جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

Access Control Policy

Version: 2.0

CODE: DICT.I.06-33.CS.E.V2.0

1 Table of Contents

1 Table of Contents 2
1 Intellectual Property Information 3
2 Document Control 4
2.1 Information 4
2.2 Revision History 4
2.3 Document Review 4
2.4 Distribution List 4
2.5 Approval 4
3 Introduction 5
4 Objective of the Policy 5
5 Applicability and Scope 5
6 Policy 5
6.1 General Policy Requirements 5
6.2 Access and Authorization Management 6
6.3 Access to Networks and Services 8
6.4 Remote Access to University Networks 9
6.5 Cancellation and Modification of Access Rights 10
6.6 Review of Login Identities and Permissions 10
6.7 Access Control for Cloud Computing Services 11
6.8 Access Control for Social Media Accounts 11
6.9 Access Control to Source Code 12
6.10User Authentication Information Management 13
6.11Access Restriction to Information 13
6.12Secure Login Procedures 13
6.13Password Management System 14
7 Cybersecurity Management Roles and Responsibilities 14
8 Policy Ownership 15
9 Policy Changes 15
10 Compliance 15
11 Related Policies, Standards and Procedures 16
12 References 17

1 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.

2 Document Control

2.1 Information

Title	Classification	Version	Status
Access Control Policy	Restricted	V2.0	Active

2.2 Revision History

Version	Author(s)	Issue Date	Changes
V1.0	Dr. Bashar AlDeeb	02/01/2021	Creation
V1.1	Dr. Samer Bani Awwad	02/03/2022	Review and Update
V2.0	Baha Nawafleh	22/12/2023	Review and Update

2.3 Document Review

Date of Next Scheduled Review
01/01/2025

2.4 Distribution List

#	Recipients
1	All DICT Departments
2	Legal Affairs
3	IAU Website
4	

2.5 Approval

Name	Position Title	Decision Number	Date
Dr. Nihad Al-Omair	Vice President of Development and Community Partnership	61945	06/03/2024

3 Introduction

Protecting information, IT assets, and technological resources is essential for the success of the IAU. To achieve this goal, Cybersecurity Management develops, establishes, and organizes necessary security operations to safeguard information and technology assets. This document defines the remote work policy within the university, in accordance with relevant IAU policies, regulatory procedures, and legal requirements.

This policy falls under the framework of the university's policies and operates under the authority granted by the authorized party from the date of its adoption.

4 Objective of the Policy

The access control policy for the IAU aims to manage and restrict logical and physical access for affiliates and information technology assets to the university's buildings, systems, and data networks.

5 Applicability and Scope

The provisions of this policy apply to all affiliates or appointees working within the university, whether on permanent or temporary contracts, whether directly or indirectly, including suppliers, external contractors, and anyone with permanent or temporary access rights to the university data, regardless of its source, form, or nature, as well as to the university's systems, devices, and databases.

6 Policy

6.1 General Policy Requirements

6.1.1 Identity Verification and Authorization: Documents related to the IAU must be verified, and their validity must be confirmed before granting logical or physical access rights to the university resources.

6.1.2 User Identity and Access Permissions: User identity and access permissions shall be determined in accordance with relevant IAU policies, regulatory procedures, and legal requirements.

6.1.3 Access to Data and Information: Access to data and information within the entity, whether accessed by affiliates or external parties, must align with the university's policies.

6.2 Access and Authorization Management

6.2.1 Authorization Management:

- An authenticated and documented process for access management must be established. This process outlines the mechanism for granting, modifying, and revoking access permissions to information and technology assets within the university. The process should be monitored and ensured for its implementation.
- User identities (User Identities) must be created in accordance with the university-specific legislative and regulatory requirements.
- User identity verification (Authentication) and validation must occur before granting users access to information and technology assets.
- A documented and approved matrix for user permissions and authorizations (Authorization) should be established, based on the principles of access control, including:
    - Need-to-Know and Need-to-Use principles.
    - Segregation of Duties principle.
    - Least Privilege principle.
- Access controls and permissions must be enforced on all technological and information assets within the university using a central access control system, such as the Lightweight Directory Access Protocol (LDAP).
- Shared accounts (Generic User) should not be used to access the university-specific information and technology assets.
- Systems should be configured to automatically log out after a specified period (Session Timeout).
- Unused user accounts should be disabled within a defined time period (recommended not to exceed 90 days).
- Settings for all identity and access management systems should be configured to send logs to a central logging and monitoring system according to the records management and cybersecurity monitoring policy.
- Users should not be granted direct access to or interaction with database systems for sensitive systems; access should be through applications only, with the exception of Database Administrators.

