerging security threats.

Monitoring and Effectiveness Metrics

* Track completion rates of mandatory trainings.
* Monitor the frequency and resolution of reported security incidents.
* Evaluate the results of phishing simulations and other awareness activities.

Enforcement Measures

* Non-compliance with mandatory training will result in disciplinary actions.
* Repeated failure to adhere to security policies may lead to termination of employment.

Procedures for Policy Review and Updates

* Annual review of the policy by the Chief Information Security Officer.
* Incorporate feedback from employees and stakeholders.
* Update training materials and awareness activities as needed.

Compliance

All employees are required to adhere to the security awareness and training policy. Failure to comply may result in disciplinary actions, up to and including termination of employment.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | [Date] | Initial creation | [Name] |