Information Technology Security Policy

Effective Date: January 2026
Version: 1.0
Classification: Internal
Last Updated: January 2026

---

1. Executive Overview

This Information Technology Security Policy establishes the framework for protecting organizational information assets, systems, and infrastructure from unauthorized access, disclosure, and malicious activities. The policy is aligned with NIST Cybersecurity Framework (CSF 2.0) and industry best practices.

---

2. Information Security Objectives

- **Confidentiality:** Ensure authorized access only
- **Integrity:** Protect data accuracy and completeness
- **Availability:** Maintain systems and services accessibility
- **Compliance:** Meet regulatory and statutory requirements
- **Risk Management:** Identify, assess, and mitigate security threats

---

3. Scope and Applicability

This policy applies to: - All employees, contractors, and third-party vendors - All organizational IT systems, networks, and data - All devices accessing corporate networks (laptops, phones, tablets) - Cloud services and external applications used for business purposes

---

4. Information Access and Authentication

4.1 User Access Controls

- **Unique user IDs:** Each employee receives a unique login credential
- **Strong passwords:** Minimum 12 characters with uppercase, lowercase, numbers, and symbols
- **Password expiry:** Reset every 90 days; no reuse of last 5 passwords
- **Multi-factor authentication (MFA):** Required for all administrative and sensitive systems
- **Access reviews:** Quarterly review of user access rights by department managers

4.2 Least Privilege Principle

- Users are granted only the minimum access necessary for their role
- Role-based access controls (RBAC) enforced across systems
- Administrative access logged and monitored
- Access immediately revoked upon employee departure

4.3 Remote Access

- **VPN requirement:** All remote connections must use company-provided VPN
- **Device requirements:** Encryption, antivirus, and updated patches mandatory
- **Monitoring:** Remote sessions logged with activity tracking
- **Session timeout:** Automatic disconnect after 30 minutes of inactivity

---

5. Data Protection and Encryption

5.1 Data Classification

- **Critical:** Customer data, financial records, trade secrets
- **Sensitive:** Internal financial data, employee information
- **Internal:** General business information
- **Public:** Published or shareable information

5.2 Encryption Standards

- **Data in transit:** TLS 1.2+ for all web communications; encrypted VPN tunnels
- **Data at rest:** AES-256 encryption for sensitive databases and backups
- **USB/removable media:** Full-disk encryption required for all company devices
- **Personal devices:** Not permitted for sensitive data; BYOD policy managed centrally

5.3 Data Retention and Disposal

- Data retained only as long as necessary for business or legal purposes
- Secure deletion: Data overwritten using industry-standard methods (NIST SP 800-88)
- Backup retention: Critical systems backed up daily; retention policy: 90 days minimum, 1 year maximum

---

6. Acceptable Use Policy

6.1 Permitted Uses

- Business communications and collaboration
- Customer and vendor interactions
- Professional development and research
- Compliant personal use (limited non-business activities during breaks)

6.2 Prohibited Uses

- Unauthorized access to systems or data
- Downloading, distributing, or creating malware
- Accessing pornography, hate content, or illegal material
- Harassment, discrimination, or threatening communications
- Circumventing security controls or system restrictions
- Intentional data destruction or system disruption
- Mining cryptocurrency using company resources
- Unauthorized software installation

6.3 Monitoring

- Email and internet usage may be monitored for security and compliance
- Network traffic analyzed for anomalies and threats
- Monitoring notices displayed at login
- Personal privacy respected; monitoring limited to business purposes

---

7. Incident Response and Reporting

7.1 Security Incident Definition

Suspected incidents include: - Unauthorized access attempts - Data breaches or suspected data leaks - Malware infections or suspicious files - Lost or stolen devices - Phishing or social engineering attempts - System unavailability or degraded performance

7.2 Reporting Procedure

Employees must report incidents immediately to: - IT Security team: security@company.com - Direct manager (for awareness) - HR (if involving personnel matters)

Do not: - Attempt to investigate on your own - Shut down systems without IT guidance - Share incident details externally - Delete evidence or logs

7.3 Response and Investigation

- IT Security team investigates within 2 hours of report

- Affected systems isolated if necessary
- Law enforcement notified for crimes (theft, data breach)
- Stakeholders and regulators notified as required by law
- Root cause analysis completed and documented

---

8. Security Awareness and Training

8.1 Mandatory Training

All employees must complete: - **Initial training:** During onboarding (2 hours) - **Annual refresher:** Security awareness training (1 hour/year) - **Role-specific training:** For administrative/sensitive roles (quarterly) - **Topics:** Password security, phishing, social engineering, data protection, incident reporting

8.2 Phishing Simulations

- Quarterly phishing simulation exercises conducted
- Employees who fall for simulations directed to remedial training
- Metrics tracked; improvement expected within 60 days

---

9. Third-Party and Vendor Security

9.1 Vendor Assessment

All third-party vendors accessing company systems must: - Complete security questionnaire - Demonstrate compliance with relevant standards (ISO 27001, SOC 2, NIST CSF) - Agree to security and confidentiality terms in contracts - Undergo annual security assessments

9.2 Vendor Access Management

- Limited, role-based access provisioned
- Monthly audit of vendor access logs
- Immediate termination of access upon contract end
- Data handling requirements clearly defined in agreements

---

10. System Security and Patch Management

10.1 Patch Management

- Security updates deployed within 2 weeks of release for critical vulnerabilities
- Operating system and software patches applied automatically where possible

- Device compliance verified before network access
- Emergency patches deployed within 24 hours

10.2 Antivirus and Threat Detection

- Antivirus software mandatory on all endpoints
- Real-time threat detection and automatic response enabled
- Endpoint Detection and Response (EDR) deployed for high-risk systems
- Threat definitions updated daily

10.3 Firewalls and Network Security

- Perimeter firewalls with intrusion detection/prevention systems
- Network segmentation isolating critical systems
- Regular vulnerability scans and penetration testing (annual)
- Logging and monitoring of all network access attempts

---

11. Physical Security

- Server rooms access restricted to authorized IT personnel
- Badge-based access with audit logs
- CCTV monitoring of sensitive areas
- Laptop/mobile device tracking enabled (MDM)
- Devices reported lost/stolen must be wiped remotely immediately

---

12. Compliance and Auditing

- Annual security audit by internal/external auditors
- Compliance assessment against NIST CSF 2.0 and applicable regulations
- Policy effectiveness reviewed semi-annually
- Board-level security reporting quarterly

---

13. Violations and Disciplinary Actions

Non-compliance may result in: - First violation: Written warning and mandatory retraining - Repeated violations: Suspension of system access for 7-30 days - Severe violations: Termination of employment - Criminal violations: Referral to law enforcement

---

Information Security Officer: [Name/Department]
Next Review Date: January 2027
Contact: security@company.com | Extension: [X]