Device Management Policy

Company-Issued Devices

Company provides laptops and mobile devices as needed for your role. Devices remain company property and must be returned upon termination.

Standard laptop refresh cycle is 3 years. Request early replacement if device is failing or inadequate for your work.

Device Setup and Configuration

IT configures devices with required software, security tools, and settings before distribution. Don't remove or disable security software.

Additional software can be requested through IT portal. Keep devices updated with latest OS and security patches.

Mobile Device Management

Company-issued mobile devices are enrolled in MDM (Mobile Device Management). MDM enforces security policies and enables remote wipe if lost.

Personal devices accessing company email must install MDM profile. MDM only manages work data, not personal data.

Device Security Requirements

Enable full disk encryption on all devices. Use strong passwords/PINs. Enable biometric authentication where available.

Lock devices when unattended. Set auto-lock to 5 minutes or less. Never leave devices in vehicles or unsecured locations.

Lost or Stolen Devices

Report lost or stolen devices to IT immediately. IT will remotely lock and wipe device to protect company data.

File police report for stolen devices. Provide report number to IT for insurance purposes.

Personal Use of Company Devices

Limited personal use of company devices is permitted if it doesn't interfere with work or violate policies.

Personal data on company devices is not private and may be accessed during investigations. Don't store sensitive personal data on company devices.

Bring Your Own Device (BYOD)

Personal devices can access company email and approved cloud services with MDM profile installed.

BYOD devices must meet minimum security requirements: current OS, passcode enabled, encryption enabled, security updates current.

Device Maintenance

Keep devices clean and in good condition. Report hardware issues to IT promptly. Don't attempt repairs yourself.

Backup important data regularly. Use approved cloud storage or network drives, not local storage only.

Software Installation

Install only IT-approved software. Request software through IT portal. Unauthorized software may be removed during security scans.

Keep all software updated. Enable automatic updates where possible. Don't disable or postpone critical security updates.

Device Return Process

Upon termination or device replacement, return device to IT within 3 business days. Backup personal data before return.

IT will wipe device and verify all company data is removed. Accessories (charger, case, etc.) must also be returned.

Remote Work Device Requirements

Remote workers receive same device standards as office workers. Ensure adequate workspace for device setup.

Use surge protector for desktop equipment. Maintain proper ventilation to prevent overheating.