Device Security and Lost Equipment Policy

TechFlow Solutions, Inc.
Policy Number: TS-SEC-001
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 procedures for securing company devices and managing incidents involving lost, stolen, or compromised equipment at TechFlow Solutions. This policy applies to all employees, contractors, and third parties who are issued or have access to company devices.

2. DEVICE SECURITY REQUIREMENTS

2.1 Physical Security

- Devices must be locked when unattended (screen lock within 5 minutes)
- Full disk encryption required (FileVault for macOS, BitLocker for Windows)
- Strong authentication (minimum 12-character password + 2FA with YubiKey)
- Cable locks mandatory in public spaces and co-working locations
- Devices cannot be left unattended in vehicles or public areas

2.2 Digital Security

- Automatic security updates enabled
- CrowdStrike Falcon Complete endpoint protection installed
- Cisco AnyConnect VPN required for all internet access outside offices
- Regular security scans performed monthly via Jamf Pro
- Personal software installation requires IT approval

3. LOST, STOLEN, OR COMPROMISED DEVICE PROCEDURES

3.1 Immediate Response (Within 2 Hours)

Employee Actions: 1. **Secure the area** - If theft suspected, do not touch potential evidence 2. **Contact Security Operations Center (SOC):** - **Primary:** security-emergency@techflow.com - **Emergency Hotline:** +1 (415) 555-HELP (4357) - **After Hours:** +1 (415) 555-9999 3. **Report to Direct Manager** and copy people@techflow.com 4. **If theft occurred, file police report immediately** and obtain incident number

Required Information: - Employee name, department, and manager - Device type, model, serial number, and asset tag (TF-2024-XXXX format) - Last known location and approximate time - Circumstances of loss/theft - Police report number (if applicable) - Potential data exposure assessment

3.2 IT Security Response (Within 15 Minutes)

Automated Response: 1. **Remote device wipe** initiated via Jamf Pro MDM 2. **Account access suspended** for all services 3. **VPN certificates revoked** immediately 4. **Email access terminated** (Google Workspace) 5. **Slack/Teams access revoked**

Manual Response: 1. **Customer data exposure assessment** completed within 1 hour 2. **P0 incident ticket** created in ServiceNow 3. **Security team notification** to security-incidents@techflow.com 4. **Executive notification** for customer data incidents

3.3 Investigation Process

Security Team Actions (Within 4 Hours): 1. **Forensic review** of device access logs (30 days prior) 2. **Data classification assessment** of exposed information 3. **Risk evaluation** using company matrix 4. **Customer notification determination** per SOC2 requirements 5. **Compliance team notification** if customer data involved

4. DEVICE REPLACEMENT PROCEDURES

4.1 Emergency Replacement (Same Day)

Eligibility: Customer Success, Sales, Engineering, Security, Executive team

Locations: - **San Francisco Office:** 10 devices maintained on-site - **Austin Office:** 8 devices maintained on-site
- **Remote Workers:** Apple Store pickup via Apple Business Manager

4.2 Standard Replacement (24-48 Hours)

Timeline: - **Critical Roles:** 24 hours (Sales, Customer Success, Engineering, Security) - **Standard Roles:** 48 hours (Marketing, HR, Finance, Operations) - **Contractors:** 72 hours (additional approvals required)

Shipping: - **Carrier:** FedEx Overnight (signature required) - **Insurance:** Full replacement value ($2,400 average) - **Tracking:** Real-time SMS and email updates

4.3 Device Configuration

Standard Laptop: MacBook Pro 14" M2 Pro - 16GB RAM (32GB for Engineering) - 512GB SSD (1TB for Engineering/Design) - Touch ID, FileVault encryption - AppleCare+ coverage included

5. EMPLOYEE LIABILITY AND INSURANCE

5.1 Employee Deductible Structure

- **Standard incidents:** $200 employee deductible
- **Negligence determination:** Up to $1,000 employee liability
- **Gross negligence:** Full replacement cost ($2,400)

5.2 Insurance Coverage

- **Carrier:** Travelers Business Insurance
- **Policy:** TF-CYBER-2024-001
- **Coverage:** $2M aggregate, $50K per incident
- **Claims Hotline:** +1 (800) 238-6225

5.3 Negligence Examples

- Device left in unlocked vehicle
- Failure to use provided security equipment
- Disabling required security features
- Unreported security concerns

6. PREVENTIVE MEASURES

6.1 Training Requirements

- **New Employee:** 2-hour device security module (Week 1)
- **Annual Refresher:** Security awareness and policy updates
- **Travel Briefing:** Required for international travel
- **Platform:** KnowBe4 security awareness system

6.2 Physical Security Equipment

- **Laptop Locks:** Kensington ClickSafe cables (all employees)
- **Privacy Screens:** 3M filters (optional, 60% adoption)
- **Secure Bags:** Pacsafe anti-theft bags (frequent travelers)
- **Office Storage:** Personal lockers in SF and Austin offices

6.3 Technical Controls

- **GPS tracking** enabled on mobile devices
- **Remote wipe** tested monthly
- **Daily backups** via Druva inSync
- **RFID asset tracking** for inventory management

7. COMPLIANCE AND MONITORING

7.1 Regulatory Requirements

- **SOC2 Type II:** Annual audit by Deloitte & Touche
- **GDPR/CCPA:** Data protection compliance
- **Customer audits:** Quarterly transparency reports

7.2 Performance Metrics

- **Incident response time:** Average 12 minutes (target <15)
- **Device recovery rate:** 15% (industry average 5-10%)
- **Training completion:** 98% annual compliance
- **Cost per incident:** $2,600 average

7.3 Audit Schedule

- **Monthly:** Device inventory verification
- **Quarterly:** Security assessment and policy review
- **Semi-annually:** Incident response testing
- **Annually:** Comprehensive program evaluation

8. CONTACT INFORMATION

8.1 Emergency Contacts (24/7)

- **Security Hotline:** +1 (415) 555-SEC1 (7321)
- **Sarah Chen (CISO):** +1 (415) 987-6543
- **Jennifer Liu (CTO):** +1 (512) 876-5432

8.2 Standard Support

- **Security Operations:** security@techflow.com, +1 (415) 555-4357
- **IT Helpdesk:** helpdesk@techflow.com, +1 (415) 555-7890
- **People Operations:** people@techflow.com, +1 (415) 555-0123

8.3 External Partners

- **Legal Counsel:** Morrison & Associates, +1 (415) 555-9876
- **Forensics:** CyberSecure Inc., +1 (512) 555-4321
- **Apple Business Support:** +1 (800) APL-CARE

9. ENFORCEMENT

9.1 Violation Categories

- **Minor:** Verbal counseling (first-time, proper reporting)
- **Moderate:** Written warning (repeat or minor negligence)
- **Major:** Disciplinary action up to termination (gross negligence)

9.2 Exception Process

- **Approval:** CISO written authorization required
- **Documentation:** Risk acceptance and compensating controls
- **Review:** Quarterly exception assessment

10. RELATED POLICIES

- Information Security Policy (TS-SEC-002)
- Remote Work Policy (TS-HR-003)
- Asset Management Policy (TS-OPS-001)
- Travel and Expense Policy (TS-FIN-002)

Approved By: - Sarah Chen, Chief Information Security Officer - December 15, 2023 - Michael Torres, Chief People 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.