UNIVERSITY
OF BAHRAIN

INFORMATION TECHNOLOGY

Wireless Security Policy

Authority / Information technology Center

Effective: 17 March 2019

Table of Contents

POLICY TITLE

Title: Wireless Security Policy

Policy Description: This policy minimizes risks associated with using wireless network access.

Policy Scope:	☐ Academic ☐ Administrative ☐ Research ☐ Student ☒ general
Policy Status	☐ New policy ☒ Revision of existing policy
Approval Authority:	University of Bahrain Council
Authority/ Owner of Policy:	Information Technology Center
Approval Date:	10 March 2019
Effective Date:	17 March 2019
Approval Date of Last Revision:	10 March 2019
Date of Next Revision:	
Related Documents:	None

Policy Stakeholders

☐ President

☐ Vice President

☐ Legal Advisor

☐ Deans

☐ Directors

☐ Faculty members

☐ Students

☐ Admin Staff

☒ All University Affiliates

1 Policy Purpose

This policy's objective is to minimize risks associated with using wireless network access. It defines controls against the threats of unauthorized access, theft of information, theft of services, and malicious disruption of services.

2 Policy Scope

This policy applies to employees, students, contracted personnel, trainees, and any third-party representatives who have been provided access to wireless services at the University of Bahrain (UOB).

3 Policy Statement

3.1 General Requirements

- The IT Center should ensure all wireless LAN accesses have approved security configurations.
- The IT Center should Use encryption protocols.
- The IT Center should maintain a hardware address (MAC address) that can be registered and tracked.

3.2 Authorization

- All deployments of wireless networks should be controlled and approved by the IT Center.

3.3 Authentication of Wireless Clients

- All access to wireless networks must be authenticated.
- The most potent form of wireless authentication permitted by the client device shall be used. WPA or WPA2 with 802.1x/EAP-PEAP must be used for most wireless devices. WPA2 is preferred wherever possible unless there is a technological limitation. A minimum of 128-bit encryption must be used. Technological Limitations should be resolved as soon as possible, and periodic review and monitoring should be performed.
- WPA keys shall be changed after a known or suspected compromise or when personnel changes occur.
- Factory default WPA keys shall be changed before deployment.

3.4 Encryption

- The most potent form of wireless encryption permitted by the client device shall be used. WPA using TKIP encryption or WPA2 using AES-CCM encryption must be used.
- Wireless equipment that does not support at least 128-bit key encryption shall not be used.

3.5 Wireless Access Control

- Direct or remote access to UOB's network should be in accordance with the Access Control and Physical Security Policy.
- Unnecessary protocols shall be blocked.
- File sharing on wireless client devices shall be disabled.

3.6 Wireless Client Security Standard

- The IT Center should ensure that all wireless clients have security-related operating system patches applied.
- The wireless solution should be secure in such a way that it can:
  - Detect and Disable Rogue APS.
  - Protect from Denial of Service and Impersonation
  - Protect Man-in-Middle

3.7 Wireless Physical Security

- Access points shall be physically secured upon proper configuration to prevent tampering and reprogramming (i.e., to prevent unauthorized physical access).
- Access points shall be placed in secure areas, such as high on a wall, in a wiring closet, or in a locked enclosure, to prevent unauthorized physical access and user manipulation. They shall not be placed in easily accessible public locations.
- If an access point's reset function is used, the device must be restored to its latest security settings.
- All security settings and baseline configurations shall be backed up and stored securely.

3.8 Wireless Logical Security

- All insecure and nonessential management protocols such as (Hypertext Transport Protocol (HTTP) and Simple Network Management Protocol (SNMP)) shall be disabled.
- If SNMP is turned on for management purposes, the SNMP community strings must be changed from their manufacturer default to unique and difficult-to-guess strings.
- When disposing of wireless equipment, all configurations and security settings must be erased completely.
- Placement of access points and channel assignments shall be such that coverage/throughput is maximized. At the same time, interference (denial of service) is kept to a minimum between different access points or WLANs.

3.9 Inventory Monitoring and Audit

- All wireless connections shall be routinely monitored, and security audits performed to verify compliance with this policy, access points and wireless devices are authorized, and to identify unauthorized activity.
- Access logs and system audit trails shall be enabled at the access point and reviewed regularly.

3.10 Deployment and Configuration

Wireless access points (WAPs) should be deployed and set up by the IT Center.

3.11 Enforcement

- Violations of this policy or supporting policies shall be subject to appropriate action, which includes:

- Temporary or permanent termination of the connectivity, depending on the nature of the violation and the time and efforts taken to resolve the issue.
- Other actions as deemed appropriate by IT Center management.

4 Roles and Responsibilities

This section identifies those responsible for sharing certain policy responsibilities, such as Approval Authority and Policy owner.

- Chief of Information Technology
- Director of Information Technology Center