UNIVERSITY
OF BAHRAIN

INFORMATION TECHNOLOGY

Access Control and Physical Security

Authority / Information Technology Center

Effective: 17 March 2019

Table of Contents

POLICY TITLE

Title:	Access Control and Physical Security Policy
Policy Description:	Maintain access control and physical security at the 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 defines the controls and standards for maintaining the University of Bahrain (UOB) 's access control and physical security to ensure all assets are secured and information remains accurate, confidential, and available when required.

2 Policy Scope

This policy applies to all UOB employees, students, contracted personnel, trainees, and third-party representatives who have been provided with access to secure areas in UOB, such as data centers and main network rooms, with all related facilities, systems, assistance, and equipment.

3 Policy Statement

3.1 Access Control

3.1.1 The IT Center should implement the necessary controls and measures to protect secure areas from unauthorized access, which are in line with UOB business requirements and based on a formal risk assessment.

3.1.2 Users accessing the information systems at UOB must not use or access an account assigned to other individuals.

3.1.3 IT Centre shall implement suitable controls over the non-UOB equipment when connected to or attempting to access the UOB network.

3.1.4 Strict controls shall be implemented regarding utility programs that may allow the user to override existing system and application controls.

3.1.5 The requester's owner and management shall approve granting access to specific IT resources or services based on the job roles and duties performed by the employee.

3.1.6 All users granted access to the computing resources should be through a unique identification code (user-ID).

3.1.7 A formal record of all registered users shall be maintained by the IT Center. This record shall be checked periodically for unused, redundant, or expired user access accounts or incorrect privileges.

3.1.8 The IT Center rules state that user accounts should be disabled for those who are retired, terminated, or inactive for a period.

3.1.9 Access rights should be reviewed whenever UOB employees change duties and/or positions.

3.1.10 The IT Center should ensure that only minimal system information is disclosed during the logon process and that system or application details are not displayed until the process is successfully completed.

3.1.11 The logon process should validate user credentials only after all the data relating to the log-on process is entered / input.

3.1.12 Any error messages during the log-on process should not be suggestive of the type or kind of error.

3.1.13 The user ID should be locked after a specified number of unsuccessful log-on attempts, as per the password security policy.

3.1.14 The log-on process and unsuccessful attempts shall be logged.

3.1.15 User IDs and passwords for administrators shall not be provided to users.

3.1.16 The IT Centre is responsible for securing the UOB network by dividing it into logical segments based on access requirements, risk management, and duty segregation.

3.1.17 IT Centre should separate the internal network from the external one with different security controls on each network.

3.1.18 The connectivity between internal and external networks shall be controlled by the IT Centre.

3.1.19 Remote users shall connect to the UOB network only through approved and designated remote access services by the IT Centre. Secure gateways and diagnostic ports shall be kept inactive until needed and kept active only for the minimum time required.

3.1.20 Access to shared folders shall be granted by the IT Centre and authorized by the folder owner and requester's management.

3.1.21 Shared folders shall be used for work purposes only. Sharing any non-work-related materials (such as photos, videos, audio files, etc.) is strictly prohibited.

3.1.22 The IT Center is responsible for providing network services needed to support business objectives by explicitly enabling needed services and disabling unneeded services.

3.1.23 Information system network access must be restricted to authorized users and systems using the principle of least privilege.

3.1.24 The IT Centre protects the application systems and related resources.

3.1.25 While creating and activating user accounts for contractors, consultants, temporary workers, or vendor personnel, the Information Technology (IT) team should ensure that the individual exists and is actively performing service for UOB.

3.1.26 Access requests for contractors, consultants, or vendor personnel to UOB information systems shall be stated only in the contractual agreement.

3.1.27 The IT Center must grant Access to UOB application systems after proper authorization from both the system owner and the requesting party's management. Access levels should be assigned based on the principle of least privilege, ensuring users receive no more access than necessary to perform their duties.

3.2 Physical Security

3.2.1 Access to UOB secure areas of information processing facilities, such as Data Centre/server room or areas where sensitive information is kept, must be restricted and clearly demonstrated to prevent any unauthorized physical access.

3.2.2 A manned reception shall be in place to restrict authorized personnel from entering UOB premises.

3.2.3 Suitable personnel will be identified to accompany housekeeping personnel during the routine cleaning of the secure areas.

3.2.4 No photographic, video, audio, or other recording equipment should be allowed into secure areas without authorization.

