EDINBORO UNIVERSITY OF PENNSYLVANIA

MOBILE DEVICE GUIDELINES

Recommended for Approval by Mr. Guilbert Brown, Vice President Finance and Administration

Approved by Dr. David Werner, Interim President on February 2, 2016

Review Date: As Required

PURPOSE

The Mobile Device Guidelines are intended to assist members of the University community to comply with University Computing Policies when using a mobile device (laptop computers, tablet devices, smartphones, usb flash drive or other external storage devices etc.). In no case do the guidelines take precedence of the policies.

SCOPE

The guidelines are applicable to any university-owned mobile device and any other mobile device used to access or store information requiring a university-provided username or password. Examples include, but are not limited to, Edinboro University e-mail, information systems like Banner, SAP and SAP Employee Self Service, secured internal websites, distance learning tools like D2L, or any document accessed via a secured network drive.

GUIDELINES

1. Prior to purchase of a mobile device, review University Policies and information specifically related to mobile devices. Review the following specific policies:
    a. Acceptable Use
    b. FERPA
    c. Information Security and Data Classification

2. Password-Protect Device and Use Encryption
    a. Password-protect the device as this will be critical should the device become either lost or stolen.
    b. Avoid using unencrypted usernames and passwords when accessing networks, applications or files.

3. Avoid using Device to Store Sensitive or Confidential Information
    a. Avoid storing sensitive or confidential information on the device whenever possible and encrypt the information when it must be stored on the device.

4. Limit Risk of Theft
    a. Avoid leaving the device in public places, visible in a parked car or checked with luggage during the flight.

5. Use Anti-virus and Related Tools/Update Device Frequently
    a. Follow the University's safe computing guidelines
    b. In particular, use anti-virus/anti-malware tools as prescribed.
    c. Ensure that all software on the device is updated frequently as these often address security concerns.

6. Enable Only Required Applications or Services
    a. Restrict the 'apps', services, etc. on the device only to those needed. Disable or remove all others. This action will reduce the exposure of the device to viruses and malware. It may also enhance the performance of the device while also extending battery life.
    b. Review security settings on required applications to be as strict as practical.

7. Report Lost or Stolen Devices
    a. Report lost or stolen devices used to access information within the scope of these guidelines to the University Police and to IT leadership immediately.
    b. Record the device's serial number to assist in recovery efforts.

8. Back-up Device
    a. In the event that sensitive or confidential information must be stored on the device, back-up the device regularly. This is important if the device is lost, stolen or damaged.

9. Dispose of the Device Properly
    a. Make certain all sensitive or confidential information is removed from the device when it is no longer going to be used.

REFERENCES:

Edinboro University Information Security and Data Classification Policy C056 - http://www.edinboro.edu/directory/offices-services/hr/policies/documents/Information Security and Data Classification Policy.pdf

CONTACT INFORMATION:

Vice President Finance and Administration
219 Meadville Street
Edinboro, PA 16444
814-732-2585