UNIVERSITY
OF BAHRAIN

INFORMATION TECHNOLOGY

Acceptable Use Policy

Authority / Information technology Center

Effective: 17 March 2019

Table of Contents

POLICY TITLE

Title:	Acceptable Use Policy
	Policy Description: this policy is to outline the acceptable use of Information Technology (IT) resources at University of Bahrain.
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 outline the acceptable use of Information Technology (IT) resources at the University of Bahrain (UOB). These rules are in place to protect the employee and UOB from unacceptable uses and practices that can expose them to risks, including virus attacks, compromise of the network, application systems and services, and legal issues.

2 Policy Scope

This policy applies to all UOB employees, students, contracted personnel, trainees, and third-party representatives who have been provided access to the UOB IT assets. It covers all information systems (Environments operated by the IT Center).

3 Policy Statement

3.1 General Requirements

- Use of the IT systems at UOB must at all the times be performed in a professional and accountable form.
- Users are responsible for protecting any information used and/or stored /accessible through their individual user accounts.
- It shall be considered an offence for one or a group of employees, to be involved in activities that disrupt the organization's ability to pursue its business objectives as per the laws of Bahrain. Actions such as the deliberate disruption of UOBs IT systems, theft and/or destruction of equipment or data services, are serious offences.
- Users are responsible for promptly reporting any theft, loss, or unauthorized disclosure of proprietary information.

- Users shall access, use, or share UOB's proprietary information only to the extent they are authorized and it is necessary to fulfill their assigned job duties.
- Each user is responsible for adherence to this policy in its letter and spirit.
- Users shall not disclose the organization's information to anyone within or outside UOB without proper authorization. All information available to the user in his/her business area or account will be in accordance with Law No. (16) of 2014 based on UOB data classification.
- Users shall not attempt to access any data or programs available on any system without authorization or explicit written approval from the system's owner.
- Users shall contact the IT Center to report any weaknesses they discover in systems and any incidents of possible misuse or violation of UOB policies to the proper authorities.
- The email system is a UOB resource, and users are expected to utilize this for business.
- The user account may not be used to participate in personal financial activity, investments, promotional contests, etc.

- IT Center shall implement suitable virus and spam control measures to minimize/reduce the chances of these infesting into the user's mailbox or spreading unwanted messages from a user's mailbox. This will be done through automatic scan for virus and spam. The findings and infections will be blocked or quarantined depending on the severity level.
- IT Center has the right to reject any infected/quarantined emails that might compromise the system or network.
- Access to another individual's email should be in accordance with the Physical Security and Access Control Policy.
- For the email system, the IT Center should implement security complied strategy to ensure the security in every process.
- All broadcast emails and accounts must be approved by the relevant directorate management.
- Broadcasting unwanted emails containing personal views on social, political, religious or other non-business-related matters are strictly prohibited.
- The IT team will ensure regular backup of e-mail messages on a daily basis

- UOB E-mail systems must be used primarily for business purposes only, and users are strictly prohibited from using them to set up personal businesses or send chain letters.
- The user is responsible for evaluating the appropriateness and the form of the broadcast emails.
- The email service is for the sole use of authorized users. Users are authorized to access, use, copy, modify or delete files and data only in their own accounts and/or the accounts which they have been authorized to access.
- All the issues related to the password to use and access email services should be in accordance with the password policy.
- The email system is a UOB resource, and users are expected to utilize it for personal use only on a limited scale. Email will not be used for personal reasons if it may interfere with the performance of the system or the employee's employment or other obligations. All messages and files composed, sent, or received using UOB's email system are and will remain the property of UOB.
- Users will not use the e-mail system to send, receive, store, redistribute or display emails or files that are illegal or unethical.
- Users will not alter the date, time, source/destination, and/or any other information that is part of the header information of an email message.
- Users are strictly prohibited from using third-party email systems and storage servers, such as Google, Yahoo, and Hotmail, to conduct UOB businesses.
- In case of offensive emails received, the originator of the offensive e-mails should be contacted by the affected user and asked to stop sending such messages or report directly to the IT Center.

3.2 Unacceptable Use

The following practices are prohibited with no exceptions:

- Downloading and storing obscene materials and pornography.
- Circumventing user authentication or security of any host, network, or account.

- Copying confidential business-related data to any removable media, such as a USB Flash Drive or External Hard Drive, without approval.
- Introducing destructive programs (e.g., viruses, self-replicating code) in order to cause intentional damage, interfere with others, gain unauthorized access, or inhibit production to UOB's Information systems.
- Concealing own identity or masquerading as other user/s (Identity Theft).
- Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Using UOB's systems to transmit any communication where the meaning of the message, or its transmission or distribution, is intended to be or is likely to be perceived as being abusive, defamatory, obscene, offensive, or harassing to the recipient or recipients thereof.
- Downloading, installing, or running security programs or utilities that reveal system security weaknesses.
- Effecting security breaches or disruptions of network communication, security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For the purposes of this policy, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing of information for malicious purposes.
- Port scanning or security scanning is prohibited unless prior notification to the IT Center is made and authorized by the IT Center Director.
- Any form of network monitoring that will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job.
- Making copies of system configuration files for the user's own unauthorized use or other people's/users' unauthorized use.
- Interfering with or denying service to any user (e.g. denial of service attack).
- Using UOB Information systems and resources for personal usage or on behalf of a third party (i.e., personal client, family member, political, religious, or charitable organization, school, etc.).

- Attempting to access systems without proper authorization.
- Using internal relay chat and P2P services

3.3 Exceptions

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

3.4 Enforcement

Penalties for breaches of the Acceptable Usage Policy will be based on the severity of the breach and can include:

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

4 Roles and Responsibilities

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

- Chief of Information Technology
- Director of Information Technology Center