Personal Computational Device Security

Portable Computational Device Security Policy

an Information Technology Services Policy

Purpose

Tennessee State Code 47-18-2901 defines that the university must have safeguards and procedures to ensure that confidential information is protected on laptops and other portable devices. Currently, all university owned laptops have enterprise drive encryption enabled by Information Technology Services (ITS) when the device is received. This policy is intended to ensure the integrity of university data that might be stored on other portable devices whether university property or personal property.

Definitions

Portable Computational Device: A computational device that can connect to a wired or wireless network and exchange data with university servers. This can include tablet computers and smart phones. Most of these devices are used to connect to the university email server for calendar, contact and email information.

Procedures to Enforce Portable Device Security

Any other portable device that connects to the ETSU email server must respect the current Active Sync Policy. This software policy requires specific security be present and active on the portable device before communication with the server is allowed. These are:

Password with complexity

The device must have a password placed on it that is of sufficient complexity to protect data resident on the device. For a portable device, this will not be required to be the same as the users Active Directory password. The minimum size will be 4 characters and must include at least 1 alpha character, 1 numeric digit and 1 special character. The password will not expire but can be changed by the user at any time.

Idle device locking

After 30 minutes of inactivity, the device will lock and not display data. The user will be required to enter their device password before it can be used.

Remote erasure

If a device is lost or stolen, the user will have the ability to erase all data on the portable device remotely. This is done by logging into the Outlook Web Access (OWA) server. ITS will also be able to assist users with this if they are unable to successfully execute the remote erasure.

Supplemental Information

Link to Tennessee State Code Annotated 47-18-2901

Approved: Information Technology Governance Council

Reviewed: November 2015

//   // //   // //   // // $(function() { $("#rightColumn").stick_in_parent({ parent: ".float_container" }); }); //