UNIVERSITY
OF BAHRAIN

INFORMATION TECHNOLOGY

Password Security Policy

Authority / Information Technology Center

Effective: 17 March 2019

Table of Contents

POLICY TITLE

Title:	Password Security Policy
Policy Description:	set the requirements for the creation and management of passwords.
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 Centre
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 set the requirements for the creation and management of passwords used to access systems and/or network resources and ensure acceptable levels of protection for such passwords.

2 Policy Scope

This policy applies to all University of Bahrain (UOB) employees, students, contracted personnel, trainees, and any third-party representatives who have been provided access to UOB's information systems and applications. It also applies to all systems, applications, databases, and other technical resources belonging to other UOB entities that are connected to or hosted at UOB.

All passwords for applicable technical resources shall comply with the requirements of this policy.

3 Policy Statement

3.1 Password Management

- Passwords, regardless of which technical resource they grant access to, should be kept private and must, therefore, not be disclosed to any other person.
- Technical resources that do not support the creation of multiple users, such as passwords allowing access to the central network or system

resources (e.g., edge router, firewall, enterprise administrator, etc.), shall be recorded on paper and stored in the department's fire-proof safe. Any change to such passwords must accompany an update to the written record.

- The fireproof safe in which passwords are stored shall be accessible only by the IT center's director.

- Administrators and developers must configure technical resources to store passwords in one-way encrypted or 'hash' form and keep them separate from application data. Salting is encouraged in this regard.

- Passwords shall never be transmitted on the network without encryption. This requirement can be met by transmitting a 'challenge' instead of the password, encrypting the password before transmission, or transmitting the communications channel.

- Allocation of passwords shall be controlled through a formal management process.

- Users must provide their personal details (Name, ID number, telephone number, and Job title) before creating new accounts and passwords. Furthermore, these details must be entered into the appropriate fields within the applicable user object or directory service. Personal ID numbers (such as national identification numbers) shall be changed with permissions configured to allow only administrators access.

- Users must use only their own user ID (s) and password(s) to access technical resources unless it is technically not feasible to do so.

- Users will be held accountable and liable for all actions performed using their assigned user ID (s) and password(s).

- Technical resources must be configured (where this is possible) to lock the user ID and prevent user access to the technical resource when an incorrect user password has been entered a specific number of times within a specific period.

- Privileged user accounts, such as administrators, super users, root, and system development, shall only be used for operations that require such elevated privileges and shall be logged off at all other times.

- All users must register in the UOB self-reset password portal to manage their passwords anytime.

3.2 Password Confidentiality

- User passwords shall always remain confidential and shall not be shared, posted, or otherwise divulged in any manner.

- Without prejudice to Above, if a password must be divulged for technical or security reasons, it must be shared either in person or by phone using already-established phone numbers, and the concerned section's management must be notified of such action.

- Passwords must be entered in non-display fields (i.e. hidden by asterisks or similar graphical representation).

3.3 Password Composition & Expiry

3.3.1 Domain & Application User Password Requirements:

- Minimum length – eight (8) characters.
- Passwords must contain at least one special character, numerical character, and letter.
- Password must be changed after a maximum period of 170 days.
- The user account must be locked out after a maximum of five (5) invalid login attempts within a maximum timeframe of one hour and automatically unlocked after a minimum of one (1) hour from the lockout.
- Any temporarily assigned passwords must be changed at the first log-on.
- The same password may not be repeated within a cycle of four (4) password changes, and the password age must be at least one (1) day.

3.3.2 Administrator, Privileged, Super User, Root, or Developer User Passwords

- Minimum length - 14 characters.
- Passwords must contain at least one special character and one numerical character.

- Password must be changed after 90 days.
- Accounts must not be locked out regardless of the number of invalid attempts.
- The same password must not be repeated within a cycle of three (3) password changes.
- Any temporarily assigned passwords must be changed at the first log-on.
- The password must be recorded on paper, sealed in an envelope, and kept in the department's fireproof safe.
- Whenever employment is terminated (for any reason) for an employee with knowledge of such passwords, the affected passwords must be changed immediately.

3.3.3 Service Accounts

All passwords of service accounts shall follow the same level of controls as applicable to the administrator, super user, root, or developer passwords as indicated in 3.3.2 Above.

3.4 Password Reset

- When a password reset is required, users are encouraged to self-reset it through the UOB self-reset password portal.
- When the user forgets the password and cannot access the self-reset password portal, the user should visit the IT Center in person and present a valid Identity document.

3.5 Authentication

The user ID and password must be authenticated. Authentication failure must provide an error message to the user that does not indicate which element of the login credentials is incorrect (e.g., "incorrect login" and not "incorrect password" or "username does not exist").

3.6 Inactivity Lock

System administrators and/or owners shall carry out the necessary configuration to cause user devices (computers, laptops) to lock after a period of inactivity not longer than twenty (20) minutes.

3.7 Disabling Default Passwords

The vendor-supplied user IDs/passwords, encryption keys, and other access codes included with vendor-supplied systems must be changed before the respective system is introduced to a production environment or disabled if applicable. Default passwords shipped with software shall be disabled or changed before live use of the software.

3.8 Prohibition of Group Passwords

- Group passwords will not be allowed to the maximum extent possible to maintain individual accountability. Where such passwords are used because of specific business requirements or technical limitations, they must be maintained solely within the group members, with clearly defined ownership of the group.

- This prohibition applies both to normal and super user accounts.

3.9 Password Selection Rules

3.9.1 Users are encouraged to create passwords that are not easy to guess yet easy to remember by the respective user.

3.9.2 Passwords should not be based on any of the following:

- Months of the year, days of the week, or any other aspect of the date (like date of birth, date of joining, anniversary, etc.);
- Family names or initials.
- Vehicle registration numbers.
- Employee No. / Employee ID or designations.

- Project or department name or references.
- Company names, identifiers, or references.
- Telephone numbers or similar all-numeric groups.
- User ID, username, group ID or other system identifier.
- More than two consecutive identical characters.
- All-numeric or all-alphabetic groups; or
- Any standard dictionary word (without incorporating special characters, mixed case, and other elements).

3.10 Exceptions

- Exceptions to this policy shall be made only when there is strong justification for preventing its application. Such exceptions shall be made only for a limited timeframe and for specific usernames and/or technical resources.
- Exceptions to this policy shall be authorized by the IT center director.
- The IT center shall review any exception granted on an annual basis, and if the justification for the exception no longer applies, it shall be immediately revoked.

3.11 Enforcement

- Violation of this policy is recognized to have potential damage ranging from minor inconvenience to catastrophic failure of national systems and/or leaking of top-secret information.
- Identified violations of this policy shall result in immediate corrective action by management, as well as possible disciplinary action. Disciplinary action will be consistent with the severity of the incident and the surrounding circumstances as determined by an investigation and may include, but may not be limited to:
    - Loss of access privileges to technical resources.
    - Disciplinary actions pursuant to the Civil Service law and executive regulation, up to and including termination of service.

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