 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Mobile Computing and Teleworking	Last Review date	10/05/2024
	Policy Number	ITC-23	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

Overview

This policy is to outline the University's requirements of mobile computing users in relation to the proper ownership of its mobile computing assets, the operational aspects and the security of information accessed whilst using such devices. The policy applies to both mobile devices issued and owned by the University of Sharjah and personally owned mobile devices. (BYOD).

Scope

This policy is applicable to all faculty, employees and students as well as all third party personnel who are using University of Sharjah's mobile computing devices such as laptops and, tablets, embedded devices and smart phones.

Purpose

The purpose of this policy is to the minimize risks associated with the use of mobile computing devices, and define controls against the threats of unauthorized access, theft of information, and malicious disruption of services

Abbreviations and Definitions

CMDB: Configuration Management Database.

The CMDB is intended to contain all relevant information about hardware and software components and the relationships between those components used in the IT infrastructure.

UoS: University of Sharjah


BYOD: Bring your own device refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.

Mobile Computing: A technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link.

Mobile computing devices: Device used in mobile computing such as, smartphones, laptops, portable PCs, tablet PCs, Personal Digital Assistants, etc.

Policy

- Mobile computing devices (e.g. laptop computers, iPad, iPhone, etc.) issued by University of Sharjah shall be used for business / academic purposes only. Only UoS approved mobile devices/laptops shall be connected to the enterprise UoS Network.


 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Mobile Computing and Teleworking	Last Review date	10/05/2024
	Policy Number	ITC-23	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

- Emails sent from mobile devices must abide by University of Sharjah's E-mail and Electronic messaging policy.
- Anti-virus software must be present on all mobile devices. This shall be as per the antivirus and malware policy.
- Loss or theft of mobile computing devices shall be reported to UoS ITC service desk immediately, mentioning criticality of information stored on the device. ITC service desk should inform the relevant teams
- All mobile computing devices (e.g. laptop computers, palm top computers, notebooks, and mobile phones) shall be used in a secure environment, using cryptographic controls for communication purposes wherever possible.
- Mobile computing devices must be kept physically secured at all times.
- When stored unattended in vehicles they must be stored locked in the vehicle. However, users shall try to avoid leaving the mobile devices in the unattended vehicles.
- Mobile devices should be protected from environmental threats such as dust, excessive heat, and radiation with suitable measures such as using protective equipment.
- When the user of a mobile device changes, it shall be ensured that no sensitive (confidential and restricted) data is present on them.
- The ownership, location and other asset details should be updated in the asset register and CMDB when the laptop is transferred to a different user.
- The relative details of the mobile equipment should be maintained so that it can be easily retrieved for any warranty or insurance purposes. (Serial Numbers, Make, Model, HDD, RAM, Operating system etc.)
- It should be ensured that only the standard and licensed operating system along with latest patches and security fixes is installed on the mobile devices.
- Critical and valuable confidential data must be backed up on a regular basis by the users.
- All the data on the laptop shall be backed up and kept in a safe and secure place before any travel by the user outside UAE.
- Use of mobile devices shall be consistent with the UoS acceptable usage policy.

Procedures

Change Management and Maintenance

1. ITC Service desk shall re-imaged / restore factory settings of the mobile computing device, before it is taken back to the store for storage and issued to another user.

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Mobile Computing and Teleworking	Last Review date	10/05/2024
	Policy Number	ITC-23	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

2. Laptops shall not be transferred internally without the knowledge of ITC Service desk. Data must be initialized before providing the laptop to the next user.
3. The Ownership, Location and other relevant Asset Details shall be updated in the Asset Register and CMDB when the mobile computing device is transferred to a different user.
4. If the mobile computing device has to be sent for repair, the data shall be secured from unauthorized access by means of removal of hard disk or encryption.

Reference

SI No	Standard Name	Control Reference
1	ISO 27001:2013	A.6.2.1