Information Security and Incident Response Policy

TechFlow Solutions, Inc.
Policy Number: TS-SEC-002
Effective Date: January 1, 2024
Last Revised: December 15, 2023
Policy Owner: Sarah Chen, Chief Information Security Officer

---

1. PURPOSE AND SCOPE

This policy establishes information security requirements, incident response procedures, and compliance protocols for TechFlow Solutions. It applies to all employees, contractors, and third parties accessing company systems, ensuring protection of customer data and maintenance of SOC2 Type II compliance.

2. PASSWORD REQUIREMENTS AND AUTHENTICATION

2.1 Password Policy Standards

Minimum Password Requirements: - **Length:** 12 characters minimum (passphrases encouraged) - **Complexity:** Must include uppercase, lowercase, numbers, and symbols - **Uniqueness:** Unique passwords for each system and service - **History:** Cannot reuse last 12 passwords - **Expiration:** 90 days for privileged accounts, no expiration for standard accounts with MFA

Password Strength Guidelines: - **Recommended:** Passphrases with 4+ random words (e.g., "Coffee-Mountain-Purple-Database-42") - **Avoid:** Dictionary words, personal information, keyboard patterns - **Tools:** 1Password Business required for password generation and storage - **Sharing:** Passwords must never be shared or written down

2.2 Multi-Factor Authentication (MFA) Requirements

Mandatory MFA Systems: - All business applications and cloud services - VPN access for remote connections - Administrative access to any system - Email and collaboration platforms (Google Workspace, Slack) - Customer-facing systems and databases

Approved MFA Methods: - **Primary:** YubiKey 5 NFC hardware tokens (company-provided) - **Secondary:** Google Authenticator or Authy mobile apps - **Backup:** Company-provided backup codes (stored in 1Password) - **Prohibited:** SMS-based authentication (due to SIM swapping risks)

MFA Implementation Timeline: - **New Employees:** MFA setup required before system access - **Existing Employees:** 100% compliance achieved and maintained - **Contractors:** MFA required for any system access - **Third Parties:** MFA required per vendor security agreements

2.3 Account Management

Account Provisioning: - **Automated Provisioning:** Role-based access via Okta identity management - **Approval Workflow:** Manager approval required for all access requests - **Least Privilege:** Minimum necessary access granted initially - **Review Cycle:** Quarterly access review and certification

Account Lifecycle Management: - **Onboarding:** Account creation on start date - **Role Changes:** Access updated within 24 hours of role change - **Termination:** Immediate account deactivation upon termination - **Dormant Accounts:** Accounts disabled after 90 days of inactivity

Privileged Account Controls: - **Separate Accounts:** Administrative accounts separate from standard accounts - **Time Limitations:** Administrative sessions expire after 2 hours - **Approval Required:** Written approval for privileged access requests - **Monitoring:** Enhanced logging and monitoring for all privileged access

3. VPN USAGE REQUIREMENTS

3.1 VPN Connection Standards

Mandatory VPN Usage: - **All Remote Work:** VPN required for any work outside TechFlow offices - **Public Networks:** Always-on VPN when using public Wi-Fi - **Customer Data Access:** VPN required for any customer data access - **Personal Devices:** VPN required if accessing company resources

Approved VPN Solutions: - **Primary:** Cisco AnyConnect (company-managed) - **Backup:** GlobalProtect (emergency use only) - **Configuration:** Centrally managed with automatic updates - **Kill Switch:** Automatic internet disconnection if VPN fails

3.2 VPN Security Requirements

Technical Requirements: - **Encryption:** AES-256 encryption for all VPN traffic - **Protocols:** IKEv2/IPSec and OpenVPN protocols only - **DNS Protection:** Company-controlled DNS servers only - **Split Tunneling:** Disabled to ensure all traffic through VPN

Usage Monitoring: - **Connection Logging:** All VPN connections logged and monitored - **Anomaly Detection:** Automated detection of unusual connection patterns - **Geographic Restrictions:** Connections from high-risk countries flagged - **Compliance Reporting:** Monthly VPN usage compliance reports

3.3 VPN Access Management

Access Provisioning: - **Role-Based Access:** VPN access based on job requirements - **Geographic Permissions:** Country-specific access permissions - **Time Restrictions:** Business hours only for some roles - **Device Registration:** Only company-managed devices allowed

Performance and Reliability: - **Multiple Gateways:** Redundant VPN gateways in multiple regions - **Load Balancing:** Automatic load balancing across gateways - **Failover:** Automatic failover to backup gateways - **Performance Monitoring:** Real-time monitoring of VPN performance

