Ibn Sina University

Mobile Computing Policy

Purpose

The purpose of this policy is to ensure that effective measures are in place to protect data in respect of the use of mobile computing, communication and storage devices. Protection should be in place to avoid the unauthorised access to or disclosure of ISU sensitive data stored and processed by these devices.

Scope

This policy applies to all ISU employees and students using mobile computing devices (Laptops, Tablets, etc.), mobile communication devices (mobile phones, smart phones, etc.) and mobile storage devices (e.g. External drives, encrypted USB memory sticks) to access ISU resources in public places, meeting rooms, and other unprotected areas both within and outside the campuses of Ibn Sina University. Note that this policy applies equally to information stored on or accessed via home PCs.
Mobile Computing devices used by contractors, or third parties, to access the ISU network, applications, and/or data are subject to the appropriate ICT Policies and guidelines, e.g. Network Connectivity Policy, Remote Access Policy, ICT Compliance Policy, Data Classification Policy and Data Handling Guidelines.
Templates covering the provision of goods and/or services by Third Parties to ISU are available from the Procurement Office, Finance Department.

Policy Statement

1. Mobile computing, communication and storage devices have become popular because of their convenience and portability. However, the use of such devices is accompanied by risks that must be recognised and addressed to protect both the physical devices and the information they contain. Special security issues that relate to mobile devices include the following:
a. Any malware (viruses, worms, Trojans) that infect the device can bypass the university's security and spread rapidly to other devices once connected back to the network;
b. If data stored on a mobile device is not backed up by the user, it could be completely lost if the device is stolen or fails;
c. Any sensitive data stored on a mobile device would be compromised should it be stolen or lost.

2. The storage of sensitive personal data on USB keys is prohibited.
3. Where it is necessary to store sensitive data on a mobile device, e.g. laptops, mobile phones, users are required to observe this policy to assure that all possible steps have been taken to keep the university's sensitive data secure.

User Responsibilities

1. The following security controls, when available, must be activated on all devices to help protect against theft of sensitive ISU information contained on a device:
a. Encryption software must be installed on all mobile devices used to store/transfer ISU sensitive data. USB devices must not be used to store/transfer sensitive personal data.
b. All mobile devices must have a password protected keyboard/screen lock that is automatically activated by a period of inactivity. The inactivity time interval should be no more than 15 minutes.
2. When not at your desk for an extended period of time your device must be physically secured (i.e., locked in a desk drawer or filing cabinet, locked in an office, or taken with you).
3. When travelling, the following is recommended practice where possible;
- Keep devices in your possession at all times.
- Do not put devices in checked baggage, and be alert to the possibility of theft when going through security checkpoints at airports.
4. When using a laptop, do not process personal or sensitive data in public places e.g. on public transport.
5. Passwords for access to ISU systems should never be stored on mobile devices where they may be stolen or permit unauthorized access to information assets.
6. If your mobile device is stolen or lost, please consult Data Protection - Guidance for Staff and Student regarding required actions.

Related Documentation

Users should be familiar and comply with the following related documents;
a. Remote Access Policy
b. Network Connectivity Policy
c. *Data Handling Guidelines*
d. *Data Protection Guidelines*

For further details on any aspect of this policy, please contact: Director, ICT Tel: 0912202278