Portable Device Policy

Objective

The purpose of the Suffolk University Portable Device Policy is to safeguard University Portable Devices and University Information on Portable Devices, including but not limited to laptops, flash drives, personal digital assistants (PDA), or hand held computers, which may be susceptible to theft or loss.

Applicability

The Portable Device Policy applies to any faculty or staff members, whether full-time or part- time, paid or unpaid, temporary or permanent, as well as all agents and representatives of the University, including any third party service provider providing services to the University who create, use or otherwise access or interact with any University Information or University Information Resource.

Definitions

Confidential Information: This information consists of University Information which falls into one of the following categories:

a. Massachusetts Personal Information (as defined herein)

b. Financial Customer Information (as defined herein)

c. Records and information the University, or any of its employees or units, is required by law to keep confidential, including but not limited to the following:
   i. Personally identifiable information about students of the University, other than “directory information,” contained in “Education Records,” i.e. records “directly related to a student”, to the extent protected by the federal law known as the Family Educational Rights and Privacy Act or “FERPA”
   ii. Records pertaining to individuals receiving health care related services from any Massachusetts licensed clinic operated by the University, to the extent they are considered confidential under Massachusetts law.
   iii. Information considered privileged under Massachusetts law, including but not limited to information consisting of or relating to communications between an individual and an employee of the University acting in their professional capacity as a licensed psychotherapist, psychologist, mental health counselor, or sexual assault counselors.

d. Information the University is required by contract, or by University policy, to keep confidential

e. Other highly sensitive personal information about an individual the disclosure of which could foreseeably result in identity theft, financial fraud, damage to reputation, or acute embarrassment, or other significant harm to the individual. Examples of such information include: information about a person’s medical condition or physical or mental health; or personnel or employee payroll records.

f. Other University Information that is proprietary to the University and that the University has a strong financial, strategic, or competitive interest in keeping confidential, or that the University is expected to keep confidential under applicable ethical norms. Examples of such information include: trade secret information, proprietary information relating to inventions or patents, research data, or personal information about volunteer research subjects collected in the course of human subject research.

Portable Devices: Any device that is easily carried or moved and capable of storing, sending and/or receiving data. These include, but are not limited to, laptops, PDAs, USB drives and cell phones.

Remote Wipe: The deletion of the contents of a Portable Device through a remote command or action by a University IT system administrator.

University Information: any information in any form whether electronic, hardcopy, audial, or otherwise which is created, collected, stored, accessed or used in connection with the operation and/or management of the University, or which is created, collected, stored, accessed or used by a party authorized by the University.

University Information Resource: any tool, device, equipment, or system used to create, collect, record, process, store, retrieve, display and transmit University Information, including but not limited to email, mainframes, servers, computers, laptops, personal digital assistants (PDA), telecommunication resources, fax machines, printers, file cabinets, software and embedded technology.

Policy

Portable Devices present unique security concerns because they are easily carried or moved and susceptible to theft, electronic invasion or unintentional exposure of data. Any use, access or storage of University Information on any Portable Devices, whether provided by the University or not, must be protected and monitored as follows to ensure appropriate security, availability and integrity:

- Portable Devices must be physically locked or otherwise appropriately secured by its user/custodian when left unattended
- University Information stored on Portable Devices should be backed up to University servers to avoid losing or compromising information
- University issued laptops and PDAs must be capable of RemoteWiping
- University issued laptops and PDAs must be configured to timeout after a period of inactivity in accordance with the Password Policy
- All University issued laptops that access Confidential Information are required to be encrypted using University encryption software in accordance with the Encryption Policy
- Confidential Information must not be stored on unencrypted removable media (such as CDs, flash drives, USB drives, external hard disks, etc.)

Contact the Information Security Officer infosecurity@suffolk.edu for questions relating to this policy and for assistance with enabling appropriate security measures for laptops and other portable devices.

Reporting Loss or Theft of a Portable Device
In the event that any University issued Portable Device is lost or stolen, the University User shall report the incident immediately to the Information Security Officer and the University Police Department.

Violation of Policy

The University reserves the right to monitor network traffic, perform random audits, and to take other steps to insure the integrity of its information and compliance with this Policy. Violations of this Policy may lead to appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks. Willful or repeated violations of this Policy may result in dismissal from the University.

Revision History

Version	**Date**	**Responsible University Office**	**Approved By**
1.0	09/14/10	Provost Office	Provost Barry Brown