4. DATA BREACH NOTIFICATION PROCEDURES

4.1 Incident Classification and Response Times

Data Breach Categories:

Category 1 - Critical (Response within 15 minutes): - Customer PII or financial data exposure - Healthcare data (PHI) exposure for healthcare clients - Credit card or payment information exposure - Large-scale data exposure (>1,000 records)

Category 2 - High (Response within 2 hours): - Internal confidential data exposure - Employee personal information exposure - Proprietary business information exposure - Security system compromise

Category 3 - Medium (Response within 24 hours): - Internal system unauthorized access - Non-sensitive data exposure - Security policy violations - Suspicious activity detection

4.2 Internal Notification Process

Immediate Notification (Within 15 minutes): 1. **Employee Discovery:** Employee discovers or suspects breach 2. **Security Operations Center:** security-emergency@techflow.com, +1 (415) 555-SEC1 3. **CISO Notification:** Immediate phone call to Sarah Chen +1 (415) 987-6543 4. **Incident Declaration:** Formal incident declared in ServiceNow

Executive Notification (Within 1 hour): - **CEO:** David Park (for Category 1 incidents) - **CTO:** Jennifer Liu (for all technical incidents) - **Legal:** Amanda Foster (for regulatory implications) - **Customer Success:** For customer-impacting incidents

Team Assembly (Within 2 hours): - **Incident Commander:** CISO or designated security lead - **Technical Team:** IT Director and relevant technical staff - **Legal Team:** Legal counsel and compliance officer - **Communications:** Marketing Director for external communications

4.3 Customer Notification Requirements

Regulatory Notification Timelines: - **GDPR:** 72 hours to regulatory authorities, no undue delay to data subjects - **CCPA:** Without unreasonable delay, no later than legally required - **HIPAA:** 60 days for individuals, 60 days for HHS, immediately for media (500+ records) - **State Laws:** Various state requirements (24 hours to several days)

Customer Notification Process: 1. **Impact Assessment:** Determine which customers affected (within 4 hours) 2. **Legal Review:** Legal approval of notification content (within 8 hours) 3. **Executive Approval:** CEO/CISO approval of customer communications 4. **Customer Notification:** Direct notification to affected customers within 72 hours 5. **Regulatory Filing:** Appropriate regulatory notifications per jurisdiction

Notification Content Requirements: - **Incident Description:** Clear explanation of what happened - **Data Involved:** Specific types of data potentially affected - **Timeline:** When incident occurred and was discovered - **Response Actions:** Steps taken to address the incident - **Customer Actions:** Recommended actions for customers - **Contact Information:** Dedicated incident response contact details

4.4 External Communication Management

Media Relations: - **Spokesperson:** CEO or designated company spokesperson only - **Message Coordination:** All external communications coordinated through legal - **Press Inquiries:** Directed to press@techflow.com - **Social Media:** Monitoring and response via marketing team

Regulatory Communications: - **Primary Contact:** Legal counsel Amanda Foster - **Regulatory Filings:** Formal notifications per regulatory requirements - **Cooperation:** Full cooperation with regulatory investigations - **Documentation:** Complete documentation of all regulatory communications

5. INCIDENT SEVERITY LEVELS

5.1 Severity Classification Matrix

P0 - Critical (15-minute response): - **Customer Impact:** Customer operations significantly impacted - **Data Exposure:** Customer PII, PHI, or financial data exposed - **System Impact:** Core business systems completely down - **Security Impact:** Active security breach with ongoing access

P1 - High (2-hour response): - **Customer Impact:** Customer operations partially impacted - **Data Exposure:** Internal confidential data potentially exposed - **System Impact:** Major system functionality degraded - **Security Impact:** Security vulnerability actively being exploited

P2 - Medium (24-hour response): - **Customer Impact:** Minor customer

impact or potential for impact - **Data Exposure:** Internal data exposed but low sensitivity - **System Impact:** Non-critical system issues - **Security Impact:** Security policy violations or suspicious activity

P3 - Low (72-hour response): - **Customer Impact:** No customer impact - **Data Exposure:** Public or low-sensitivity data only - **System Impact:** Minor system issues or maintenance needed - **Security Impact:** Security awareness or training issues

5.2 Escalation Triggers

Automatic Escalation Events: - **No Response:** No response to initial notification within SLA timeframe - **Severity Increase:** Incident severity increases during investigation - **Customer Complaints:** Customer escalation or dissatisfaction - **Media Attention:** Incident gains public or media attention - **Regulatory Interest:** Regulatory authority requests information

