TechCorp

IT Security Policy

Version 3.1 | Effective: January 1, 2026

Classification: Internal - Confidential

Owner: Chief Information Security Officer (CISO)

Next Review Date: July 1, 2026

This document establishes the information security policies, standards, and guidelines for TechCorp and all its subsidiaries. Compliance with this policy is mandatory for all employees, contractors, and third-party partners who access TechCorp systems or data.

1. Purpose and Scope

This IT Security Policy establishes the framework for protecting TechCorp information assets against unauthorized access, disclosure, modification, destruction, or interference. It applies to all information systems, data, networks, applications, and cloud services owned, operated, or managed by TechCorp, regardless of location or hosting model.

The scope of this policy encompasses:

- All employees, contractors, interns, and temporary workers
- All computing devices (company-owned and BYOD) that access TechCorp resources
- All cloud services and SaaS applications used for business purposes
- All data created, received, stored, or transmitted in the course of business
- All physical locations including offices, data centers, and remote work environments
- All third-party vendors, partners, and service providers with access to TechCorp data

This policy is reviewed and updated semi-annually by the Information Security team and approved by the CISO and CTO. All employees receive notification of policy changes and must acknowledge updated versions within 14 days.

2. Access Control and Identity Management

2.1 Authentication Requirements

All access to TechCorp systems must be authenticated using approved methods. The following minimum requirements apply:

- Passwords must be at least 16 characters long and include a mix of uppercase, lowercase, numbers, and special characters
- Multi-factor authentication (MFA) is required for all systems. Acceptable second factors include hardware security keys (preferred), authenticator apps (TOTP), and push notifications. SMS-based MFA is not permitted for production systems
- Passwords must not be reused across systems and must not match any of the previous 24 passwords
- Password managers (1Password for Teams) are mandatory for storing and generating credentials
- Biometric authentication is permitted as a convenience factor but must not be the sole authentication method

2.2 Authorization and Least Privilege

Access to systems and data follows the principle of least privilege. Users are granted only the minimum access necessary to perform their job functions.

- Access requests must be submitted through the IT Service Portal and approved by the resource owner and the employee manager
- Privileged access (admin, root, superuser) requires additional approval from the Security team and is subject to quarterly review
- Service accounts must use API keys or certificates rather than passwords, rotated every 90 days, and monitored for anomalous usage
- Temporary elevated access may be granted through the just-in-time (JIT) access system for up to 8 hours

2.3 Access Reviews

Access rights are reviewed regularly to ensure continued appropriateness:

- Quarterly: All privileged access reviewed by Security team and resource owners
- Semi-annually: All user access reviewed by department managers
- Immediately: Access revoked upon role change, transfer, or termination
- Annually: Comprehensive access certification by all resource owners

2.4 Single Sign-On (SSO)

All SaaS applications and internal systems must integrate with TechCorp centralized identity provider (Okta) for single sign-on. Applications that do not support SAML 2.0 or OIDC require a security exception approved by the CISO. The current exception list is maintained in the security wiki and reviewed quarterly.

3. Network Security

3.1 Network Architecture

TechCorp network infrastructure follows a zero-trust architecture model where no device, user, or network segment is implicitly trusted. All access decisions are made based on identity, device posture, and contextual signals.

- Network segmentation isolates production, staging, development, and corporate environments
- All inter-segment traffic passes through next-generation firewalls with deep packet inspection
- Micro-segmentation is enforced at the workload level in cloud environments using service mesh and security groups
- Default-deny firewall rules: all traffic is blocked unless explicitly allowed by an approved rule

3.2 Virtual Private Network (VPN)

Remote access to internal resources requires connection through the corporate VPN (WireGuard). VPN requirements include:

- Split-tunnel VPN is not permitted; all traffic must route through the VPN when connected
- VPN sessions automatically disconnect after 12 hours of inactivity
- VPN clients must verify device compliance (OS patch level, disk encryption, antivirus) before granting access
- Geographic restrictions: VPN access is blocked from countries on the OFAC sanctions list

3.3 Wireless Security

All TechCorp office wireless networks use WPA3-Enterprise with certificate-based authentication. Guest networks are isolated from corporate resources with bandwidth throttling and content filtering. Personal hotspots may not be used to connect company devices without VPN.

3.4 DNS and Web Filtering

TechCorp deploys DNS-level filtering and web proxy services to block known malicious domains, phishing sites, and categories of content that pose security risks. Categories blocked include: malware distribution, command-and-control, cryptomining, newly registered domains (less than 30 days old), and anonymizing proxies.

