 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	BYOD	Last Review date	19/5/2021
	Policy Number	IT-10	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

Overview

This policy establishes a standard set of rules and requirements that help manage and control the use of personally-owned end user devices, like laptops, smart phones, and tablets for the University of Sharjah academic / business requirements.

Scope

The policy is applicable to all Faculty, employees and students, including but not limited to, contractors, third party users, consultants, and temporary users at the University of Sharjah who wish to use personally-owned mobile computing devices and laptops for business/academic purposes.

All users bringing in BYOD devices act as an asset owner and are responsible to commit to relevant controls as per this policy.

All computing devices, laptops/ purchased by UOS are not considered as BYOD and will not apply to this policy.

Purpose


The purpose of this policy is to empower UoS all users to choose a device of their preference, including personally-owned consumer smartphones, tablets and laptops, to carry out UoS approved business / academic transactions. This policy intends to provide direction to embrace BYOD strategy in a secure and controlled manner.

Policy

Usage of Smart-Phones, Laptops and Internet

All UOS faculty, employees, students and third party are allowed to use their own personal computing devices for Administrative / Academic purposes. As per below policy statements.


1. BYOD users are entitled to maintain the confidentiality of the UOS related information shared.
2. The university reserves the sole right to cancel the eligibility of BYOD at any time without giving any prior notice
3. UOS withhold the rights to audit computing devices for verifying the usage of authorized software and OS versions.
4. All users shall refrain from the installation of any software or download any content against any legal or regulations while using those devices as BYOD.
5. Users shall not use any “jailbreak” version of operating systems on their laptops.
6. All UOS employees shall be obliged to maintain confidentiality and integrity of all University information stored on their BYOD devices.

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	BYOD	Last Review date	19/5/2021
	Policy Number	IT-10	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

7. Users are expected to use their devices in an ethical manner at all times and adhere to the UOS “Acceptable Use Policy”. Staff shall ensure due diligence when BYOD service is availed
8. Appropriate HR contractual clauses need to be enforced and BYOD clauses shall be incorporated in contract (employee contract / students admission forms)
9. All information shared by an employee shall have proper classification and document labelling.

Protection of the device from unauthorized access

1. BYOD users must secure personally-owned computing devices that are used for business / academic purposes, from unauthorized access and/or modifications and/or loss or theft of the device.
2. In case of any loss or theft of the device, all complains should be reported to ITC Service desk / Information security team.
3. BYOD users shall never leave desktops/laptops unattended for an extended period of time unless it has been properly safeguarded with controls like screen lock.
4. BYOD users are required to provide username and password while logging in the devices to avoid unauthorized access.
5. BYOD devices, where possible shall be configured to remote wipe the data in case of any data compromise.
6. Physically secure your laptops when not in use.
7. Laptops must always be carried in person and not be checked in as baggage while travelling.
8. BYOD devices users shall ensure personal responsibility of UOS data while working in personal / public spaces
9. In the event where desktop/laptop equipment are required to be sent to workshops for repairing purpose, the user of the device shall ensure all the logged in applications and services are appropriately logged-off and all university related information is secured.
10. Users must install suitable antivirus/antimalware software on their laptops and mobile devices with updated signature. This Antivirus software must automatically update signatures.
11. UOS data shall not be downloaded to BYOD computing devices and should be stored only in UoS Network.
12. All removable media devices shall automatically be scanned on connecting to Computing devices.

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	BYOD	Last Review date	19/5/2021
	Policy Number	IT-10	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

13. BYOD users shall use only the licensed version of software on their laptops.
14. Appropriate Network access control measures and posture assessment must be carried with automated IT controls while allowing BYOD devices to network.

Reference

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

UoS Policy reference:

- UoS Wireless Security Policy_V0.1
- UoS Network Security Policy_V0.1
- UoS Mobile Computing and Teleworking Policy_V0.1
- UoS IT Service Management policy_V0.1