UNIVERSITY
OF BAHRAIN

INFORMATION TECHNOLOGY

Computer Security Policy

Authority / Information technology Center

Effective: 17 March 2019

Table of Contents

POLICY TITLE

Title: Computer Security Policy	
Policy Description: The policy aims to provide a secure computing environment where data is processed.	
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

The objective of the Computer Security policy is to provide a secure computing environment where data is processed. All computers at University of Bahrain (UOB) shall be configured and used as per this policy.

2 Policy Scope

This policy applies to all UOB Computers owned by UOB or used by UOB employees, contracted personnel, trainees and third party's representatives.

3 Policy Statement

3.1 Computer Protection

- Computer workstations must be locked when the workspace is unoccupied and shut down completely at the end of the workday.
- IT Center is responsible for managing computer antivirus and endpoint security portfolio.
- It is the user's responsibility to report any malicious activity, virus-like activity, or insufficient or unavailability of the antivirus client to the IT Center.
- No user shall have the privilege/rights to disable the antivirus software on his computer.
- All computers shall be configured to generate alerts at the central antivirus server as well as the infected computer.

- Where infected files have not been quarantined, they shall be cleaned manually using tools provided by the vendor or reliable third parties.
- All virus-detected incidents shall be logged as deleted, quarantined, or cleaned by the IT Center.
- Secure user profiles and computer settings shall be configured in a professional manner to protect the confidentiality of data and computing facilities while in use.
- Users should not be able to change the Web browser security settings.
- Where possible and necessary, the add/remove program option shall be disabled.
- Access to registry editing shall be prevented.
- All nodes on the network shall be monitored for patch deployment on a regular basis.
- Users at UOB shall not be provided with local administrator privileges; the local administrator account shall be managed by IT Center and T technicians in some colleges.
- Portable computing devices such as laptops and tablets should be locked away.
- All the classified information regarding computers and the surrounding areas should be in accordance with Law No. (16) 2014 concerning state secrets law.

3.2 Exceptions

All exceptions to this policy shall be explicitly reviewed by the Chief of Information Technology and approved by the Director of the IT Center. If any exceptions to this policy are approved, they shall be valid for a specific period and shall be reassessed and re-approved if necessary.

3.3 Enforcement

Violations of this policy and supporting policies shall result in corrective action by management. Disciplinary action will be consistent with the severity of the incident as determined by an investigation and may include, but may not be limited to:

- Loss of access privileges to information assets
- Other actions as deemed appropriate by civil services Bureau (CSB) rules.

4 Roles and Responsibilities

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

- Chief of Information Technology
- Director of Information Technology Center