NOVA SOUTHEASTERN UNIVERSITY NSU Florida		
POLICY TITLE: University Owned Cellular-Enabled Device Policy		
POLICY OWNER: Chief Information Security Officer		
POLICY CLASS - IDENTIFIER: Operational - MP		**POLICY CODE NO:** INFOSEC03
EFFECTIVE DATE: 5/7/2019	**LAST REVIEW:** N/A	**REVIEW PERIOD:** 3 years

Policy Statement

Nova Southeastern University (NSU) may, at its discretion and in accordance with this policy, provide employees or contractors with *Cellular-Enabled Mobile Devices*[1], at NSU's expense, for the primary purpose of conducting NSU business. All Cellular-Enabled Mobile Devices that are paid for by NSU are the property of NSU and the employee is responsible for ensuring the *Acceptable Use*[2] and security of the device and the *University Data*[3] present on the device as outlined in this policy.

The policy establishes the eligibility for positions which may receive an NSU-owned Cellular-Enabled Mobile Device and sets procedures for monitoring and controlling costs related to the use of Cellular-Enabled Mobile Devices. This policy outlines the Cellular-Enabled Mobile Devices supported by Office of Innovation and Information Technology (OIIT), guidelines for acceptable use, and other administrative topics relating to Cellular-Enabled Mobile Device acquisitions.

This document outlines the university's policy for purchasing, deploying, and supporting Cellular-Enabled Mobile Devices. Cellular-Enabled Mobile Devices are provided to employees where it has been determined that they are required primarily to meet the business requirements of the university.

Business requirements should have a clear connection to the User's job responsibilities which include, but are not limited to:

1. Positions which provide on-call or afterhours business operations support;
2. Positions which must be available to conduct NSU business when away from the office (frequent business-related travel, field and mobile campus staff);
3. Positions which require frequent international communication;
4. Positions which must be available on university business while in other time zones outside the position's normal work day;
5. Positions which have a need to enable communication in areas or situations where conventional telephones or network access is not available or accessible;
6. Positions which need to support periodic emergencies, such as hurricanes or other serious emergency events where staff who are needed during these events would be placed on call.

[1] *A Cellular-Enabled Mobile Device is a portable non-wired computing device such as a smartphone or tablet with cellular connectivity.*

[2] *NSU's Acceptable Use Policy is applicable to all University-provided Cellular-Enabled Mobile Devices.*

[3] *University Data is any personally identifiable information, including, but not limited to, personal identifiers such as name, address, phone number, date of birth, Social Security number, and student personal identification number; personally identifiable information contained in student education records as that term is defined in the Family Educational Rights and Privacy Act, 20 USC 1232g and its implementing regulations (collectively, "FERPA"); protected health information as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103 and its implementing regulations (collectively, "HIPAA"); nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809 and its implementing regulations (collectively, "GLBA"); Controlled Unclassified Information (CUI) as this term is defined in the NIST Special Publication 800-171; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards ("PCI-DSS"); any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person as those terms are defined in the General Data Protection Regulation (GDPR), personal information as that term is defined in the Florida Information Protection Act of 2014 ("FIPA"); driver's license numbers; state or federal identification numbers such as passport, visa or state identity card numbers; and any other personal-related information as to any of NSU's students, parents and guardians of students, sponsors of students, employees, alumni, donors, potential donors, or any NSU-related person or person who is involved in any NSU activity.*

NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

POLICY TITLE: University Owned Cellular-Enabled Device Policy		
POLICY OWNER: Chief Information Security Officer		
POLICY CLASS - IDENTIFIER: Operational - MP		**POLICY CODE NO:** INFOSEC03
EFFECTIVE DATE: 5/7/2019	**LAST REVIEW:** N/A	**REVIEW PERIOD:** 3 years

Management Intent

This policy shall:

- Support employees' critical job duties relating to mobile communications.
- Improve lifecycle management of Cellular-Enabled Mobile Device acquisitions and expenses.
- Enhance data security of these devices and services.

Policy Scope

This policy applies to employees, contractors, and other workers at NSU in the United States and Puerto Rico, including all personnel affiliated with third parties that maintain Cellular-Enabled Mobile Devices on behalf of NSU, hereafter referred to as *Users* or *Responsible Parties*.

