Standard for Mobile Computing Devices

Objective

In accordance with the Information Security and Acceptable Use Policy, all mobile computing devices owned or managed by UTD must comply with the following standard. This standard also applies to personally-owned mobile computing devices used to store Confidential or Controlled Data (i.e., a personally-owned smartphone used to access UTD email).

Mobile computing devices are tablets, smart phones, or other devices designed to be easily portable that do not run a traditional operating system such as Windows, Mac OS, or Linux. They often use an operating system such as iOS, Android, or Windows Phone and are capable of creating, storing, or processing University Data. (Requirements for laptops or tablets that use a traditional operating system are available in the Standard for Desktops and Laptops.)

Authentication

All mobile computing devices must be configured to require authentication based on a PIN, passcode, or biometric scan in order to unlock the screen and access the device. After a period of inactivity not to exceed 15 minutes the device must lock automatically and require the user to correctly authenticate again.

Encryption

UTD-issued mobile computing devices must be encrypted.

Any personally owned computing devices on which Confidential Data is stored or created must be encrypted in a manner which protects the Confidential Data from unauthorized access.

Physical Security

Mobile computing devices should be physically secured in situations where theft is likely (i.e. place inside vehicle trunk when traveling, do not leave unattended at a coffee shop or food court, and/or lock in hotel safe when provided).

Applications

The Information Security Office recommends installing and configuring an application that allows the owner of the device to locate it in the event it is lost or stolen.

Data Removal

Users are required to remove University Data from any device before giving it to a third-party for maintenance, re-use, or trade-in. Users of mobile devices may initiate a remote wipe sequence using self-service tools within the Outlook Web Access portal, in the event that their device is synchronizing via Exchange ActiveSync. Mobile computing devices may also be subject to remote wiping by

authorized University personnel in the event owner's affiliation with UTD ends, the device is lost or stolen, or at the direction of the CISO to contain an incident.

Exemptions

In the event that compliance with this mobile device standard cannot be met, please contact infosecurity@utdallas.edu to submit an exemption request which will be approved or denied by the CISO. Denied exemption requests may be appealed to the UTD President for final decision.