Escalation Contacts: - **P0 Incidents:** Immediate CISO and CEO notification - **P1 Incidents:** CISO and CTO notification within 1 hour - **P2 Incidents:** Security team manager notification within 4 hours - **P3 Incidents:** Assignment to security team member

5.3 Incident Response Team Roles

Incident Commander (CISO or designee): - **Overall Response:** Coordinates entire incident response - **Decision Authority:** Makes critical decisions during incident - **External Communications:** Manages external stakeholder communications - **Resource Allocation:** Assigns resources and expertise as needed

Technical Lead (IT Director or Senior Engineer): - **Technical Investigation:** Leads technical analysis and forensics - **System Recovery:** Manages system restoration and recovery - **Evidence Collection:** Ensures proper evidence collection and preservation - **Root Cause Analysis:** Conducts technical root cause analysis

Legal and Compliance (Chief Legal Officer): - **Regulatory Requirements:** Ensures compliance with notification laws - **Legal Strategy:** Manages legal implications and strategy - **Customer Contracts:** Reviews customer notification obligations - **Documentation:** Ensures proper legal documentation

Communications (Marketing Director): - **Customer Communications:** Manages customer notification and updates - **Internal Communications:** Coordinates internal team communications - **Media Relations:** Manages media inquiries and public relations - **Stakeholder Updates:** Provides regular updates to stakeholders

6. RESPONSE TEAM ROLES AND RESPONSIBILITIES

6.1 Core Response Team Structure

Tier 1 - Security Operations Center (24/7): - **Staff:** 2 security analysts (rotating shifts) - **Responsibilities:** Initial incident detection, triage, and escalation - **Tools:** SIEM monitoring, automated alerting, incident ticketing - **Response Time:** Immediate acknowledgment, 15-minute initial assessment

Tier 2 - Security Team (Business Hours + On-Call): - **Staff:** 4 security specialists and 1 security manager - **Responsibilities:** Incident investigation, containment, and initial response - **Tools:** Forensic tools, threat intelligence, security orchestration - **Response Time:** 30 minutes for P0, 2 hours for P1

Tier 3 - Executive Response Team (On-Call): - **Staff:** CISO, CTO, Legal Counsel, CEO - **Responsibilities:** Strategic decisions, customer communications, regulatory compliance - **Authority:** Full authority to make business decisions during incidents - **Response Time:** 1 hour for P0, 4 hours for P1

6.2 Extended Response Team

Technical Specialists: - **Infrastructure Team:** Network and system administration expertise - **Development Team:** Application and database expertise - **Cloud Security:** AWS and cloud platform security expertise - **External Consultants:** Third-party incident response specialists

Business Stakeholders: - **Customer Success:** Customer impact assessment and communications - **Sales:** Customer relationship management during incidents - **Product Management:** Product impact assessment and prioritization - **Finance:** Financial impact assessment and insurance coordination

Support Functions: - **HR:** Employee communications and support - **Facilities:** Physical security and access control - **Procurement:** Emergency procurement and vendor coordination - **Administrative:** Meeting coordination, documentation, logistics

6.3 Training and Readiness

Regular Training Programs: - **Monthly Tabletop Exercises:** Scenario-based incident response training - **Quarterly Simulations:** Full-scale incident response simulations - **Annual Certification:** Incident response certification for all team members - **External Training:** Industry conferences and professional development

Readiness Assessment: - **Response Time Testing:** Regular testing of notification and response times - **Tool Proficiency:** Regular testing of incident response tools and procedures - **Documentation Reviews:** Quarterly review and update of response procedures - **Lessons Learned:** Post-incident review and procedure improvement

7. COMMUNICATION PROTOCOLS

7.1 Internal Communication Channels

Primary Communication Platform: - **Slack:** #security-incidents channel for real-time coordination - **Conference Bridge:** Dedicated incident response bridge number - **Email:** security-incidents@techflow.com for formal notifications - **Mobile:** Emergency notification via phone calls and SMS

Communication Templates: - **Initial Notification:** Standardized incident declaration template - **Status Updates:** Regular update template with standard information - **Resolution Notice:** Incident closure and lessons learned template - **Executive Summary:** High-level summary for executive team

7.2 External Communication Management

Customer Communication Strategy: - **Transparency:** Proactive, honest communication about incidents - **Timeliness:** Regular updates every 2 hours during active incidents - **Specificity:** Clear information about impact and resolution steps - **Follow-up:** Post-incident communication with lessons learned