4. Data Protection and Encryption

4.1 Data Classification

All TechCorp data must be classified according to the four-tier classification system: Public, Internal, Confidential, and Restricted. Data owners are responsible for classifying their data and ensuring appropriate controls are applied.

4.2 Encryption Standards

The following encryption standards are mandatory across all TechCorp systems:

- Data in transit: TLS 1.3 (preferred) or TLS 1.2 with strong cipher suites. TLS 1.0 and 1.1 are prohibited. Certificate pinning required for mobile apps.
- Data at rest: AES-256-GCM for all Confidential and Restricted data. Full-disk encryption (BitLocker/FileVault) mandatory on all endpoints.
- Database encryption: Transparent Data Encryption (TDE) for databases containing customer data. Column-level encryption for PII fields.
- Key management: All encryption keys managed through AWS KMS or HashiCorp Vault. Keys rotated annually or immediately upon suspected compromise.
- Email encryption: S/MIME or PGP for sensitive communications. All email with Confidential/Restricted data to external recipients must be encrypted.

4.3 Data Loss Prevention (DLP)

TechCorp deploys DLP controls across email, cloud storage, endpoints, and web traffic to prevent unauthorized exfiltration of sensitive data. DLP rules detect and block: credit card numbers, Social Security numbers, API keys in code, customer PII in unapproved channels, and bulk data transfers exceeding thresholds. Violations trigger alerts to the SOC.

4.4 Data Retention and Disposal

Data must be retained only as long as required by business need, legal obligation, or regulatory requirement:

- Customer data: Duration of customer relationship plus 3 years
- Employee records: Duration of employment plus 7 years
- Financial records: 7 years per IRS requirements
- Security logs: 1 year hot storage, 6 years cold storage
- Marketing data: 2 years from last engagement

When data reaches end of retention, it must be securely destroyed per NIST SP 800-88 guidelines. Physical media shredded with certificate of destruction.

5. Endpoint Security

5.1 Device Management

All devices accessing TechCorp resources must be enrolled in MDM (Jamf for macOS, Intune for Windows). MDM enforces:

- OS updated to latest stable version within 14 days of release (7 days for critical patches)
- Full-disk encryption enabled and verified
- Firewall enabled with default-deny inbound rules
- Automatic screen lock after 5 minutes of inactivity
- CrowdStrike Falcon EDR agent installed and active
- Approved antivirus with real-time scanning and daily signature updates

5.2 BYOD Policy

Personal devices may access TechCorp email and collaboration tools through managed profiles. BYOD devices must have: current OS, encryption enabled, screen lock. BYOD may not access production systems, source code, or Restricted data. TechCorp may remotely wipe the managed profile on loss, theft, or separation.

5.3 Removable Media

Use of removable storage (USB, external drives, SD cards) is prohibited unless authorized by Security for documented business needs. Authorized media must be encrypted and tracked.

6. Cloud Security

6.1 Cloud Service Providers

TechCorp primarily uses AWS with GCP for AI/ML workloads. All resources provisioned through Terraform and must comply with the cloud security baseline.

6.2 Cloud Security Controls

- AWS Organization with SCPs enforcing guardrails on all accounts
- Resources tagged with: owner, environment, data-classification, cost-center, expiration-date
- Public access to storage blocked by default via organization policies
- CSPM continuously scans for misconfigurations and compliance violations
- Container images scanned before deployment; Critical/High CVEs blocked
- Secrets in AWS Secrets Manager or HashiCorp Vault, never in code or env vars

6.3 SaaS Application Security

All SaaS applications require Security team approval. Evaluation covers: SOC 2 compliance, encryption, SSO support, API security, data residency, breach notification. Shadow IT discovery performed monthly.

7. Application Security

7.1 Secure Development Lifecycle (SDL)

All TechCorp software follows a Secure Development Lifecycle integrating security at every phase:

- Design: Threat modeling using STRIDE for new features and architectural changes
- Development: Annual secure coding training; OWASP Top 10 mandatory for all developers
- Code Review: Peer review with security checklist; automated SAST on every pull request
- Testing: DAST in staging; dependency scanning (Dependabot/Snyk); annual penetration testing
- Deployment: Immutable infrastructure; automated rollback; canary deployments for production
- Operations: RASP and WAF on all public-facing applications

7.2 Vulnerability Management

Vulnerabilities triaged by CVSS score:

- Critical (9.0-10.0): Patch within 24 hours or apply compensating control
- High (7.0-8.9): Patch within 7 days
- Medium (4.0-6.9): Patch within 30 days
- Low (0.1-3.9): Patch within 90 days

Exceptions require documented risk acceptance from system owner and CISO. Vulnerability dashboard reviewed weekly.

