Information Security Policy

Effective Date: April 7, 2025

Last Revised: April 7, 2025

Policy Owner: Information Technology Department

Purpose

This policy establishes guidelines and requirements for protecting [Company Name]'s information assets and systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Scope

This policy applies to all employees, contractors, consultants, temporary workers, and other personnel who have access to [Company Name]'s information assets, regardless of location or employment status.

Policy Statements

Access Control

1. **Principle of Least Privilege:** Users shall be granted the minimum system access necessary to perform their job functions.
2. **Account Management:**
   - All user accounts must be uniquely identifiable to individual users
   - Shared accounts are prohibited except where technically necessary and approved by IT
   - Access rights must be reviewed quarterly
   - Access must be promptly revoked when no longer required
3. **Authentication:**
   - Multi-factor authentication is required for all remote access and privileged accounts
   - Passwords must comply with the Password Policy
   - Default credentials must be changed before systems are deployed in production

Asset Management

1. All information assets must be:
   - Identified and inventoried
   - Classified according to sensitivity (Public, Internal, Confidential, Restricted)

- Labeled appropriately
- Protected according to their classification level

2. Asset owners must be designated for all information assets and are responsible for their protection.

Network Security

1. **Perimeter Protection:**
   - Firewalls must be deployed at network boundaries
   - Intrusion detection/prevention systems must be implemented
   - All network traffic must be monitored and logged
2. **Segmentation:**
   - Networks must be segmented based on security requirements
   - Critical systems must reside in separate security zones
3. **Wireless Networks:**
   - Corporate wireless networks must use WPA3 encryption at minimum
   - Guest networks must be segregated from corporate networks

System Security

1. **Hardening:**
   - All systems must be hardened according to industry best practices
   - Unnecessary services, applications, and ports must be disabled
   - Default configurations must be modified to enhance security
2. **Patching:**
   - Security patches must be applied within:
     - Critical: 24 hours
     - High: 7 days
     - Medium: 30 days
     - Low: 90 days
3. **Malware Protection:**
   - All systems must have approved anti-malware solutions installed
   - Anti-malware definitions must be updated daily
   - Scans must be performed weekly at minimum

Data Protection

1. **Encryption:**
   - Confidential and Restricted data must be encrypted in transit and at rest
   - Minimum encryption standards: AES-256 for data at rest, TLS 1.3 for data in transit
   - Encryption keys must be properly managed and protected
2. **Data Handling:**
   - Confidential information must not be stored on unencrypted portable devices
   - Clear desk and clear screen policies must be enforced
   - Data must be securely disposed of when no longer needed

Incident Response

1. All security incidents must be reported to the IT Security team immediately.
2. The Incident Response Plan must be followed to:
   - Identify and contain the incident
   - Eradicate the cause
   - Recover affected systems
   - Analyze and document lessons learned
3. Records of security incidents must be maintained.

Business Continuity

1. Critical systems must have:
   - Regular backups
   - Documented recovery procedures
   - Tested recovery capabilities
2. Disaster recovery and business continuity plans must be:
   - Documented
   - Tested annually
   - Updated based on test results

Compliance and Auditing

1. System logs must be maintained for all critical systems and retained for at least 12 months.
2. Security controls must be regularly audited for effectiveness.
3. Compliance with this policy and related standards must be verified through:
   - Regular self-assessments

  - Internal audits
  - External assessments where required

Third-Party Security

1. Third parties must comply with this policy when accessing or processing company information.
2. Security requirements must be included in all contracts with third parties.
3. Third-party security must be assessed before engagement and periodically thereafter.

Enforcement

Violations of this policy may result in:

- Revocation of system access
- Disciplinary action up to and including termination
- Legal action where applicable

Related Documents

- Password Policy
- Acceptable Use Policy
- Data Classification Policy
- Incident Response Plan
- Business Continuity Plan

Exceptions

Exceptions to this policy must be:

- Documented
- Approved by the Chief Information Security Officer
- Reviewed annually

Review

This policy shall be reviewed annually and updated as necessary to reflect changes in technology, business requirements, or regulatory obligations.

For questions about this policy, contact the Information Security team at security@companyname.com.