12. Mobile Device

Overview

Defines measures that should be followed to ensure safety and security of UAEU information stored on mobile devices.

Scope

This policy applies to all users at UAEU, who are locally or remotely accessing the UAEU network.

Objective

The objective of this policy to provide best possible security measures for the mobile devices.

Policy

1. Users must follow and implement UAEU Mobile Devices IT Security controls for securing protected data stored on the mobile devices. UAEU critical or protected data must not be stored on the mobile devices unless effective security controls have been implemented to protect the data. Users must use encryption or equally effective measures on the mobile devices that store UAEU critical or protected data. Other effective measures include physical protection that ensures only authorized access to the stored information.
2. **Personally owned devices**
   a) An appropriate passcode/ password must be set.
   b) Device must be configured to auto-lock after a period of inactivity (not more than 10 minutes).
   c) The loss or theft of a device must be reported to IT Help Desk (reset the user password etc.).
3. **University Owned Devices**
   Devices supplied by the University must meet the minimum security requirements listed above and in addition the following requirements:
   a) No unauthorized changes to supplied device
   b) Device must return to the University, when they are no longer required.