Device Security Requirements

An authentication mechanism to verify the identity of the User and to maintain e-mail access is required on all mobile devices issued by the university. The Responsible Parties may not tamper with or circumvent these administrative settings. Storage of unencrypted University Data on Cellular-Enabled Mobile Devices is prohibited. For questions concerning the encryption of University Data on Cellular-Enabled Mobile Devices, please contact NSUMobile@nova.edu.

NSU's Right to Audit and Protect

NSU has the right to, at will:

- Audit University Data residing on university-owned Cellular-Enabled Mobile Devices
- Modify, including remote wipe or reset to factory default, the registered Cellular-Enabled Mobile Device's configuration remotely.

Device Reset and Data Deletion

Device User understands and accepts the device will be remotely wiped under the following circumstances:

- Device is lost, stolen, or believed to be compromised.
- Device is found to be non-compliant with this policy or other NSU policy.
- Device was issued to a User that no longer has a working relationship with NSU.
- Other reasons that may compromise the confidentiality, integrity or availability of University Data.

Device Support

OIIT administers all contracts with providers of mobile equipment and service. OIIT also provides consultation about equipment, accessories, and monthly service plans.

OIIT provides full technical support for university issued Cellular-Enabled Mobile Devices only. No support is implied or will be provided for any other Cellular-Enabled mobile devices or third-party applications.

- NSU will provide basic hardware/software support including installation, configuration, and diagnostic troubleshooting.
- NSU will coordinate warranty repair services with the vendors. Apple devices must be taken to an Apple store for warranty hardware malfunctions (water/physical damage does not apply).
- NSU will provide diagnostic troubleshooting for connection to the university wireless network.

User Responsibilities

Users will be responsible for:

- The backup of any data they need to retain.
- Securing the device and the data it contains by using a PIN or other password protection and enabling automatic lockout (mandatory).
- Installing any needed software updates.
- Reporting lost or stolen devices within three (3) calendar days to NSUMobile@nova.edu and to their colleges/department's telecom contact and the Public Safety Department at 954-262-8999.
- Securing the device in a protective cover or case.
- Using the device consistent with the manufacturer's specifications (no jail-broken devices).
- Department Heads are responsible for overseeing the use of mobile devices in their unit and reviewing mobile device needs at least quarterly to ensure the university is using devices effectively.
- Usage reports for unused devices will be sent to the college/department telecommunications contact monthly. After three months of no usage, the line will be automatically cancelled unless specifically pre-authorized.
- Should the university incur incremental costs as a result of personal use of mobile devices, Users are responsible for reimbursing the costs. Users are responsible for securing the mobile devices in their custody and for promptly arranging for the return of the mobile devices via email to OIIT at NSUMobile@nova.edu when its use is no longer necessary or upon separation from NSU.

Equipment Orders

All requests for new devices must be approved by the college/department Business Officer and the Dean or VP funding the request and submitted by the college/department's telecommunications contact. OIIT is the only organizational unit authorized to purchase Cellular-Enabled Mobile Devices. The university does not reimburse individuals for the purchase of mobile equipment.

- Equipment purchases and monthly recurring costs will be charged to the User's cost center. Devices that are assigned to departmental employees as needed (e.g., several shift employees) may be issued under the employee title to the Department head.
- The Director of Sponsored Programs is responsible for approving charges to federally sponsored projects for costs associated with mobile equipment.
- Each department is responsible for notifying OIIT of staff changes and cancellations of service. Until a request to cancel service is submitted via service manager by the telecom representative, each department will continue to be responsible for the cost of service for each line.

- Please return devices which will no longer be used to OIIT for proper handling. Devices must be factory reset before being returned.
- Monthly costs for devices continue until the plan is paid in full. At the department's discretion, employees may purchase their university phone upon leaving their position. The employee will need to provide written supervisor approval authorizing the request and be responsible for any associated costs for the phone equipment. All university-owned phones will be wiped of all University Data upon purchase by employees leaving their position.