- Application managers and cybersecurity management must ensure separation of duties and least privilege principles when granting access privileges to the university users.
- Clear procedures for managing service accounts should be documented and approved, ensuring secure management between applications and systems. Interactive login through service accounts should be disabled.
- Multi-Factor Authentication (MFA) must be required for accessing:
  - All university information and network assets remotely.
  - Webmail for accessing the university email services.
  - All external web applications.
  - User accounts with critical and sensitive privileges on technology and information assets.
  - Access to sensitive systems and systems used for managing those sensitive systems and monitoring them for all users.
  - All cloud accounts for users with critical and sensitive privileges.
  - Social media login operations.
- When using Multi-Factor Authentication (MFA), it should employ at least two of the following methods:
  - Knowledge (something the user knows, like a password).
  - Possession (something the user has, like a software or hardware token for generating one-time passwords, also known as "One-Time Password").
  - Inherence (something the user is, like a biometric trait such as fingerprint).

6.2.2 Granting Access:

- User Access Requirements:
- Access to data networks or information is based on work and security requirements. Access control and access rules should be determined for each system, considering:
  - Security requirements for business applications.
  - Specific user work requirements for information access or operation ("Need-to-Know" principle).

- ○ All access attempts should be denied unless approved under the terms of this policy.
- ○ Legal and/or contractual commitments to restrict and protect access to information systems.
- ○ All types of access to information systems, except basic requests agreed upon with DICT, should be formally approved by cybersecurity management.

- External parties should not be granted access to the university resources and operational information assets without signing a confidentiality agreement approved by the university.
- Access rights are granted based on user requests through an approved form or system, specifying the system name, type of request, and permission. Approval is obtained from the direct manager and the System Owner based on the user's matrix of permissions and authorizations.
- Users should be granted access to the university-specific information and technology assets in alignment with their roles and responsibilities.
- A unified procedure should be followed to create user identities, allowing tracking of activities performed using a "User ID" and linking it to the user, such as writing <first initial>.<last name>, or the pre-defined affiliate ID assigned by the General Human Resources Management.
- Disabling concurrent logins from multiple computing devices at the same time.
- Access requirements for critical and sensitive accounts, in addition to the controls mentioned in the User Access Requirements section, must adhere to the controls listed below for all accounts with critical and sensitive privileges:
- Individual access rights should be assigned to users requesting critical and sensitive privileges (Administrator Privilege) based on their job responsibilities, considering the principle of segregation of duties.
- Enabling password history tracking to monitor the number of password changes.
- Changing default account names, especially accounts with significant and sensitive privileges such as "Root" and "Admin" accounts.
- Preventing the use of accounts with critical and sensitive privileges in daily operational tasks.

6.3 Access to Networks and Services

6.3.1 Cybersecurity management must ensure that access to networks and services is controlled based on work and security requirements, with specific access control rules for each network. These rules should consider:

- Network security requirements or network service requirements.
- Specific user work requirements to access the network or network service ("Need" principle).
- Legal and/or contractual commitments to restrict or protect access to assets.

6.3.2 Information Technology Management should ensure the following:

- Logical access to network devices and software should be limited to system administrators within the university.
- Access to programmable network devices such as Routers, Switches, and Firewalls should be restricted to network administrators within the university.
- The use of network diagnostic and security tools should be limited to network administrators only, in line with their job responsibilities.
- Access to all network settings and security-related data (such as dial-up numbers and IP addresses) should be restricted to the team responsible for cybersecurity management and DICT.

