جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

Password Management policy

Version: 2.0

CODE: DICT.I.06-15.CS.E.V2.0

1 Table of Contents

2 Intellectual Property Information

This document is the intellectual property of the Deanship of Information and Communication Technology (DICT) at Imam Abdulrahman bin Faisal University (IAU). The content of this document is intended solely for authorized recipients. Any distribution, disclosure, publication, or copying of this document without written permission from DICT is strictly prohibited.

3 Document Control

3.1 Information

Title	Classification	Version	Status
PASSWORD MANAGEMENT POLICY	RESTRICTED	V2.0	ACTIVE

3.2 Revision History

Version	Author(s)	Issue Date	Changes
V1.0	DR. BASHAR ALDEEB	26/04/2021	CREATION
V1.1	DR. SAMER BANI AWWAD	24/05/2022	REVIEW AND UPDATE
V2.0	BAHA NAWAFLEH	14/12/2023	REVIEW AND UPDATE

3.3 Document Review

Date of Next Scheduled Review
01/01/2025

3.4 Distribution List

#	Recipients
1	ALL DICT DEPARTMENTS
2	LEGAL AFFAIRS
3	IAU WEBSITE
4	

3.5 Approval

Name	Position Title	Decision Number	Date
DR. NIHAD AL-OMAIR	VICE PRESIDENT OF DEVELOPMENT AND COMMUNITY PARTNERSHIP	61945	06/03/2024

4 Introduction

Protecting information and technology assets is essential for the success of the IAU. To achieve this goal, the IAU has established Cybersecurity Management to develop, establish, and organize the necessary processes to safeguard information and technology assets. This document defines the Password Management policy within the IAU in accordance with relevant regulatory, legislative, organizational policies, and procedures.

This policy is integrated within the framework of the IAU's policies and falls under the authority granted by the entity responsible from the date of its adoption.

5 Policy Objectives

This policy defines the standards and procedures necessary for providing security controls for passwords and their management.

6 Applicability and Scope

The provisions of this policy apply to all affiliates or individuals engaged in work within the IAU, whether through permanent or temporary contracts, directly or indirectly. This also includes external suppliers, contractors, and anyone who has permanent or temporary access rights to the IAU's data, regardless of its source, format, or nature, and to the systems, devices, and databases of the IAU.

7 Policy

7.1 General Policy Requirements

7.1.1 Regular account passwords must contain a minimum of eight (8) characters, while important and sensitive accounts (such as system administrator accounts) must have a minimum of twelve (12) characters.

7.1.2 Passwords must be case-sensitive and include both lowercase and uppercase characters.

7.1.3 Each password must include at least one special character.

7.1.4 Systems should be designed to enforce users to change the initial temporary password for new accounts upon their first login and retain a history of the last five passwords for an account to prevent password reuse.

7.1.5 Users should be notified before their password expires, reminding them to change their password before expiration.

7.1.6 Passwords must not be displayed on the screen as they are entered. Additionally, the password verification file stored within the application system must be encrypted.

7.1.7 Users are responsible for safeguarding their passwords, and each individual is accountable for activities performed through their respective user identity.

7.1.8 Users are not allowed to perform the following actions:

- Using the same method to send passwords to open files or links that require a password, through various communication methods such as email, instant messaging, text messages, etc.
- Sharing passwords with other affiliates.
- Disclosing passwords to anyone.
- Writing passwords on paper.
- Storing passwords in unprotected files.
- Storing passwords as plain text.
- Using the "Hint" feature to remember passwords.
- Enabling automatic password saving.
- Using the "Remember Password" feature in applications/systems.

7.1.9 Passwords should not include the "username."

7.1.10 First name, middle name, or last name of the user should not be used in passwords.

7.1.11 When using the Simple Network Management Protocol (SNMP), community strings should be configured differently from standard default settings like "public," "private," and "system." These strings should also be distinct from interactive login passwords. Additionally, key fragmentation should be used if available (for example, SNMP v3).

7.1.12 Secure methods and algorithms should be used for storing and processing passwords, such as Hashing Functions.

7.1.13 Passwords must not contain any information related to the IAU or its geographic location.

7.1.14 All default passwords for accounts with significant privileges, such as root or administrator accounts, should be changed as soon as the system becomes operational.

7.1.15 Accounts with critical and sensitive privileges should be assigned to a single administrator responsible for the password.