Regulatory Communication: - **Legal Review:** All regulatory communications reviewed by legal team - **Timely Filing:** Notifications filed within required timeframes - **Complete Information:** Full disclosure per regulatory requirements - **Ongoing Cooperation:** Continued cooperation with regulatory investigations

7.3 Crisis Communication Procedures

Crisis Communication Team: - **Lead:** CEO David Park - **Backup:** CMO or designated spokesperson - **Legal Advisor:** Chief Legal Officer Amanda Foster - **Technical Advisor:** CISO Sarah Chen

Crisis Communication Protocols: - **Unified Messaging:** Single, consistent message across all channels - **Rapid Response:** Initial response within 2 hours of public disclosure - **Stakeholder Priority:** Customers, employees, partners, media, public - **Message Control:** All communications pre-approved by crisis team

8. REGULATORY COMPLIANCE REQUIREMENTS

8.1 SOC2 Type II Compliance

Control Requirements: - **Incident Response:** Documented incident response procedures and testing - **Change Management:** Formal change management for security systems - **Access Controls:** Regular review and certification of access rights - **Monitoring:** Continuous monitoring and alerting for security events

Evidence Collection: - **Incident Documentation:** Complete documentation of all security incidents - **Control Testing:** Regular testing of security controls and procedures - **Risk Assessments:** Annual risk assessments and control evaluations - **Third-Party Reviews:** Annual SOC2 audit by external auditor

8.2 Data Protection Regulations

GDPR Compliance (EU Data): - **Data Protection Officer:** Designated DPO for GDPR compliance - **Privacy by Design:** Privacy considerations in all system designs - **Data Subject Rights:** Processes for handling data subject requests - **Cross-Border Transfers:** Standard Contractual Clauses for data transfers

CCPA Compliance (California Data): - **Consumer Rights:** Processes for handling consumer privacy requests - **Data Inventory:** Comprehensive inventory of personal data processing - **Opt-Out Mechanisms:** Clear opt-out processes for data sales - **Service Provider Agreements:** Compliant agreements with service providers

HIPAA Compliance (Healthcare Clients): - **Business Associate Agreements:** Signed BAAs with healthcare clients - **Administrative Safeguards:** Administrative controls for PHI protection - **Physical Safeguards:** Physical controls for PHI access and storage - **Technical Safeguards:** Technical controls for PHI transmission and storage

8.3 Industry-Specific Requirements

Financial Services (PCI DSS): - **Cardholder Data:** Special handling for payment card information - **Network Segmentation:** Separate network segments for card data processing - **Regular Testing:** Quarterly vulnerability scans and annual penetration testing - **Vendor Management:** PCI compliance for all payment processing vendors

Healthcare (HITECH): - **Breach Notification:** Enhanced breach notification requirements - **Risk Assessments:** Regular risk assessments for PHI processing - **Workforce Training:** Specialized training for healthcare data handling - **Audit Controls:** Enhanced audit controls for PHI access

9. CONTACT INFORMATION

9.1 Emergency Response Contacts (24/7)

- **Security Operations Center:** security-emergency@techflow.com, +1 (415) 555-SEC1 (7321)
- **CISO:** Sarah Chen, +1 (415) 987-6543
- **CTO:** Jennifer Liu, +1 (512) 876-5432
- **CEO:** David Park, +1 (415) 234-5678

9.2 Incident Response Team

- **Security Manager:** security-manager@techflow.com, +1 (415) 555-7890
- **IT Director:** Marcus Rodriguez, marcus.rodriguez@techflow.com
- **Legal Counsel:** Amanda Foster, amanda.foster@techflow.com
- **Customer Success Director:** customer-incidents@techflow.com

9.3 External Partners

- **Incident Response Partner:** CyberSecure Inc., +1 (512) 555-4321
- **Legal Counsel:** Morrison & Associates, +1 (415) 555-9876
- **Insurance:** Travelers Cyber, +1 (800) 238-6225
- **PR Firm:** Strategic Communications, +1 (415) 555-1234

Approved By: - Sarah Chen, Chief Information Security Officer - December 15, 2023 - Amanda Foster, Chief Legal Officer - December 15, 2023 - Jennifer Liu, Chief Technology Officer - December 15, 2023 - David Park, Chief Executive Officer - December 15, 2023

This policy is proprietary and confidential to TechFlow Solutions, Inc.