6.4 Remote Access to University Networks

6.4.1 Remote access to information and technical assets should be granted after obtaining prior authorization from the Cybersecurity Management and restricted using Multi-Factor Authentication (MFA).

6.4.2 Records of remote login sessions must be stored and monitored, considering the sensitivity of information and technology assets.

6.4.3 Remote access from outside the country to sensitive systems is generally prohibited, except in exceptional cases with official approval from the Cybersecurity Management.

6.4.4 Remote access should be provided based on a need-to-know basis and for official purposes only.

6.4.5 Any remote access should utilize necessary encryption methods (such as Secure Transport Protocol, Secure Port Layer Protocol, and Virtual Private Network) to secure network communication.

6.4.6 Users with remote access should ensure that their computers or workstations, owned by the university or themselves, are:

- Not connected to any other network simultaneously.
- Equipped with up-to-date antivirus, anti-spyware programs, and personal firewall.

6.4.7 Information Technology Management controls all remote access operations through a limited number of managed access points.

6.4.8 All remote access requests must be approved by Cybersecurity Management, Information Technology Management, and system owners.

6.4.9 Remote access users are responsible for the consequences if remote access is misused.

6.4.10 Information Technology Management must ensure the logging of all remote access activities, including IP addresses and login identifiers.

6.4.11 Remote access account activity should be monitored by Information Technology Management.

6.4.12 Remote access to the university's information systems by external parties should only be provided when there is a strong justification. If remote access to external parties is granted to the university's information systems/networks, the following should be observed:

- Their access should be limited to specific information systems/networks required for their assigned tasks.
- Network and monitoring administrators should oversee their access and activities.

6.5 Cancellation and Modification of Access Rights

6.5.1 General Human Resources Management should notify DICT when a user transitions, changes roles, or terminates/ends their employment with the university. DICT should then suspend or modify the user's access rights based on their new job responsibilities.

6.5.2 If a user's access rights are suspended, event records related to the user should not be deleted but preserved in accordance with the cybersecurity event log management policy.

6.6 Review of Login Identities and Permissions

6.6.1 The cybersecurity management, in collaboration with application managers, conducts periodic reviews of login identities (User IDs) and verifies access permissions to information and technical assets based on user job responsibilities, following the principles of access control and permissions. Login identities on sensitive systems are reviewed at least once every three months.

6.6.2 Periodic reviews of user permissions (User Profiles) for information and technical assets are conducted according to access control and permissions principles. Permissions for sensitive systems are reviewed at least once a year.

6.6.3 Login identities and permissions used for remote work must be reviewed at least once a year.

6.6.4 Upon identifying any misuse of privileged access rights, application managers must restrict these privileges and inform the relevant system administrator to take further action.

6.6.5 Official records must be maintained and updated for all registered users in the permissions matrix for each system/application.

6.7 Access Control for Cloud Computing Services

6.7.1 Access identities and permissions for all accounts with access to cloud services must be managed throughout their lifecycle.

6.7.2 Confidentiality of user identities, accounts, and permissions must be ensured, including requesting users to maintain their privacy.

6.7.3 Secure session management must be practiced, including session authenticity, lockout mechanisms, and session timeout.

6.7.4 Measures to detect and prevent unauthorized access attempts should be implemented, such as setting limits on unsuccessful login attempts.

6.8 Access Control for Social Media Accounts

6.8.1 Dedicated social media accounts for the university should be used, not individual accounts.

6.8.2 Registration must be done using official information (official email dedicated for social media platforms and official mobile number), and personal information should not be used.

6.8.3 Social media accounts must be authenticated and maintain consistent identity across all used accounts. This facilitates recognizing official accounts and detecting fraudulent accounts.

6.8.4 A secure and unique password must be used for each social media account. Passwords should be changed periodically, and reusing previously used passwords is prohibited.

6.8.5 Security questions must be activated, updated, and securely documented.

6.8.6 User account permissions for social media accounts should be managed based on operational needs, considering the sensitivity of the accounts, level of permissions, and the type of devices and systems being used.