7.3 API Security

All APIs must implement: OAuth 2.0 or API key auth, rate limiting, input validation, output encoding, and logging. Public APIs require security review. GraphQL APIs must have query depth limiting and cost analysis.

8. Incident Response

8.1 Incident Response Plan

TechCorp maintains a comprehensive incident response plan aligned with NIST SP 800-61. Tested via quarterly tabletop exercises and annual full simulations. Team includes Security, Engineering, Legal, Communications, and executives.

8.2 Incident Classification

- SEV1 Critical: Confirmed breach, ransomware, system compromise. Immediate 24/7 response, executive notification in 30 min.
- SEV2 High: Potential exposure, phishing success, multi-system malware, DoS. Response within 1 hour.
- SEV3 Medium: Policy violation, failed attacks, suspicious activity. Response within 4 business hours.
- SEV4 Low: Informational events, minor deviations. Response within 1 business day.

8.3 Breach Notification

For confirmed breaches involving personal information, TechCorp notifies affected individuals within 72 hours (GDPR). Notification includes: incident description, data types affected, mitigation steps, recommended actions, and contact info. Regulatory authorities notified as required by law.

9. Business Continuity and Disaster Recovery

9.1 Recovery Objectives

- RTO: 4 hours for Tier 1 (customer-facing), 24 hours for Tier 2 (internal)
- RPO: 1 hour for Tier 1 (continuous replication), 24 hours for Tier 2 (daily backups)
- Backup testing: Monthly restore tests for critical DBs; quarterly full-environment recovery

9.2 Backup Requirements

- Databases: Continuous replication to secondary region, 35-day point-in-time recovery
- File storage: Daily incremental, weekly full, retained 90 days
- Config/IaC: Version control with off-site mirror
- All backups encrypted AES-256 in geographically separate region
- Backup integrity verified automatically; failures alert on-call engineer

9.3 DR Testing

DR tests quarterly for Tier 1, annually for Tier 2. Includes failover, data integrity validation, performance benchmarks, and failback. Results documented with tracked remediation.

10. Compliance and Audit

10.1 Regulatory Framework

- SOC 2 Type II: Annual audit (Security, Availability, Confidentiality)
- GDPR: DPAs with all EU processors; DPIAs for high-risk processing; appointed DPO
- CCPA/CPRA: Consumer data access, deletion, and opt-out mechanisms
- HIPAA: BAAs for healthcare customers; administrative, physical, technical safeguards
- PCI DSS Level 1: Annual QSA audit for payment processing
- ISO 27001: Certified ISMS with annual surveillance audits

10.2 Internal Audits

Risk-based audits throughout the year. Findings classified Critical/High/Medium/Low. Remediation: Critical 30 days, High 60, Medium 90, Low 180. Overdue findings escalated to CISO and CTO.

10.3 Security Metrics

Monthly executive reporting on:

- MTTD and MTTR for security incidents
- Phishing simulation click and reporting rates
- Systems with critical/high vulnerabilities past SLA
- Security training completion rate
- Security exceptions and risk acceptances
- Third-party risk assessment completion

Appendix A: Approved Security Tools

- Identity & Access: Okta (SSO/MFA), 1Password (password management)
- Endpoint: CrowdStrike Falcon (EDR), Jamf Pro (macOS), Intune (Windows)
- Network: Cloudflare (WAF/DDoS), WireGuard (VPN), Palo Alto (firewall)
- Cloud: AWS Security Hub, Wiz (CSPM), Terraform (IaC)
- Application: Snyk (dependency scanning), SonarQube (SAST), Burp Suite (DAST)
- Data: AWS KMS / HashiCorp Vault (keys), Nightfall (DLP)
- Monitoring: Datadog (observability), Splunk (SIEM), PagerDuty (incidents)
- GRC: Vanta (compliance), ServiceNow (risk management)

Appendix B: Security Contacts

SOC: soc@techcorp.com | 24/7 Hotline: +1-888-SEC-TCOP

CISO Office: ciso@techcorp.com

Security Architecture: secarch@techcorp.com

Incident Response: incident@techcorp.com

Vulnerability Disclosure: security@techcorp.com

Privacy & Data Protection: dpo@techcorp.com

Appendix C: Document History

- v1.0 (Jan 2023): Initial policy release
- v2.0 (Jul 2023): Added cloud security and zero-trust sections
- v2.1 (Jan 2024): Updated encryption standards, added BYOD policy
- v3.0 (Jul 2025): Major revision: API security, CSPM, DLP; ISO 27001 alignment
- v3.1 (Jan 2026): Updated vendor requirements, SaaS governance, incident classification