INSPIRING BUSINESS INNOVATION

ACCESS CONTROL POLICY

Version 1.1

Policy Number:

1. Table of Contents

1. Table of Contents 2
2. Property Information 3
3. Document Control 4
3.1. Information 4
3.2. Revision History 4
3.3. Review, Verification and Approval 4
3.4. Distribution List 4
4. Policy Overview 5
4.1. Purpose 5
4.2. Scope 5
4.3. Terms and Definitions 5
4.4. Change, Review and Update 7
4.5. Enforcement / Compliance 7
4.6. Waiver 7
4.7. Roles and Responsibilities (RACI Matrix) 8
4.8. Relevant Documents 8
4.9. Ownership 9
5. Policy Statements 10
5.1. Access Control Policy 10
5.2. Access to Networks and Network Services 11
5.3. User Registration and De-Registration 13
5.4. User Access Provisioning 14
5.5. Management of Privileged Access Rights 15
5.6. Management of Secret Authentication Information of Users 15
5.7. Review of User Access Rights 16
5.8. Removal or Adjustment of Access Rights 17
5.9. Use of Secret Authentication Information 17
5.10. Information Access Restriction 18
5.11. Secure Log-On Procedures 19
5.12. Password Management System 19
5.13. Use of Privileged Utility Programs 20
5.14. Access Control to Program Source Code 20

2. Property Information

This document is the property information of Imam Abdulrahman bin Faisal University - ICT Deanship. The content of this document is **Confidential** and intended only for the valid recipients. This document is not to be distributed, disclosed, published or copied without ICT Deanship written permission.

3. Document Control

3.1. Information

Title	Classification	Version	Status
ACCESS CONTROL POLICY	Confidential	1.0	validated

3.2. Revision History

Version	Author(s)	Issue Date	Changes
0.1	Alaa Alaiwah - Devoteam	November 17, 2014	Creation
0.2	Nabeel Albahbooh - Devoteam	November 27, 2014	Update
0.3	Osama Al Omari – Devoteam	December 23, 2014	QA
1.0	Nabeel Albahbooh – Devoteam	December 31, 2014	Update
1.1	Muneeb Ahmad – ICT, IAU	21 April 2017	Update

3.3. Review, Verification and Approval

Name	Title	Date
Lamia Abdullah Aljafari	Quality Director	
Dr. Saad Al-Amri	Dean of ICT	

3.4. Distribution List

Copy #	Recipients	Location

4. Policy Overview

This section describes and details the purpose, scope, terms and definitions, change, review and update, enforcement / compliance, wavier, roles and responsibilities, relevant documents and ownership.

4.1. Purpose

The main purpose of **Access Control Policy** is to:

Limit access to information and information processing facilities, ensure authorized user access and to prevent unauthorized access to systems and services, make users accountable for safeguarding their authentication information, and prevent unauthorized access to systems and applications.

4.2. Scope

The policy statements written in this document are applicable to all IAU's resources at all levels of sensitivity; including:

- All full-time, part-time and temporary staff employed by, or working for or on behalf of IAU.
- Students studying at IAU.
- Contractors and consultants working for or on behalf of IAU.
- All other individuals and groups who have been granted access to IAU's ICT systems and information.

This policy covers all information assets defined in the *Risk Assessment Scope Document* and will be used as a foundation for information security management.

4.3. Terms and Definitions

Table 1 provides definitions of the common terms used in this document.

Term	Definition
Accountability	A security principle indicating that individuals shall be able to be identified and to be held responsible for their actions.

Asset	Information that has value to the organization such as forms, media, networks, hardware, software and information system.
Availability	The state of an asset or a service of being accessible and usable upon demand by an authorized entity.
Confidentiality	An asset or a service is not made available or disclosed to unauthorized individuals, entities or processes.
Control	A means of managing risk, including policies, procedures, and guidelines which can be of administrative, technical, management or legal nature.
Guideline	A description that clarifies what shall be done and how, to achieve the objectives set out in policies.
Need to Know	A user is only granted access to the information he needs to perform his tasks (different tasks/roles mean different need-to-know and hence different access profiles).
Need to Use	A user is only granted access to IT facilities (e.g., equipment, applications, procedures and rooms) he needs to perform hi task/job/role.
Information Security	The preservation of confidentiality, integrity, and availability of information. Additionally, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.
Integrity	Maintaining and assuring the accuracy and consistency of asset over its entire life-cycle.
Owner	A person or group of people who have been identified by Management as having responsibility for the maintenance of the confidentiality, availability and integrity of an asset. The Owner may change during the lifecycle of the asset.
Policy	A plan of action to guide decisions and actions. The policy process includes the identification of different alternatives such as programs or spending priorities, and choosing among them on the basis of the impact they will have.
Provisioning	A process of assigning or revoking access rights for users to information, systems and services.
Risk	A combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
System	An equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, control, display, switching, interchange, transmission or reception of data

	and that includes computer software, firmware and hardware.

Table 1: Terms and Definitions

4.4. Change, Review and Update

This policy shall be reviewed **once every year** unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes of this policy shall be exclusively performed by the Information Security Officer and approved by Management. A change log shall be kept current and be updated as soon as any change has been made.

4.5. Enforcement / Compliance

Compliance with this policy is **mandatory** and it is to be reviewed periodically by the Information Security Officer. All IAU units (Deanship, Department, College, Section and Center) shall ensure continuous compliance monitoring within their area.

