Mobile Device Policy

Document ID: IT-HW-004 **Last Updated:** 2024-01-30 **Owner:** IT Security
Classification: Internal

Overview

This policy governs the use of mobile devices (smartphones, tablets) for NovaTech business purposes, including company-provided devices and personal devices used for work (BYOD).

Device Options

Company-Provided Devices

Available for roles requiring frequent mobile access: - Sales representatives - Executives - On-call engineers - Field support staff

Available devices: | Device | Storage | Eligibility | |——–|———|————-| | iPhone 15 Pro | 256GB | Standard | | iPhone 15 Pro Max | 256GB | Executive | | Samsung Galaxy S24 | 256GB | Standard (Android preference) | | iPad Pro 12.9” | 256GB | Specific roles only |

Bring Your Own Device (BYOD)

Employees may use personal devices for work with: - Manager approval - Enrollment in Mobile Device Management (MDM) - Compliance with security requirements

BYOD Stipend: $50/month for employees using personal devices for work

---

Mobile Device Management (MDM)

All devices accessing NovaTech data must enroll in MDM (Microsoft Intune).

Requirements

- Automatic enrollment for company devices
- BYOD enrollment during onboarding
- MDM enables:
  - Remote wipe capability
  - Security policy enforcement
  - App distribution
  - Device encryption verification

Privacy (BYOD)

MDM on personal devices: - **Cannot see:** Personal emails, texts, photos, browsing history - **Can see:** Device model, OS version, installed work apps, compliance status - **Can do:** Wipe work data only (not personal data)

Security Requirements

All Devices

- Screen lock required (PIN minimum 6 digits, or biometric)
- Encryption enabled
- Automatic updates enabled
- Lost/stolen reported within 24 hours

Company Devices

- No jailbreaking or rooting
- Only approved apps from managed app store
- Personal use limited and at company discretion

BYOD Devices

- Minimum OS version: iOS 16+ or Android 13+
- Work apps installed in managed container
- Device must pass security health check

Approved Applications

Required Work Apps

App	Purpose
Microsoft Outlook	Email and calendar
Slack	Team communication
Okta Verify	Multi-factor authentication
Microsoft Authenticator	Backup MFA

Optional Work Apps

App	Purpose
Salesforce	Sales teams
Zoom	Video conferencing
Notion	Documentation
GitHub Mobile	Engineering teams

Request Process

Company Device Request

1. Submit request in ServiceNow > "Mobile Device Request"
2. Provide:
   - Business justification
   - Device preference
   - Shipping address
3. Manager approval required
4. Ships within 5 business days

BYOD Enrollment

1. Download Microsoft Intune Company Portal
2. Sign in with NovaTech credentials
3. Follow enrollment prompts
4. Install required work apps

International Travel

Before Travel

- Notify IT Security of travel dates and destinations
- Review country-specific guidelines
- Enable device tracking (Find My iPhone/Android)

High-Risk Countries

Some countries require additional precautions: - Use a travel-only device (available from IT) - VPN required at all times - Minimize sensitive data on device - Report any device inspection by authorities

Contact security@novatech.com before travel to high-risk regions.

Lost or Stolen Devices

Immediate Actions

1. Report to IT Security immediately: security@novatech.com or #security-urgent
2. IT will initiate remote wipe
3. Change your NovaTech password
4. File police report if stolen

Company Devices

- Replacement provided after incident review
- No cost for first incident
- Pattern of loss may require review

BYOD

- Work data remotely wiped
- Personal data unaffected
- Employee responsible for device replacement

Device Return

Company Devices

Return required when: - Leaving NovaTech - Upgrading to new device - Role change removes eligibility

Return process: 1. Back up any personal data (if permitted) 2. IT wipes device 3. Ship to IT or return at office

BYOD Offboarding

- Unenroll from MDM
- Work apps and data automatically removed
- Personal data unaffected

Cost Responsibility

Item	Company Device	BYOD
Device cost	Company	Employee
Monthly service	Company	$50/month stipend
Repairs (normal use)	Company	Employee
Accidental damage	Case-by-case	Employee
International roaming	Pre-approved expenses	Expense reimbursement

---

Compliance

This policy supports: - SOC 2 Type II requirements - GDPR data protection - Industry security standards

Violations may result in device access revocation and disciplinary action.

Related Documents: Security Best Practices (IT-SEC-010), VPN Setup Guide (IT-ACC-003), BYOD Agreement Form (IT-HW-005)