NEOMED OPERATIONAL POLICY	Policy No: 3349-OP-360
OPERATIONAL POLICY TITLE: Mobile Computing Device Policy	EFFECTIVE DATE: July 1, 2010
RESPONSIBLE DEPARTMENTS: Information Technology	Approval Authority: Responsible Office:

(A) PURPOSE

Mobile computers allow NEOUCOM faculty and staff to have computing resources at hand in meetings/classes, enable those who travel on University business to be maximally functional and productive while away, and equip those who occasionally work at home to eliminate duplication of resources, files, etc. Along with the privilege of using University owned mobile computers, comes additional responsibility to safeguard them from potential theft or damage. If a mobile device is stolen or lost, there are additional security implications for any data that might have been stored on that device as well. This Policy addresses actions that must be taken in order to minimize the risk of the theft of University-owned mobile devices and the associated costs to the University Community. The purpose of this Policy is to govern the use and liability of University-owned mobile computing equipment. This Policy should be read and thoroughly understood prior to acquiring and using mobile computing equipment.

(B) SCOPE

All University-owned mobile computers are governed by this Policy including systems made available as primary workstations, checked out through the IT department, assigned within a departmental office, or purchased through grant dollars for specific projects.

This Policy is applicable to all current University staff, faculty, or administrators, and students who are using mobile computing devices provided or loaned to them by a University department. University-owned mobile computing devices are for University use only and may not be used for personal projects or entertainment.

(C) DEFINITIONS

(1) “Mobile Computing Devices” are portable-computing devices that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to an agency's IT infrastructure and/or data systems.

Specific examples of mobile computing devices may include but not limited to: laptop and tablet computers, PDA (personal digital assistant), and wireless phones.

(D) LIABILITY

(1) NEOUCOM departments are responsible for the security and safety of their assigned mobile device and will be fully liable if stolen, lost, destroyed or not returned.

(2) NEOUCOM departments will be required to reimburse the Office of Information Technology for the full replacement cost of the mobile device if it is stolen, lost, destroyed or not returned. The replacement cost will be determined by the Information Technology Department at the time of the loss.

(3) NEOUCOM departments are responsible for full repair or replacement cost if a mobile device is damaged or made inoperable by misuse or neglect.

(4) Departments providing departmental devices to students or student organizations for use will be liable for the replacement cost of the unit should it become stolen, lost, or damaged while in the students possession, or is or not returned.

(5) The department will have full discretion on cost recovery of the asset from the end user in possession of the mobile device.

(6) If an end user is required to reimburse the Department for one of the loss events outlined in the Policy, the end user understands that the replacement cost and/or replacement device become the property of NEOUCOM.

(7) If a separation event occurs from NEOUCOM; layoff, retirement, termination, or resignation of employment occurs, the person reimbursing for a loss event is not entitled to receive any financial or equipment consideration upon separation.

(E) USER RESPONSIBILITIES

(1) Physical Protection and Reasonable Care

(a) Each user of a University-owned mobile device is responsible for the security of that device, regardless of whether the device is used in the office, at one's place of residence, or in any other location such as a hotel, conference room, car or airport. Users are expected to provide reasonable care and effort to protect the mobile device.

(b) Carrying cases and devices should be labeled accordingly so in the event of a loss the equipment might be returned.

(c) Special care should be taken with the security of the mobile device. Equipment must not be left unattended in public areas. Do not leave your office unlocked, even for a brief time, if your mobile device is not secured in the office.

(d) Do no store mobile devices in a locked car or car trunk, as severe temperatures may damage it and the car may be broken into if the device can be seen.

(2) Security Data

(a) Do not download, store or record data that includes any personally identifiable information such as: student/faculty/staff/alumni/vendor Name, Address, SSN, account number, credit card number, etc. which if lost or stolen could be used-for-Identity-theft.

(b) The user is responsible for the security of all NEOUCOM data stored on, or carried with, the device. The user is responsible to make sure that virus protection updates, operating system updates and virus scans are performed regularly.

(c) Do not alter any system software or hardware configuration unless instructed to do so by someone from the Information Technology Department.

(d) Additional application software should not be loaded onto a mobile device unless approved by the Information Technology Department.

(e) Safeguard the device and data by ensuring the mobile device is "locked" or the user is logged off when not in use.

(3) Inventory Tracking

(a) If a separation event occurs from NEOUCOM; layoff, retirement, termination, or resignation of employment occurs, the device, all peripherals, and carrying case need to be returned to the Helpdesk in the IT department on the last day of work.

(F) ENFORECEMENT

Failure to follow this Policy and these procedures may result in loss of computer privileges and/or other disciplinary actions.

Unless the special permission of a senior executive is obtained, all workers who have stolen University property, acted with insubordination, or been convicted of a felony must be terminated immediately. Such instant terminations must involve both escort of the individual off the premises and assistance in collecting and removing the individual's personal effects.

NEOMED OPERATIONAL POLICY	Policy No: 3349-OP-360
OPERATIONAL POLICY TITLE: Mobile Computing Device Policy	EFFECTIVE DATE: July 1, 2010
RESPONSIBLE DEPARTMENTS: Information Technology	Approval Authority: Responsible Office:

REFERENCES

FORMS

CROSS-REFERENCE

REVISION HISTORY

RULE PROMULGATED UNDER

LEGAL