3.2.5 UOB employees and visitors shall obtain permission before entering the secure areas.

3.2.6 The server room should not be used for storage of any combustible material or hazardous materials.

3.2.7 No eatables shall be brought inside the server room.

3.2.8 For employee/visitor access control system to secure areas, the following details should be captured:

3.2.8.1 Name

3.2.8.2 CPR

3.2.8.3 Date

3.2.8.4 Entry time

3.2.8.5 Exit time

3.2.9 Visitors shall be escorted by authorized UOB staff while entering secure areas.

3.2.10 Access to secure areas outside normal working hours shall be specifically authorized and logged.

3.2.11 Access to secure areas shall be revoked immediately upon termination or resignation of employees or completion of a consultation or vendor agreement.

3.2.12 Access rights to secure areas shall be reviewed and updated regularly.

3.2.13 Wherever possible, multiple entry points to secure areas should be closed, and all authorized personnel shall be directed to enter the secure areas through a common entrance.

3.2.14 Third-party personnel and vendors shall avoid unsupervised working in secure areas, both for safety reasons and to prevent opportunities for malicious activities.

3.2.15 UOB premises shall contain suitable environmental controls to reduce the risk of damage from fire, flood, or other site disasters. Requirements for power, heating, and cooling shall be appropriately addressed.

3.2.16 All secure areas at UOB will be provided with effective fire detection systems, fire alarm systems, and firefighting equipment adequate for the room's size. They will be protected from

theft, flood, excessive heat, and other environmental hazards. Security personnel on duty will always attend to the alarm system to respond to incidents.

3.2.17 The integrity of power, temperature, and humidity control equipment shall be monitored regularly.

3.2.18 All data-secured area equipment shall be provided with a UPS-based power supply, which will be backed up by generator sets.

3.2.19 Adequate detection controls and safety devices, such as fire alarms, smoke detectors, fire suppression systems, etc., should be placed in all secured areas.

3.2.20 The air conditioning systems must be inspected and serviced every six months to ensure they function efficiently. The temperature in secured areas must be maintained between 18°C and 24°C.

3.2.21 Maintenance contracts shall be maintained for a speedy recovery from the failure of air conditioners.

3.2.22 The air conditioning system should be effective, and the temperature in the secured areas should be monitored regularly.

3.2.23 Power going to secure areas should be through an uninterruptible power system (UPS). The UPS should be ensured to be always in working condition.

3.2.24 Circuit breakers of appropriate capacity should be installed to protect the hardware against increased power voltage.

3.2.25 Generators should be provided for power generation in case the general power lines fail.

3.2.26 Self-activating emergency lamps should be placed in secured areas to handle abrupt power failures.

3.2.27 Uninterruptible Power Supplies (UPS) and backup generators must undergo preventive maintenance annually, as per the specifications provided by the vendors. Detailed logs of maintenance history should be maintained to track performance and anticipate potential failures.

3.2.28 Data cables, power and telecommunication lines shall be protected by conduits from any damage, interference, and interception.

3.2.29 Power and telecommunication cables should be segregated.

3.2.30 The UPS and batteries should be provided with the recommended ambience, with special attention to temperature control, humidity, a dust-free environment, etc.

3.2.31 The UPS must be kept on, and the power cord must be properly secured to the equipment. The battery cords must also be properly connected.

3.2.32 It must be ensured that no unauthorized person tampers with or changes the switch settings on the UPS.

3.2.33 Hardware maintenance refers to all activities involved in the upkeep, repair, and review of hardware resources after installation to ensure proper functioning, fault correction, performance improvement, and adaptation of the hardware to the IT environment.

3.2.34 Equipment should be maintained in accordance with the supplier's recommended service intervals and specifications.

3.2.35 Only authorized maintenance personnel should carry out repairs and service equipment.

3.2.36 The activities of on-site maintenance personnel should be supervised to ensure that they don't have unauthorized access to UOB's data.

3.2.37 All equipment/media taken off-premises shall be authorized.

3.2.38 An approved list of authorized signatories shall be prepared and maintained.

3.3 Exceptions

All exceptions to this policy shall be explicitly reviewed by the Chief of Information Technology and approved by the IT Centre Director, Safety and Security Department, Building & Maintenance Department, and Vice President for Information Technology, Administration, and Finance affairs. If any exceptions are approved and valid for a specific period, they shall be reassessed and re-approved if necessary.

3.4 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:

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
- Building & Maintenance Director
- Safety and Security Director
- Vice President for Information Technology, Administration and Finance Affairs