INFORMATION TECHNOLOGY SECURITY MANUAL
TechCorp IT Security Department - Version 4.1

CHAPTER 1: INFORMATION SECURITY OVERVIEW

1.1 Security Framework

TechCorp follows the NIST Cybersecurity Framework with additional industry-specific controls. Our security program addresses identification, protection, detection, response, and recovery capabilities.

Information is classified as Public, Internal, Confidential, or Restricted based on sensitivity and impact of unauthorized disclosure.

1.2 Roles and Responsibilities

All employees are responsible for protecting company information and systems. The Chief Information Security Officer (CISO) oversees the security program.

Department heads are accountable for security within their areas. IT Security team provides guidance, monitoring, and incident response.

CHAPTER 2: ACCESS CONTROL

2.1 User Account Management

User accounts are provisioned based on job role and business need. Access follows the principle of least privilege - users receive minimum access necessary to perform their duties.

Account reviews are conducted quarterly. Terminated employee access is revoked immediately upon HR notification.

2.2 Multi-Factor Authentication

MFA is required for all systems containing sensitive data including email, VPN, cloud applications, and administrative interfaces.

Approved MFA methods include authenticator apps, hardware tokens, and SMS (for low-risk applications only).

2.3 Password Requirements

Passwords must be at least 12 characters with complexity requirements. Passphrases are encouraged over complex passwords.

Password managers are provided to all employees and are required for storing work-related credentials.

CHAPTER 3: DATA PROTECTION

3.1 Data Classification and Handling

Public data can be freely shared. Internal data is for employee use only. Confidential data requires need-to-know access. Restricted data has the highest protection requirements.

Customer data must be handled according to privacy regulations including GDPR and CCPA. Data retention policies specify storage duration and disposal requirements.

3.2 Encryption Standards
Data at rest must be encrypted using AES-256 or equivalent. Data in transit must use TLS 1.2 or higher.

Full disk encryption is required on all laptops and mobile devices. Cloud storage must use customer-managed encryption keys where available.

3.3 Backup and Recovery
Critical data is backed up daily with weekly full backups. Backup integrity is tested monthly. Recovery procedures are documented and tested quarterly.

Backups are stored in geographically separate locations with same security controls as production data.

CHAPTER 4: NETWORK SECURITY

4.1 Network Architecture
Corporate network uses segmentation to isolate critical systems. Guest networks are separated from corporate resources.

Firewalls inspect all traffic with default-deny policies. Intrusion detection systems monitor for suspicious activity.

4.2 Remote Access
VPN access is required for all remote connections to internal resources. Split tunneling is prohibited for corporate devices.

Remote desktop solutions must use multi-factor authentication and session recording for privileged access.

4.3 Wireless Security
Corporate WiFi uses WPA3 encryption with certificate-based authentication. Personal device access requires registration and compliance verification.

Guest WiFi provides internet-only access with content filtering and bandwidth limitations.

CHAPTER 5: INCIDENT RESPONSE

5.1 Incident Classification
Security incidents are classified as Low, Medium, High, or Critical based on impact and scope. Response times vary by classification level.

Critical incidents require immediate notification to CISO and executive leadership. All incidents are tracked and documented.

5.2 Response Procedures
Incident response team includes representatives from IT, Security, Legal, and Communications. Response plan includes containment, eradication, recovery, and lessons learned phases.

Forensic procedures preserve evidence while minimizing business disruption. External experts may be engaged for complex incidents.

5.3 Business Continuity
Disaster recovery plans are tested annually. Critical systems have defined recovery time objectives (RTO) and recovery point objectives (RPO).

Alternate facilities and cloud resources provide backup capability. Communication plans ensure stakeholder notification during outages.

CHAPTER 6: COMPLIANCE AND AUDIT

6.1 Regulatory Compliance
TechCorp complies with SOX, PCI DSS, HIPAA (where applicable), and other relevant regulations. Compliance status is monitored continuously.

Third-party assessments validate security controls annually. Findings are tracked and remediated according to risk priority.

6.2 Security Awareness Training
All employees complete security awareness training annually with quarterly updates. Role-specific training is provided for IT staff and privileged users.

Phishing simulation exercises are conducted monthly with additional training for users who fail tests.

Training effectiveness is measured through assessments and incident metrics.