Policy 5.14
Smart Device Security Policy

Responsible Official: Enterprise CIO and Sr. Vice Provost for Library Services and Digital Scholarship
Administering Division/Department: LITS: Library & IT Services
Effective Date: January 01, 2012
Last Revision: July 20, 2017

Policy Sections:

Overview

This policy explains Emory's official position on the security requirements of smart devices that access Emory Exchange e-mail, and/or store sensitive Emory data. Emory maintains a centrally managed service that supports the synchronization of data between smart devices and the Emory Exchange messaging and calendaring system: Exchange ActiveSync (EAS).

Applicability

This policy applies to any smart device, either Emory owned or privately owned, that accesses Emory Exchange e-mail, and/or stores sensitive Emory data.

Policy Details

To improve the security of Emory data stored on smart devices, Emory requires the following security settings (when supported) on all smart devices storing sensitive Emory data and/or using the EAS service:

- 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 Emory's IT infrastructure where feasible (e.g. EAS servers). Any device that is not capable of meeting these requirements is prohibited from being used to store Emory data classified as confidential or restricted (student records, patient records, financial records, etc.).

ActiveSync Devices

Emory Exchange users with devices that are capable of performing ActiveSync connections to retrieve messaging and calendaring information must use Emory's Exchange ActiveSync Server (EAS). Smart devices capable of enforcing the

necessary security configuration settings via EAS are required.

For a list of mobile ActiveSync clients and their support for these requirements:
http://it.emory.edu/security/smart_device/

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 Emory Service Desk so that a remote wipe of the device may be initiated. Users must also immediately change their Emory password to protect against unauthorized access to other Emory 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 ActiveSync, or via the device's built-in reset utility.

Sanctions:

- Failure to comply with this policy may have legal consequences and may result in:
  - Suspension or termination of access;
  - Disciplinary actions (up to and including termination of employment) in accordance with applicable university policy.

Definitions

Smart device – A mobile computing device such as smartphone or tablet.

Exchange ActiveSync (EAS) – A protocol developed by the Microsoft Corporation that allows for the synchronization of e-mail, calendars, tasks, and contacts between a Microsoft Exchange e-mail server and a mobile device. EAS is supported on most non-BlackBerry smart devices.

IMAP – (Internet Message Access Protocol) A commonly used protocol that defines how messages are retrieved from an e-mail server. IMAP does not support synchronizing calendaring, contacts, or tasks.

Related Links

- Current Version of This Policy: http://policies.emory.edu/5.14
- Mobile Device Setup Information for Android and IOS (http://it.emory.edu/office365)
- List of mobile ActiveSync clients and their support for these requirements (http://it.emory.edu/security/smart_device)

Contact Information

Subject	Contact	Phone	Email
Clarification of Policy	Brad Sanford	404-727-2630	brad.sanford@emory.edu

Revision History

- Version Published on: Mar 17, 2016 *(Updated sanctions language)*
- Version Published on: Mar 17, 2016 *(Updated to remove BES)*
- Version Published on: Jan 06, 2012 *(Original Publication)*