Wake Forest University

Standard

Security Standards for Mobile Devices

Legal Department / Director of Information Security

Revision History

Revision	Date	Summary	Editor
1.0	November 19, 2012	Original release	Joel Garmon

Wake Forest University
Security Standard for Mobile Devices

Introduction and Purpose

All WFU departments and employees are responsible for protecting WFU information no matter where it is stored. The widespread use of Smartphone, notepad, and tablet technology by WFU employees has increased the risk of unauthorized disclosure of sensitive information in violation of WFU policy and federal and state laws and regulations. All users accessing WFU information on mobile devices must comply with this standard.

Definitions

The Information Security Department is responsible across the University for all aspects of information and data security and complying with laws and regulations related to cyber security.

Information Systems (IS) Security is in the Information Systems Department and is responsible for all information and data security within IS. IS Security is also used as a resource for Information Security

Scope

This standard is applicable to all WFU departments, schools, and offices that have any device that synchronizes with a WFU network or data source and/or stores WFU data. This includes faculty, staff, student contracted employees and temporary employees.

Standard

1. For all smart phones or note pad type devices, the following security mechanisms must be implemented:
   - At least a 4 character PIN/password required at power-on or resume inactivity time-out
   - After a maximum of 10 minutes inactivity the device must require a PIN to be entered for further use (except for answering a telephone call).
   - After the entry of 10 consecutive invalid PINs the device will be wiped automatically preventing further use of the device or access to Confidential Information.
   - The device must be able to be to have data deleted or wiped remotely.
   - All WFU data stored on the device must be encrypted.

2. The user must contact the WFU Service Desk or Information Security if their device is stolen or lost immediately after discovery of the theft or loss. In addition, the user must obtain approval prior to cancelling or changing their cellular service for the lost or stolen device. This is to allow time to remotely wipe the device prior to connectivity being lost.
3. The user must contact the WFU Service Desk or Information Security immediately in the event the user becomes aware of or suspects any other compromise of their Smartphone/PDA.
4. All University data must be confirmed removed from the device prior to employee separation or the device may be wiped.

Contact Information Security at infosec@wfu.edu