Endpoint Protection Policy

Document ID: IT-SEC-015 **Last Updated:** March 2024 **Owner:** IT Security **Applies To:** All Company Devices

---

Overview

This policy outlines NovaTech's endpoint protection requirements for all company-owned and managed devices. Endpoint protection is critical to our security posture and compliance requirements.

Scope

In-Scope Devices

Device Type	Protection Required
Company laptops	Full protection suite
Company desktops	Full protection suite
Company mobile devices	Mobile protection
Virtual workstations	Full protection suite
Developer machines	Full protection suite

Out of Scope

- Personal devices (covered by BYOD policy)
- Production servers (covered by server security policy)
- Network equipment (covered by network security policy)

Required Protection Components

1. CrowdStrike Falcon

Our primary endpoint protection platform

Features Enabled

Feature	Status	Description
Next-Gen Antivirus	Required	ML-based malware detection
EDR	Required	Endpoint detection and response
Device Control	Required	USB and peripheral control
Firewall Management	Required	Host-based firewall
Vulnerability Assessment	Enabled	Continuous scanning

Agent Requirements

```
Minimum Version: 6.58.0
Update Policy: Automatic
Tamper Protection: Enabled
Uninstall Protection: Enabled (IT admin only)
```

2. Disk Encryption

macOS (FileVault)

- **Status:** Required
- **Key escrow:** IT-managed recovery keys
- **Enforcement:** MDM policy

Windows (BitLocker)

- **Status:** Required
- **Key escrow:** Azure AD
- **TPM:** Required

Linux

- **Status:** Required
- **Method:** LUKS full disk encryption

3. Firewall

Requirements

Setting	Value
Status	Always On
Inbound default	Block
Outbound default	Allow
Stealth mode	Enabled

Allowed Inbound

- None by default
- AirDrop (internal network only)
- Screen sharing (IT-approved only)

4. Screen Lock

Setting	Requirement
Auto-lock	5 minutes maximum
Password required	After sleep/screensaver
Login password	Required

Mobile Device Protection

iOS Devices

MDM Requirements (Jamf)

- Device enrollment required
- Passcode: 6+ digits
- Face ID/Touch ID: Allowed
- Auto-lock: 5 minutes maximum
- Find My: Enabled
- Remote wipe: Enabled

Required Apps

- Okta Verify
- Slack
- Microsoft Defender

Android Devices

Requirements

- Work profile enrollment
- Device encryption: Required
- Screen lock: PIN, pattern, or biometric
- Unknown sources: Disabled

USB and Peripheral Controls

USB Device Policy

Device Type	Policy
Storage devices	Blocked (exceptions via IT)
Keyboards/Mice	Allowed
Webcams	Allowed
Audio devices	Allowed
Printers	Allowed (network only)
Unknown devices	Blocked

Exception Process

1. Submit request via IT Service Portal
2. Business justification required
3. Manager approval
4. IT Security review
5. Time-limited approval (30-90 days)

Software Controls

Approved Software

Software installation is managed through: - **macOS:** Jamf Self Service - **Windows:** Company Portal - **Linux:** Approved package repositories

Blocked Categories

Category	Reason
Peer-to-peer software	Data loss risk
Remote access tools (unapproved)	Security risk
Cryptocurrency miners	Resource abuse
Hacking tools	Policy violation
Unauthorized VPNs	Security bypass

Developer Exceptions

Engineering roles have approved exceptions for: - Docker Desktop - Local development servers - Package managers (Homebrew, npm, pip) - IDEs and development tools

---

Network Security

VPN Requirements

Scenario	VPN Required
Public WiFi	Yes
Home network	Recommended
Coffee shops	Yes
Hotels	Yes
Office network	No

DNS Security

- Company DNS servers required when on VPN
- DNS over HTTPS enabled
- Malicious domain blocking active

Monitoring and Alerting

What Is Monitored

Data	Purpose	Retention
Malware detections	Security	2 years
Process execution	Threat hunting	90 days
Network connections	Security analysis	30 days
File modifications	Incident response	30 days
Login attempts	Security	1 year

What Is NOT Monitored

- Personal browsing content
- Personal file contents
- Keystrokes
- Camera/microphone
- Personal email content

Alert Thresholds

Event	Action
Malware detected	Auto-quarantine, IT notified
Suspicious process	Alert to security team
Policy violation	User warning, IT notified
Multiple failures	Account review

Compliance Verification

Automated Checks

Devices are automatically verified for: - CrowdStrike agent status - Disk encryption status - OS patch level - Firewall status - Screen lock configuration

Non-Compliant Devices

Severity	Condition	Action
Critical	No endpoint protection	Network access blocked
High	Encryption disabled	24-hour remediation deadline
Medium	Outdated OS (>30 days)	7-day remediation deadline
Low	Minor policy deviation	User notification

Remediation

1. User receives automated notification
2. Self-service remediation instructions provided
3. IT available for assistance
4. Escalation after deadline

Incident Response

User Responsibilities

If you suspect a security issue:

1. **Disconnect** from network (if active threat)
2. **Report** to security@novatech.com immediately
3. **Do not** attempt to investigate yourself
4. **Preserve** device state (don't restart)
5. **Document** what you observed

IT Security Response

1. Remote isolation of device (if needed)
2. Investigation initiated
3. User contacted for information
4. Device may be collected for forensics
5. Replacement device provided

Updates and Patching

OS Updates

OS	Policy
macOS	Auto-update enabled, 7-day deferral max
Windows	Auto-update enabled, 7-day deferral max
Linux	Weekly update window

Critical Security Updates

- Applied within 72 hours
- May require immediate restart
- User notification provided

CrowdStrike Updates

- Automatic, continuous
- No user intervention required

Exceptions

Approved Exceptions

Some roles may have documented exceptions: - Security researchers (controlled environment) - IT administrators (management tools) - Legal hold devices (preservation)

Requesting an Exception

1. Submit via IT Security Portal
2. Document business need
3. Risk assessment by IT Security
4. VP approval required
5. Time-limited (max 1 year)
6. Annual review

Training Requirements

All employees must complete: - Annual security awareness training - Endpoint security module - Phishing simulation exercises

Completion tracked in Workday Learning.

Enforcement

Compliance

- Endpoint protection is mandatory
- Non-compliance may result in network access revocation
- Repeated violations escalated to management

Violations

Violation	Consequence
Disabling protection	Network access suspended
Tampering with agent	Security investigation
Unapproved software	Removal, warning
Repeated non-compliance	HR involvement

Contact

- **IT Security:** security@novatech.com
- **IT Help Desk:** it-help@novatech.com
- **Emergency:** +1-512-555-4357

Related Documents: Acceptable Use Policy (IT-SEC-001), BYOD Policy (IT-SEC-020), Incident Response (IT-SEC-030)