Sean Jameson
Vice President & CIO
s.jameson@fdu.edu
973-443-8830

MOBILE COMMUNICATIONS DEVICE POLICY ISSUE 4.0

Date: September 1, 2026

CONTENTS

I. POLICY STATEMENT 2
II. OVERVIEW 2
III. ELIGIBILITY 2
III.A Approvals 2
III.B Device Returns 3
III.C Supervisor Procedures and Responsibilities 3
IV. Employee Responsibilities 3
V. Security Controls 4
VI. Application Management 4
VII. Security and Data Protection Requirements 4
VIII. Supported Platforms 5
IX. Enrollment Requirements 6
X. Records, Privacy, Monitoring, and Legal Process 6
XI. Exceptions 6

I. POLICY STATEMENT

Fairleigh Dickinson University (FDU) provides approved, eligible employees with university-owned mobile communications devices. The primary purpose of a university-owned device is to support official University business; reasonable incidental personal use is permitted when it does not create additional cost, interfere with duties, violates law or University policy, or compromise security.

This policy establishes financial, administrative, security, privacy, safety, and lifecycle requirements for mobile devices used to access, process, store, or transmit FDU information or connect to FDU systems.

II. OVERVIEW

Effective September 1, 2026, Fairleigh Dickinson University (FDU) has adopted a revised mobile communications device policy. The primary purpose for having a Fairleigh Dickinson University owned smartphone, tablet, or MiFi is for official University business.

The University provides data only devices (MiFi) as needed to eligible employees for business purposes.

FDU may, in some cases, purchase and own mobile communication devices to be assigned to groups (departments, offices, laboratories, etc.) and which may be loaned temporarily to individual employees or be shared by groups of employees for specific business purposes only. This may be done only if usage is exclusively for essential University business. The University will conduct periodic audits to confirm that usage is exclusively for business.

Additionally, mobile communication devices that are required to conduct research projects and charged to sponsored program budgets must be obtained through a SAMI Support Ticket.

Mobile communication devices should not be selected as an alternative to other means of communication when such alternatives (such as WIFI) provide adequate but less costly service to the University.

III. ELIGIBILITY

The issuance of a university phone is limited. The following employees may be eligible for a university issued smartphone tablet, or MiFi device, or reimbursement for business expenses incurred on employee-owned mobile communications devices:

- Employees with duties requiring immediate accessibility.
- Employees who are required to spend significant time outside their normal work area.
- Employees who have duties beyond normal business hours.

III.A Approvals

Approval for the issuance of a university communications device will be at the Vice President, Senior Associate Vice President or Officer level and each mobile communications device will be approved by the person responsible for the budget from which the charges will be paid.

USAN Voice Services will work with the user to select the mobile communications device and attachments unless the budget manager requests something special.

Eligible equipment will be provided upon completion of a Mobile Device Request Form.

III.B Device Returns

Mobile Communications Device equipment supplied by the University remains the property of the University and must be returned upon termination of employment or when requested. If an employee fails to do so, the employee will be charged for replacement equipment and all monthly charges incurred after they leave.

III.C Supervisor Procedures and Responsibilities

Supervisors will work with eligible employees to determine the mobile communications device option that best meets the needs of the University and the employee. Eligible employees and supervisors will complete the Mobile Device Request Form to request the device.

Thereafter, supervisors are responsible for ensuring that mobile communications device use is commensurate with established policy and are required to reevaluate periodically (at least annually) the continuing need for the mobile communications devices assigned to their subordinates.

In the event an employee is terminated or is otherwise ineligible for the device, the supervisor must complete the Mobile Device Request Form within three (3) business days.

IV. Employee Responsibilities

When utilizing mobile communication devices for University business or personal use, employees have the following responsibilities:

Employees are responsible for the safekeeping, care, and use of smartphones and attachments assigned to them.

Replacing lost or damaged equipment due to negligence may be at the employee's expense.

Employees utilizing smartphones, or similar devices that store electronic files, data, email messages or other potentially sensitive University data are required to notify USAN Voice Services using the Mobile Device Request Form within 24 hours of the loss or theft of their device. If theft is suspected, employees must file a police report and cooperate with law enforcement to ensure FDU's interest in preserving confidential information is respected.

Individuals to whom smartphones have been provided are responsible for the security and maintenance of the phones and must promptly report any damage, theft, or vandalism by opening a SAMI Support ticket.

When traveling internationally, it is the employee's responsibility to open a SAMI Support Ticket to ensure the international feature is added to their mobile device to reduce the risk of incurring very costly data usage.