6.8.7 Permissions of service providers managing social media accounts or automated monitoring of these accounts must be restricted to prevent impersonation or identity protection.

6.8.8 Access to the university's social media accounts should be limited to specific devices.

6.8.9 Review of login credentials and permissions used for the university's social media accounts should be conducted at least once a year.

6.9 Access Control to Source Code

6.9.1 Application managers must ensure that all source codes are centrally compiled and governed in a software library.

6.9.2 Application managers should avoid unnecessary disclosure of system configuration information that could be useful to attackers by:

- Preventing the server field in Hypertext Transfer Protocol (HTTP) headers from revealing the web server's brand and version.
- Ensuring that directory listings of files on the web server are not indexed, as this could expose files not intended to be public.
- Ensuring that the source code of executable programs and scripts cannot be displayed by the server through a web browser.

6.9.3 For web applications, application managers and cybersecurity management should review the source code of client-side scripting languages, such as HTML and JavaScript, to ensure they do not contain unnecessary information, such as:

- Developer names (which can be used in social engineering).
- Disabled features.
- Details about permissions and standards.
- Third-party tools in use, which may have known vulnerabilities.

6.9.4 Reviewing error messages returned by the web application to ensure they do not disclose unwanted information.

6.9.5 Cybersecurity management and application managers must ensure that IT administrators do not have access to the program source code or the ability to modify program behaviour by changing their configuration parameters.

6.9.6 Accurate and up-to-date records of software source code libraries must be maintained.

6.10 User Authentication Information Management

6.10.1 Application managers must ensure:

- Identity and authentication are verified through passwords before allowing users to access all information systems within the university.
- Review and revoke permissions for personnel immediately upon the termination of their professional service with the entity.
- For all transfer cases, a review of all current access privileges for the user is conducted according to approved job requirements. Based on the review, access privileges are modified or revoked accordingly.

6.11 Access Restriction to Information

6.11.1 Application managers must ensure the following:

- Critical and sensitive applications that handle sensitive data operate on a dedicated operating system.
- Restrict user and support staff access to sensitive system information and application system functions.
- Physical and/or logical isolation of sensitive systems is practiced.

6.11.2 Except for Database Administrators, direct access or interaction with databases by any user is prohibited. This should be carried out solely through applications, based on authorized permissions. This includes implementing security solutions that limit or prevent Database Administrators from accessing classified data.

6.12 Secure Login Procedures

6.12.1 The system should define the allowed number of unsuccessful login attempts, including:

- Logging both successful and unsuccessful login attempts.
- Introducing a time delay before allowing further login attempts or outright denying any additional attempts without specific authorization.
- Application managers should periodically review all unsuccessful login attempts.
- Configuring alerts on the Security Information and Event Management (SIEM) system to notify the security operations team of any suspicious activities or incidents.

6.13 Password Management System

6.13.1 System administrators (application, database, operating systems, networks, etc.) must ensure the secure storage (encryption) of user names and passwords for information systems, as well as their handling and distribution.

6.13.2 System administrators (application, database, operating systems, networks, etc.) are responsible for changing all default system user names and passwords as soon as these systems are obtained.

6.13.3 Users must immediately change passwords if there is any suspicion of password compromise, and this must be promptly reported to the DICT and cybersecurity management.

7 Cybersecurity Management Roles and Responsibilities

Cybersecurity management shall:

7.1.1 Adopt the policy from the authorized entity and work on its implementation.

7.1.2 Adopt the standards, procedures, and guidelines to ensure necessary compliance with the security requirements of the university's operations.

7.1.3 Ensure alignment between this policy and the university's activities.

7.1.4 Resolve any conflicts arising from this policy.

7.1.5 Provide the necessary resources for identifying, purchasing, and implementing technical solutions to fulfil the accepted policy requirements for asset utilization whenever possible.

7.1.6 Disseminate the cybersecurity compliance policy and data governance to all departments, affiliates, and authorized users of the university, or those who will be granted access to the technical and information assets.

