جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Wireless Security	Last Review date	19/5/2021
	Policy Number	IT-32	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

Overview

This wireless policy defines the use of wireless services within the University of Sharjah and specifies how wireless networks shall be managed, configured and used.

Scope

This policy is applicable to all wireless systems, and information processing facilities, personnel as well as all third party personnel who are connected to UoS wireless networks.

Purpose

The purpose of this policy is to minimize risks associated with the use of wireless network access and define controls against the threats of unauthorized access, theft of information, and theft of services and malicious disruption of services by ensuring seamless wireless network services.

1. Wireless Local Area network is managed securely.
2. Security technologies are implemented as per the standard

Abbreviations and Definitions

AAA – Authentication, Authorization and Accounting

AD active directory Identity access management

Policy

Access and Authentication to Wireless Network

1. Only University of Sharjah AD IDs shall be granted access to connect to the enterprise wireless network.
2. The wireless connection to faculty, employees and users shall be only for domain registered devices with the University of Sharjah network.
3. Wireless accessed Guest accounts and student or staff BYOD devices must have Network access control with minimums AV protection and acceptable patch level enforced. This access must be regulated with appropriate technologies such as, RADIUS/TACACS with the relevant AAA (Authentication, Authorization and Accounting) controls aligned with University IAM.
4. UoS faculty, employees and students' wireless connection must be aligned with university authentication policy. Connection request shall be approved by the concerned department prior to access.
5. Guest wireless access shall be as per the automated approvals process.

6. The University of Sharjah password policy shall be followed for access to wireless networks. Passwords and information on wireless medium shall not be stored in clear text. The strongest form of wireless authentication permitted by the client device shall be used.
7. Wireless communication enabled devices should have strong user authentication such as WPA2.
8. Wireless access points shall require user and device authentication at the access point before granting access to University of Sharjah network services
9. Wireless networks design shall avoid physical and logical interference with other network equipment

Guest wireless access

Guest users shall be authenticated using a unique password sent through registered mobile number.

Access to University of Sharjah applications from guest network shall be restricted.

University of Sharjah Guest wireless network and WLAN (Internal network) shall be segregated.

Terms and conditions of guest wireless network usage must be developed and shared with the registered user. The following shall be at a minimum:

1. Conducting or participating in illegal activities, including gambling, accessing or downloading obscene contents
2. Solicitations for any purpose which are not expressly approved by UNIVERSITY OF SHARJAH management
3. Revealing or publicizing proprietary or confidential information
4. Uploading or downloading commercial software in violation of its copyright interfering with the normal internet services is prohibited.
5. Appropriate technical controls shall be used to prevent excess internet bandwidth utilization

Monitoring, Audit and Administration of University of Sharjah WLAN infrastructure

All wireless LANs shall be routinely monitored and security audits performed to verify that security configurations comply with this policy.

The Information Security Team will conduct yearly audits of access points to ensure that security configurations conform to this policy and related Information Security Policies of University of Sharjah

Access logs and system audit trails shall be maintained and routinely monitored through **SIEM**

Security incident event management systems.

Wireless network systems should be subject to periodic risk assessment by the operations and security teams.

The Administrators are required to change factory default settings and use strong administrative passwords on all wireless devices to ensure higher-level of security.

All insecure and nonessential management protocols shall be disabled.

To the extent possible, the Administrators shall ensure that their wireless implementation and associated security technologies are up-to-date with evolving standards and best practices.

Reference

Sl No	Standard Name	Control Reference
1	ISO 27001:2013	A.6.2.1, A.13.1.1, A.13.2.1