V. Security Controls

Authentication/Device Access

- All devices must be secured with a passcode complying with minimum complexity requirements.
- The passcode should be a minimum of 6 digits, but an alphanumeric password is preferred.
- Biometric authentication (facial scanning or fingerprint) should be enabled when available.
- The screen lock timeout should not exceed 5 minutes.
- Devices will wipe after 10 incorrect password attempts

Encryption

- Encryption will be enforced at device enrollment
- Removable storage devices will be encrypted. No FDU data should be stored on storage devices that do not support encryption.

OS Integrity

- Any devices determined to be rooted, jailbroken, or running a modified or third-party OS should be immediately disabled.
- Approved OS updates must be installed in a timely fashion.
- We maintain standards for supported OS versions and may require an upgrade if a device falls outside those standards.

VI. Application Management

Approved Applications

- FDU provided applications will be deployed through a managed app store (VPP/ASM or managed Google Play).
- Apps must be installed from an approved app store.
- Installation from untrusted/third-party app stores is prohibited
- Apps may be restricted and blocked from use

App Security

- Prevent data backup to personal cloud locations
- Restrict copy/paste between managed and unmanaged apps
- Encrypted application data at the OS level

App Updates

- Managed apps will be updated automatically
- Automatic updates will be enforced for apps installed by the end user

VII. Security and Data Protection Requirements

FDU currently manages certain University-issued mobile devices through approved device management services. Additional University-issued mobile devices will be enrolled in and managed through approved services as FDU expands its device-management program.

Any mobile device accessing FDU resources must comply with the following minimum requirements. University Systems and Networking or the Chief Information Security Officer (CISO) may impose stronger controls based on data sensitivity, role, threat conditions, or legal and contractual obligations.

- Run an operating system and configuration currently supported by the carrier and FDU. Enable automatic operating system and application security updates.
- Use a passcode, password, biometric control, or equivalent screen lock that meets FDU standards; configure automatic locking after a reasonable period of inactivity.
- Use device encryption and secure boot when supported. Do not disable security, management, logging, encryption, or endpoint-protection controls.
- Use FDU-approved multifactor authentication and approved applications for FDU email, files, collaboration, and other University services.
- Enroll an FDU-owned device in FDU-approved device or application management.
- Do not root, jailbreak, sideload untrusted applications, use unsupported application stores, or otherwise circumvent vendor or FDU security controls.
- Store the minimum necessary University information on the device and use approved FDU storage and sharing services. Protected University information may not be stored in personal cloud storage, personal email, consumer messaging, unapproved notetaking or AI services, or removable media.
- Do not share an assigned device, authentication factor, passcode, FDU account, or managed work profile with another person. Do not approve an unexpected MFA request.
- Use caution on public or untrusted networks. Use FDU-approved secure access methods when required and disable unnecessary wireless interfaces and automatic connections.
- Do not connect a device known or suspected to be compromised to FDU systems. Cooperate with required security updates, quarantine, investigation, preservation, and remediation.

VIII. Supported Platforms

Apple iOS/iPadOS/visionOS/watchOS

- Two previously supported releases which are actively updated
- OS must not be jailbroken or modified.
- Beta releases restricted except in cases of internal testing

Android

- OSes must be installed and supported by the hardware vendor. Third-party OSes are not supported unless approved by OIRT.
- Releases must be actively supported and updated
- Must be supported by Android Enterprise
- OS must not be rooted or modified
- Beta releases restricted except in cases of internal testing

All FDU owned devices must

- Be purchased through FDU approved vendors
- Support Automated Device Enrollment (ADE) or Zero Touch enrollment workflows

IX. Enrollment Requirements

All FDU owned devices must:

- Be enrolled in an FDU MDM solution during activation
- Be enrolled with Supervision (iOS/iPadOS) or Fully Managed (Android)
- Activation or enterprise lock will be enabled at enrollment/activation

X. Records, Privacy, Monitoring, and Legal Process

University business records created, received, or stored through a mobile device remain subject to applicable retention schedules, legal holds, discovery, audit, public-disclosure obligations, and University policy. Users must conduct University business in approved systems, so records can be retained and produced when required and must not delete or move information to avoid retention or review.

FDU may collect and review information about devices, accounts, applications, networks, location, inventory, security, and usage to administer services, protect University interests, investigate incidents or misconduct, and comply with law. Collection should be limited to legitimate University purposes and handled under applicable policy. Users should have no expectation of privacy in FDU-owned devices or FDU-managed accounts and data.

XI. Exceptions

Exceptions must be documented, time-limited, supported by business justification and compensating controls, and approved by the budget officer responsible and the appropriate policy owner. Security exceptions require written approval from the CISO or designee. An exception may be revoked when risk, law, technology, or business conditions change.