Mobile Device Guidelines

Hofstra University values the security of confidential information maintained on its computer systems. Mobile devices, such as cell phones and computer tablets, are powerful computers capable of storing sensitive data and are often used as an extension of a workplace computer. Using a mobile device, which can be easily lost or stolen, to access University data, including email, increases the risk of unauthorized access to and disclosure of this information. Various New York State and federal laws require the University to protect sensitive information and to notify individuals in certain circumstances where there is a security breach relating to personal information.

Definitions

Mobile Devices ("Devices") - Small devices easily carried and transported by a single person, which have the capability of storing, processing, and/or transmitting data. This includes but is not limited to laptops, notebooks, tablets, smartphones, personal data assistants (PDAs), flash drives, USB drives, zip drives, and external hard drives.

Sensitive Information – All information protected by all applicable laws, including, but not limited to, the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA), as well as information that is considered confidential to the University's operations.

Scope

These guidelines describe the minimum security requirements for all Devices used to access University data, regardless of whether the Device is University-issued or personally owned. Specific types of Sensitive Information, such as medical information, may be subject to more stringent requirements than those listed here.

GUIDELINES

Users of Devices are expected to take all reasonable and appropriate measures to protect the Device and Sensitive Information from unauthorized access, such as securing the Device at all times and enabling available security features. All use of Devices on the Hofstra network must conform to the provisions outlined in the Hofstra University *Acceptable Use Guidelines* found on the Hofstra portal (http://www.hofstra.edu/pdf/StudentAffairs/StudentServices/IT/itscs/ACCEPTABLE_USE_GUIDELINES.pdf).

Users are expected to:

1. Have password protection set on the Device. The password must be at least 4 characters in length and have a strong value that is not a common name or easily guessed (e.g.1234). The password should be regularly changed to protect the Device.

2. For Devices with screens, configure the Device to lock when idle, requiring the user to enter his or her password to unlock the Device. Users are encouraged to use the minimum

screen lock time setting available for the Device. Devices should lock after no more than 5 minutes of inactivity. See links below for instructions on how to enable this for your device. If you don't see your device's Operating System listed, please contact the Help Desk.

Instructions on how to set a screen lock for your Device:
For Apple, iOS: http://support.apple.com/kb/HT4175
For Android:
- Nexus Devices: https://support.google.com/nexus/answer/2819522?hl=en&ref_topic=3416293
- Other Devices: https://support.google.com/android/answer/3094742 (provides links to other manufacturer websites)

3. Properly secure University data, including Sensitive Information, stored on the Device. Due to increased security concerns, storing Sensitive Information on a Device is strongly discouraged; employees working remotely should store Sensitive Information on the University's network drive where possible. However, if stored, Sensitive Information must always be encrypted.

Instructions for how to encrypt Sensitive Information:
- On an iOS device, where the device itself is password-protected, all data on the device is automatically encrypted.
- On Android ***Nexus*** devices there is a separate step for encrypting data on the device. It can be found here: https://support.google.com/nexus/answer/2844831?hl=en&ref_topic=3416293

- For all other devices (including laptops and flash drives), contact the Help Desk for instructions on how to encrypt data. Special software may be required.

4. Have the Device's remote erase feature, if available, enabled. Users should review and familiarize themselves with erase procedures before using a Device. Information on erasing a Device can be found on the Hofstra portal (http://www.hofstra.edu/About/IT/HelpDesk/HelpDesk_mobilewipe.html). If a Device is lost, Users must immediately take steps to remotely erase the data.

5. Notify their management of the loss or theft of a Device.

6. Ensure all Sensitive Information is removed from the Device before it is returned, exchanged or disposed.

Users who have any questions regarding the use of their Device should contact the Help Desk (516-463-7777). The Help Desk can assist with questions such as how to remotely erase the Device, enable security settings or ensure that encryption is appropriately implemented to protect data on the Device.