Mobile Device Management

Purpose

Tennessee Code Annotated § 47-18-2910 specifies that state agencies must have safeguards and procedures to ensure that confidential information is protected on laptops and other portable devices. All college owned laptops in use by faculty or staff have enterprise drive encryption enabled by Information Technology. This policy is intended to ensure the integrity of college data that might be transmitted or stored on other portable devices used by DSCC faculty and staff regardless of whether the device is college property or personal property.

Scope

The policy applies to all laptops or other portable devices used by DSCC faculty and staff that connects to the DSCC email server(s) and other college systems regardless of whether the device is college property or personal property. The college recognizes and allows employees, although not required, to use a mobile device to connect to the college's resources to access and synchronize email data, contacts and calendar information. All usage must comply with state and federal laws, as well as the college's policies governing appropriate use of technology (including the Computing, Network and Communications Acceptable Use Policy 11:02:04:00).

Policy

1. Use with E-mail
   Any portable device used by faculty or staff that connects to the DSCC email server must respect the current mobile device management policy. This software-enforced policy requires specific security be present and active on the portable device before communication with the server is allowed. These are:
   a. Password requirements:
      i. The device must be configured with a password, PIN, or biometric authentication.
      ii. The minimum length of the password or PIN will be 4 characters. Longer passwords are encouraged if the device has the capability.
      iii. The password must be complex if the device is capable of complex passwords. A complex password would contain at least 1 alpha character, 1 numeric digit and 1 special character.
   b. Idle device locking:
      i. After 10 minutes of inactivity, the device will lock and not display data. The user will be required to enter their device password to unlock the device.
   c. Remote erasure

i. If a device is lost, stolen or taken out of service, the user will have the ability to erase all data on the portable device remotely. Information Technology staff will also be able to assist users with this process.
ii. In the event of 10 failed login events, the system will automatically remotely wipe the device.

2. Use with Other Systems

   Self-Service Banner and the Jaggaer application are considered acceptable for use with personal mobile devices, however, *personal* mobile devices should not be used to access the college's Enterprise Resource Planning system (currently Ellucian Banner) or any other system that contains personally identifiable information, bank account information or credit card information for students, employees, alumni or vendors of the college.

3. Report a Lost or Stolen Mobile Device

   It is the employee's responsibility to report a lost or stolen mobile device containing any college data (including e-mail) to the Vice President for Information Technology and Facilities Management. The IT staff will assist with the remote wipe of the device as needed.

Compliance

All DSCC employees are expected to abide by this policy. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or suspension.

Definitions

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

Revision History

New policy approved by Admin Council on July 29, 2016.
Policy revised July 2024. Policy approved by Administrative Council on 7/30/2024