7.1.16 If there is suspicion that a password has been compromised, the user must immediately change the password and inform the Cybersecurity Management about the incident.

8 Roles and Responsibilities

The Cybersecurity Management responsibilities:

8.1.1 Cybersecurity Management shall ensure that the policy is approved by the authorized party and work on its implementation.

8.1.2 Cybersecurity Management shall approve the standards, procedures, and guidelines to ensure necessary compliance with the security requirements of the IAU's operations.

8.1.3 Cybersecurity Management shall ensure alignment between this policy and the IAU's activities.

8.1.4 The Cybersecurity Management shall resolve any conflicts arising from this policy.

8.1.5 Cybersecurity Management shall provide the necessary resources for identifying, purchasing, and implementing technological solutions to fulfil the policy's requirements wherever possible.

8.1.6 Cybersecurity Management is responsible for disseminating the Cybersecurity policy to all authorized departments, affiliates, and users of the IAU who have or will be granted access to technological and informational assets.

8.1.7 Cybersecurity Management shall coordinate with relevant departments to monitor compliance and implementation.

8.1.8 The Cybersecurity Management shall regularly review the policy according to the established timeline.

The Deanship of Information and Communication Technology shall:

8.1.9 Commit to this policy, implement the controls mentioned in this policy, and report any security incidents to the Cybersecurity Management.

8.1.10 Secure and enable password security settings for all information technology systems within the IAU.

8.1.11 Review incorrect login attempts and administrative authorization logs daily.

Top Management, Heads of Departments, Heads of Units, and Advisers shall:

8.1.12 Ensure the sharing of this policy with all affiliates within the IAU.

8.1.13 Report any violations or non-compliance with this policy to the Cybersecurity Management.

8.1.14 Ensure that all affiliates within the IAU shall adhere to the provisions of this policy and report any security incidents or non-compliance with the provisions of this policy to the Head of Cybersecurity Management.

9 Policy Ownership

The person responsible for this policy is the Head of Cybersecurity Management within the IAU.

10 Policy Changes

The policy should be reviewed at least annually or whenever there are changes in legislative and regulatory requirements. Any changes should be documented and approved by the authorized entity within the IAU.

11 Compliance

All affiliates within the IAU and external parties (vendors/contractors) must adhere to the provisions of this policy. The Head of Cybersecurity Management within the IAU must ensure continuous monitoring of compliance and submit necessary reports to the authorized entity periodically.

Necessary actions must be taken to ensure compliance with the provisions of this policy. This is to be achieved through periodic reviews by the Cybersecurity Management or relevant departments. Corrective actions should be taken by the authorized entity within the IAU, in accordance with recommendations provided by the Head of Cybersecurity Management, in case of any violations of this policy. Disciplinary measures, proportionate to the severity of the incident and the investigation findings, should be implemented. These disciplinary measures may include, but are not limited to:

- Revoking access privileges to data, IT assets, and systems connected to the IAU.
- Issuing written warnings or termination of employment, as deemed appropriate by the IAU.

Non-compliance with any provisions of this policy requires prior authorization from the Cybersecurity Management to take appropriate actions. These actions should align with the policies and regulations of the IAU, as well as contractual terms with any individuals or entities engaged with the IAU.

12 Related Policies

- DICT.I.06-01.CS.E.V2.0 - General Cybersecurity Policy
- DICT.I.06-02.CS.E.V2.0 - Cybersecurity Compliance Policy.
- DICT.I.06-29.CS.E.V2.0 - Encryption Policy
- DICT.I.06-09.CS.E.V2.0 - Cybersecurity Incident Management Policy
- DICT.I.06-26.CS.E.V2.0 - Clear Desk and Clear Screen Policy
- DICT.I.06-33.CS.E.V2.0 - Access Control Policy

13 References

Department Name	The National Institute of Standards and Technology (NIST)	ISO 27001:2013	Cybersecurity Controls for Cloud Computing	Cybersecurity Controls for Social Media Accounts for Entities	Cybersecurity Controls for Remote Work	Cybersecurity Controls for Sensitive Systems	Basic Cybersecurity Controls
Using Confidential Authentication Information	IA-5(1), IA-5(4), IA-2	A.9.3.1	-	-	-	5-1-2-2	1-3-2-2 ,1-2-2
Password Management System	IA-6	A.9.4.3	-	-	-	5-1-2-2	1-3-2-2

----------End of Documentation----------