Device Purchase Guidelines

- T-Mobile is the authorized cellular carrier for Nova Southeastern University. Device pricing and offers may be obtained by contacting NSUMobile@nova.edu.
- Users are authorized to spend up to $700 on a cellular phone.
- Phone replacements are authorized no less than every 36 months.
- Exceptions will be considered by the executive office for the following reasons:
  - Position level - Deans and Vice Presidents are authorized to spend up to $1200.
  - Positions which require specialized devices.
  - Locations which do not have adequate T-Mobile coverage.
  - Users who damage or lose their device.

International Calling/Travel

For detailed procedural information on Cellular-Enabled Mobile Devices, please consult the Cellular-Enabled Mobile Devices Service Level Objectives (SLO) located on the NSU Telecommunications website: https://www.nova.edu/telecom/wireless-services/employees/cell-policy.html

- All university Cellular-Enabled Mobile Devices will be blocked for international usage except for those Users who have been approved to have international coverage by their department/college Center Head.
- Authorized international travel/calling will be paid by the User's department and must be approved by the college/department's Business Officer and submitted to the college/department's telecom contact within one week of travel.

International Loaner Program

For those Users who have not been assigned a university Cellular-Enabled Mobile Device, OIIT provides three international devices from AT&T. These phones will be made available to all departments. The traveler will need to contact his/her department's telecommunications contact to reserve a phone. These devices are supplied on a first come first serve basis. The telecommunications contact will need to place the request into service manager at least two weeks in advance.

The international plan is $10.00/day plus the cost for the initial service plan ($52.06). The initial plan and all usage charges will be the responsibility of the department requesting the loaner. If the device is lost or stolen, the department will be responsible for the charge to replace the phone. The device must be returned to OIIT unlocked and reset within one week of the User's return.

Please note that this program has been designed for Users who travel infrequently or for those who do not have a university-owned Cellular-Enabled Mobile Device. If the User travels internationally on a regular basis, OIIT recommends that the department purchase a cell phone for the employee.

Supported Devices / Synchronization Mail Clients

- Supported Devices: Apple iOS and Samsung
- Supported E-mail client: MS Outlook
- Supported Calendar and contacts: MS Outlook
- No other mail clients will be supported. Users will only be able to access their NSU email through the MS Outlook mail client.

Non-Compliance

Violations of NSUs policies regarding Cellular-Enabled Mobile Devices, including but not limited to, tampering with or attempting to circumvent any of the university controls, may subject the Responsible Parties to potential disciplinary action, up to and including termination in accordance with the Office of Human Resources Employee Policies. Documentation regarding any sanction imposed for violation of the Cellular-Enabled Mobile Device Policy shall be retained in the sanctioned employee's personnel file.

References/Source Documents

1. *NIST Special Publication 800-53 Revision 4: Media Protection Family*
2. *NSU Cellular-Enabled Mobile Devices Service Level Objectives (SLO) located on the NSU Telecommunications website: https://www.nova.edu/telecom/wireless-services/employees/cell-policy.html*
3. *NSU Acceptable Use Policy (https://www.nova.edu/portal/oiit/policies/forms/information-security-acceptable-use-policy.pdf)*

NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

POLICY TITLE: University Owned Cellular-Enabled Device Policy

POLICY OWNER: Chief Information Security Officer

POLICY CLASS - IDENTIFIER: Operational - MP | **POLICY CODE NO:** INFOSEC03

EFFECTIVE DATE: 5/7/2019 | **LAST REVIEW:** N/A | **REVIEW PERIOD:** 3 years

Approvals

George L. Hanbury, II
President & Chief Executive Officer

____

Date: ______________________________

Harry Moon
Executive Vice President and Chief Operating Officer

DocuSigned by:
Harry K. Moon, M.D.
40CB54E3AD924CE...

Date: 5/15/2019 | 4:58 PM EDT

Tom West
VP and Chief Information Officer
APPROVED AS TO BUSINESS CONTENT

____

Date: 05/09/2019

Charles Rodholm
Chief Information Security Officer
APPROVED AS TO SECURITY CONTENT

____

Date: 5/8/19

Thomas Panza
Panza, Maurer & Maynard, P.A.
APPROVED AS TO LEGAL FORM

____

Date: 05/07/19