****

|  |  |
| --- | --- |
| Section: | IT |
| Title: | Mobile Device Standard |
| Effective Date: | 10/1/2013 |
| Approved By: | Information Technology |
| Responsible Unit: | Information Technology |
| History: |  |
| Related Documents: |

1. **INTRODUCTION**

This document describes the security requirements for mobile devices including tablets, mobile phones and laptops.

1. **DEFINITIONS**

Mobile device – a mobile phone or laptop

1. **STANDARD**

All mobile device users should employ the security mechanisms provided by their device to prevent unauthorized users from accessing content or using the device. This typically will include the use of pin codes that are required every time the device is powered on or on a periodic basis (i.e. every 4 hours), remote wipe capability where an authorized person can remotely trigger the device to erase the user supplied content, encryption requiring credentials to access data, and remote location service so the device can be located if its misplaced**.** Laptop users should use a password to access the operating system.

Mobile devices are particularly susceptible to theft. Users should be aware of the location of their mobile devices at all times and lock the device in the trunk of the car, use the safe in a hotel room, use a cable lock kit when the device will be left unattended, etc.

Sensitive data should not be stored on mobile devices. Any reports, spreadsheets, databases or Word documents which include student data, human resources data or financial data should be stored on network drives and accessed through the VPN.

1. **RELATED DOCUMENTS- None**
2. **HISTORY - None**