7.1.7 Coordinate with relevant departments for monitoring compliance and execution.

7.1.8 Regularly review the policy according to the defined timeline.

The Deanship of Information and Communication Technology shall:

7.1.9 Adhere to this policy, implement the controls specified in this policy, and report any security incidents to the General Management of Cybersecurity Management.

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

7.1.10 Ensure the dissemination of this policy to all affiliates within the university or department.

7.1.11 Report any breaches or non-compliance with this policy to the Cybersecurity Management.

7.1.12 Ensure that all personnel within the university must adhere to the provisions of this policy and report any security incidents or non-compliance with any provisions outlined in this policy to the Head of Cybersecurity Management.

8 Policy Ownership

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

9 Policy Changes

The policy must be reviewed at least annually or when there are changes in legislative and regulatory requirements. Changes should be documented and approved by the authorized party within the university.

10 Compliance

All personnel within the university and external/contracted parties must comply with the provisions of this policy. The Head of Cybersecurity Management in the university must ensure continuous monitoring of compliance and submit necessary reports to the authorized party regularly.

All rights reserved for Deanship of ICT ©

جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Necessary measures must be taken to ensure compliance with the provisions of this policy. This includes periodic review by the Cybersecurity Management or relevant departments, and corrective actions should be taken by the authorized party within the university based on recommendations provided by the Head of Cybersecurity Management regarding any violations of this policy. Disciplinary actions, proportional to the severity of the incident as determined by the investigation, may include, but are not limited to:

- Revoking access rights to data, IT assets, and university systems.
- Issuing a written warning or terminating the employment of the individual, as deemed appropriate by the university.

Non-compliance with any provisions of this policy, without obtaining prior exemption from the Cybersecurity Management, may result in appropriate actions in accordance with the university's policies and regulations, or as suitable based on contractual terms with individuals or entities contracted with.

11 Related Policies, Standards and Procedures

- DICT.I.06-01.CS.E. V2.0 - General Cybersecurity policy
- DICT.I.06-02.CS.E. V2.0 - Cybersecurity Compliance Policy
- DICT.I.06-21.CS.E. V2.0 - Data Classification Policy
- DICT.I.06-39.CS.E. V2.0 - Network Security Policy
- DICT.I.06-10.CS.E. V2.0 - Cybersecurity Event Log and Monitoring Management Policy
- DICT.I.06-22.CS.E. V2.0 - System Acquisition, Development, and Maintenance Policy
- DICT.I.06-15.CS.E. V2.0 - Password Management policy
- DICT.I.06-14.CS.E. V2.0 - Web Application Security Policy
- DICT.I.06-49.CS.E.V2.0 Identity And Access Management Standards
- DICT.I.06-60.CS.E.V2.0 Asset Classification Standards
- DICT.I.06-69.CS.E.V2.0 Password Management standards
- DICT.I.06-68.CS.E.V2.0 Cybersecurity Events Logs and Monitoring Management standards
- DICT.I.04-36.CS.E.V2.0 System Acquisition, Development and Maintenance Procedures

12 References

Department Name	National Institute of Standards and Technology (NIST)	ISO 27001:2013	Cybersecurity Controls for Cloud Computing	Cybersecurity Controls for Social Media Accounts of Entities	Cybersecurity Controls for Remote Work	Cybersecurity Controls for Sensitive Systems	Core Cybersecurity Controls
Access Control to Operational Systems	AC-2, AC-7, AC-8, AC-9, IA-2, IA-5, IA-6, IA-8	A.11.5.1, A.11.5.2, A.11.5.3	١- ش-٢ -٢	1-2-2 2-2-2	1-2-2	1-2-2 2-2-2	3-2-2
Use of Confidential Authentication Information	IA-5(1), IA-5(4), IA-2	A.9.3.1	١- ش-٢ -٢	1-2-2 2-2-2	1-2-2	1-2-2 2-2-2	3-2-2
Network Access	AC-1, AC-6, AC-17, AC-18, AC-20, CM-7, SC-1, SC-7	A.11.4.1	١- ش-٢ -٢	1-2-2 2-2-2	2-2-2	1-2-2 2-2-2	3-2-2

-- End of Document --