Northeastern University

Procedure Supporting the Policy on Mobile Devices

Revised October 1, 2019

Subject Area: **Eligibility, Security, and Disposal of Surplus Devices**
Policy Title: **Policy on Mobile Devices**
Responsible Office: **Office of the SVP for Finance**

Purpose

Policy-enabling procedures that may change from time to time, and as such, are at a level of detail that are not well-suited for inclusion in the policy documentation. This document has been incorporated into the policy by reference, and carries equal weight to the policy document itself.

Personal Mobile Device Requirements

ITS will evaluate mobile devices before authorizing them to connect to NU computing resources. This step ensures that a device has capabilities to enable a basic level of security to protect our network and the information that is accessible on it. It is important that the Eligible Employee use this information when selecting a personally-owned device if it is intended to be used with NU computing resources. The process to do so is as follows:

- Prior to requesting exception approval, the Eligible Employee must demonstrate that a Personal Mobile Device meets the same standards used to evaluate University-owned devices. Steps:
    - Please access the Mobile Devices category on NEU's Procurement Services site https://northeastern.sharepoint.com/sites/finance/Preferred%20Suppliers/Commodities/Mobile%20Devices.aspx. For new devices, check the carrier's website to see that your preferred device is offered. This will indicate whether a device has been pre-qualified for use on the NEU network. Please print the website page with the device listed to certify compliance with this requirement.
    - In situations where a personal mobile device is already in use on another plan, direct communication with the authorized carrier of service is necessary. The Procurement Services site a point of contact for each University-authorized service provider. An email from the service provider is sufficient demonstration that the device meets the University's standards.

Security Requirements

The following security requirements apply to ***all*** mobile devices (Personal Mobile Devices as well as University-owned) that access University data (including webmail and web calendars). Such devices must be:

- Configured to require a PIN number or password with a minimum of 4 unique characters to operate after starting up or after locking;
- Configured to automatically lock after not more than 15 minutes of inactivity;

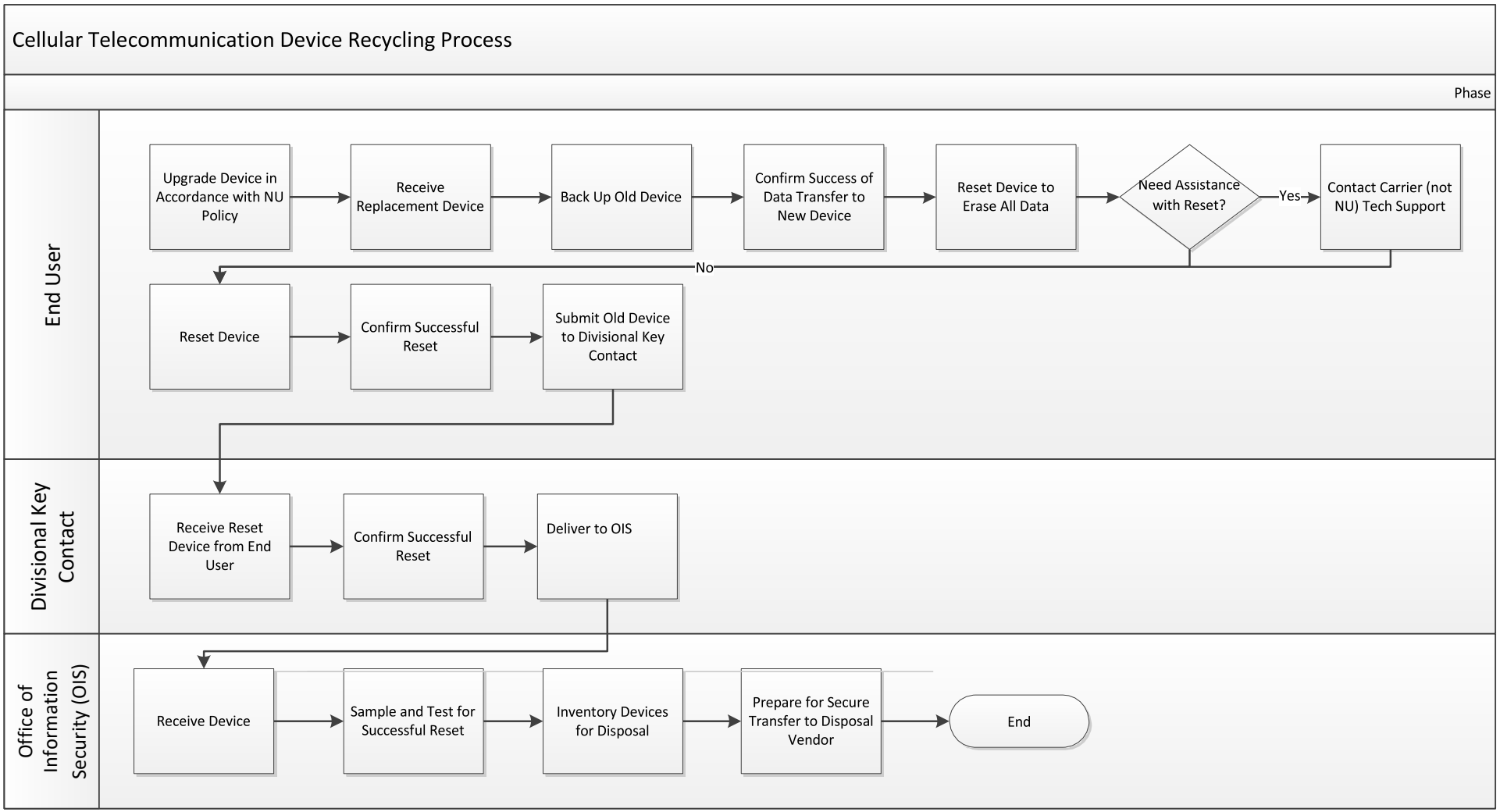
- Configured to automatically wipe their data after not more than 10 incorrect password/PIN entries, and
- Have remote wipe capability enabled, and
- Have encryption enabled, where technically feasible

By using ***any*** mobile device to access confidential University data or the University network, an employee is in agreement with and promises to maintain at all times required security measures on personally owned or University owned devices. In addition, the employee gives the University permission to wipe and locate that device in the event of loss or theft of any device covered under the Cellular Telephone and Mobile Device Policy.

Upon the loss or theft of a University-owned device or a personal mobile device used to access confidential University data, the employee shall notify ITS immediately and provide any necessary login information to access the device's remote wipe and "find my device" capabilities. The University accepts no liability for personal data lost, whether the data was on an NU -owned device or a personal device. Several options are available to preserve personal information on University devices at little to no cost to the employee. The University will not bear the cost for employees to back up personal data on personal or University-owned devices.

Device Recycling Procedure

Please reference the process flow on the following page.


Cellular Telecommunication Device Recycling Process
Phase
End User
Upgrade Device in Accordance with NU Policy
Receive Replacement Device
Back Up Old Device
Confirm Success of Data Transfer to New Device
Reset Device to Erase All Data
Need Assistance with Reset?
Yes
Contact Carrier (not NU) Tech Support
No
Reset Device
Confirm Successful Reset
Submit Old Device to Divisional Key Contact
Divisional Key Contact
Receive Reset Device from End User
Confirm Successful Reset
Deliver to OIS
Office of Information Security (OIS)
Receive Device
Sample and Test for Successful Reset
Inventory Devices for Disposal
Prepare for Secure Transfer to Disposal Vendor
End