IT USE GUIDELINE

IT User Guideline – Mobile Device Security

This Guidance document explains UA's official recommended position on the security requirements of smart devices that access UA's Exchange e-mail, and/or store sensitive University data. UA maintains two major services that support the synchronization of data between smart devices and UA's Exchange messaging and calendaring system: BlackBerry Enterprise Server (BES) and Exchange ActiveSync (EAS)

Effective as of: **12/1/2011**

Sponsor and Approvers:

J. Ashley Ewing, UA Information Security Officer

John McGowan, CIO

Status of Guideline: **Published**

Audience:

This IT Guideline should be observed by:

Students ☐ Faculty ☒ Staff ☒

Contractors/suppliers ☒

Other (specify) ☐ Click here to specify "other".

Statement of need and purpose:

This policy applies to any smart device either University owned or privately owned that accesses UA's Exchange e-mail systems, and/or stores sensitive or regulated UA data.

Guideline:

To improve the security of University sensitive and regulated data stored on smart devices, UA requires the following security settings (when supported) on all smart devices storing sensitive UA data and/or using the University BES or EAS services:

- A non-trivial numeric device passcode with a minimum required length of four characters. Passcodes consisting of additional character sets or greater lengths are allowed.
- An inactivity timeout to automatically lock the device after a maximum of fifteen minutes
- Data storage encryption (when supported by the device)

- Automatic data wiping after ten failed passcode entry attempts
- Enable the ability to remotely wipe data from lost/stolen devices
- Prohibit users from modifying or disabling security safeguards

These requirements will be enforced by UA's IT infrastructure where feasible (e.g. BES and EAS servers). Any device that is not capable of meeting these requirements is prohibited from being used to store University data considered confidential or restricted (student records, patient records, financial records, etc.). Users who are not storing sensitive University data considered confidential or restricted on their device, and are using the BES or EAS service to connect to Exchange, may request an exemption from this policy. In order to receive an exemption, they must assert that they are not storing any sensitive data on any smart device that they use.

BlackBerry Devices

University Exchange users wishing to use a BlackBerry device to access their email and calendar must use the Universities BlackBerry Enterprise Server (BES), which ensures a proper connection with the Universities Exchange environment and enforces the required security policies.

ActiveSync Devices

University Exchange users with devices that are capable of performing ActiveSync connections to retrieve messaging and calendaring information must use the University's Exchange ActiveSync Server (EAS). Smart devices capable of enforcing the necessary security configuration settings via EAS are required.

IMAP and Other Protocols

Many smart devices have the ability to retrieve email using IMAP and other mail protocols or services. While this allows for email access, it does not provide access to other components such as the calendar, nor does it enforce security policies. Individuals may use IMAP to access email from a smart device, but the device must also be configured to conform to the requirements of this policy in order to protect the email contents from disclosure.

Lost or Stolen Devices

Users are required to immediately report lost or stolen smart devices to the OIT Service Desk so that a remote wipe of the device may be initiated. Users must also immediately change their UA password to protect against unauthorized access to other UA IT resources.
The wiping of a smart device will result in the loss of ALL data on the device, including contacts, pictures, notes, applications, text messages, etc. Smart device users should always maintain a current backup of their device(s) so that data may be easily restored in the event that a device must be wiped.

Decommissioned Devices

Smart devices that will no longer be used must be wiped and reset to factory defaults before disposal. This may be done through BES, ActiveSync, or via the device's built-in reset utility.

Sanctions

Failure to Comply with University's Smart Device Security Guidance document may result in:

- Suspension or termination of access;
- Disciplinary actions (up to and including termination of employment) in accordance with applicable university policy or regulatory policy;
- Civil or criminal prosecution.

Compliance:

Compliance to Guidelines is voluntary but recommended. Not adhering to guidelines can cause disruption to services, security exposures, and/or adverse impacts to other users. Enforcement of guidelines is addressed when deviations cause issues for others or result in known and significant security exposures and are handled through the organizational management structure.