UNIVERSITY
OF BAHRAIN

INFORMATION TECHNOLOGY

Incident Management Policy

Authority / Information technology Center

Effective: 17 March 2019

Table of Contents

POLICY TITLE

Title:	Incident Management Policy
Policy Description: aims to mitigate or minimize any harm to users.	
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 aims to ensure the consistent and professional management of information security incidents at the University of Bahrain (UOB) to mitigate or minimize harm to users, information systems, and related devices.

2 Policy Scope

All information created or received by UOB in any format, whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically, or accessed remotely. All employees, students, trainees, and third-party contractors working for or on behalf of UOB and any other person are permitted to have access to UOB premises. In addition to that, UOB manages, holds, or processes information systems with related devices and components. Moreover, all locations UOB's information is accessed, including home use.

3 Policy Statement

3.1 Incident Management

- All users are responsible for reporting actual, suspected, threatened, and potential information security incidents to the IT Center.

- User management is responsible for ensuring that staff in their area comply with all information security requirements and follow the procedures for reporting information security incidents.

- Any information regarding the incident response and management should be by Law no. (16) 2014 concerning protecting state information and documents based on UOB data classification.

- Information security incidents should be assessed according to the incident classification scale provided by the IT Center.

- All information security incidents shall be recorded and archived as a reference or for analysis.

- Where applicable, In the event of critical incidents, infected information systems shall be disconnected from UOB's network until the incident has been resolved and risks sufficiently mitigated.

- The IT Center shall document guidance and procedures for detecting, assessing, and resolving security vulnerabilities, events, and incidents as a reference.
- Responsibilities for reporting and escalating security vulnerabilities, events, and incidents should be clearly defined and communicated to all relevant personnel. "Handler"

- Information security incident reports should be provided to concerned parties periodically.
- Preventive, detective, and corrective controls should be taken into consideration by the IT Center.

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 exist, they shall be approved and valid for a specific time 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 deemed appropriate by Civil Services Bureau (CSB) rules.

4 Roles and Responsibilities

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

- Chief of Information Technology
- Director of Information Technology Center