In case of ignoring or infringing the information security directives, IAU's environment could be harmed (e.g., loss of trust and reputation, operational disruptions or legal violations), and the fallible persons will be made responsible resulting in disciplinary or corrective actions (e.g., dismissal) and could face legal investigations.

A correct and fair treatment of employees who are under suspicion of violating security directives (e.g., disciplinary action) has to be ensured. For the treatment of policy violations, Management and Human Resources Department have to be informed and deal with the handling of policy violations.

4.6. Waiver

Information security shall consider exceptions on an individual basis. For an exception to be approved, a business case outlining the logic behind the request shall accompany the request. Exceptions to the policy compliance requirement shall be authorized by the Information Security Officer and approved by the ICT Deanship. Each waiver request shall include justification and benefits attributed to the waiver.

The policy waiver period has maximum period of 4 months, and shall be reassessed and re-approved, if necessary for maximum three consecutive terms. No policy shall be provided waiver for more than three consecutive terms.

4.7. Roles and Responsibilities (RACI Matrix)

Table 22 shows the RACI matrix[1] that identifies who is responsible, accountable, consulted or informed for every task that needs to be performed. There are a couple of roles involved in this policy respectively: ICT Deanship, Information Security Officer (ISO), Human Resources Department / Administrative Unit (HR/A), Owner and User (Employees, Faculty Members, Students, Contractors, Consultants and Third Parties).

Roles / Responsibilities	ICT	ISO	HR/A	Dept. Mgr.	Owner	User
Determining the required access rights of users to assets.	R,C	C		C	R,A	I
Adhering to information security policies and procedures pertaining to the protection of information.	C	C	C			R,A,I
Reporting actual or suspected security incidents to ICT Deanship	A,C	C			I	R
Ensuring resigned or terminated employee return all IAU's assets interested before they complete termination process.	C	C	R,A	I		
Revoking access rights (logical and physical) to assets upon employee termination or change.	R,A	C	C			
Ensuring the protection of information / infrastructure systems, according to the technological mechanisms defined by the system / application design team.	R,A	R,C				
Investigating breaches of security controls, and implementing additional compensating controls when necessary.	R,A	R,C			I	
Implementing proper controls to protect assets.	R,A	C			I	
Reviewing user access rights and privileges in a regular basis.	R,A	C	C		R,C	
Approving user access registration form.	C	C		R,A	C	I

Table 2: Assigned Roles and Responsibilities based on RACI Matrix

4.8. Relevant Documents

The followings are all relevant policies and procedures to this policy:

- Information Security Policy
- Human Resource Security Policy

[1] The responsibility assignment RACI matrix describes the participation by various roles in completing tasks for a business process. It is especially useful in clarifying roles and responsibilities in cross-functional/departmental processes. **R** stands for Responsible who performs a task, **A** stands for Accountable (or Approver) who sings off (approves) on a task that a responsible performs, **C** stands for Consulted (or Consul) who provide opinions, and **I** stands for Informed who is kept up-to-date on task progress.

- Physical and Environmental Security Policy
- Operations Security Policy
- Communications Security Policy
- Compliance Policy
- Risk Management Policy
- Change Management Procedure
- Physical and Logical Access Control Procedure
- Human Resource Security Procedure

4.9. Ownership

This document is owned and maintained by the ICT Deanship of University of Imam Abdulrahman bin Faisal.

5. Policy Statements

The following subsections present the policy statements in 14 main aspects:

- Access Control Policy
- Access to Networks and Network Services
- User Registration and De-Registration
- User Access Provisioning
- Management of Privileged Access Rights
- Management of Secret Authentication Information of Users
- Review of User Access Rights
- Removal of Adjustment of Access Rights
- Use of Secret Authentication Information
- Information Access Restriction
- Secure Log-On Procedures
- Password Management System
- Use of Privileged Utility Programs
- Access Control to Program Source Code

5.1. Access Control Policy

1. Access to information shall be controlled based on business and security requirements and the access control rules defined for each IAU's system. These rules shall include the followings:
    a. Both logical and physical access controls.
    b. Security requirements of IAU's business applications.
    c. An identified business requirement for the user to have access to the information or business process (both 'need-to-know' and 'need-to-use' principles).
    d. All access is denied unless specifically approved under the provisions of this policy.

   e. Changes in user permission whether performed automatically or by an administrator.
   f. Legal and/or contractual obligation to restrict and protect access to IAU's systems.

2. Access for contractors or third parties personnel to IAU's business information assets shall be provided only based on a contractual agreement. This agreement shall include, but not be limited to:
   a. The terms and conditions for access provided.
   b. The security responsibilities of the contractors or third parties personnel.
   c. Agreement by the contractors or third parties personnel to abide to IAU's information security policies.

Ref# [ISO/IEC 27001: A.9.1.1]

5.2. Access to Networks and Network Services

1. Access to networks and network services shall be authorized and controlled based on business, security requirements and access control rules defined for each network. These rules shall take include the followings:
   a. Security requirements of the network or network services.
   b. An identified business requirement for the user to have access to the network (e.g., use of VPN or wireless network) or network services ('need-to-have' principle).
   c. The user's security classification and the security classification of the network.
   d. The user's authentication requirements for accessing various network services.
   e. Monitoring and managing of the use of network services.
   f. The authorization mechanisms for determining who is allowed to access which networks and network services.
2. All computers shall be not connected to IAU network and be allowed full access to all network resources and the Internet unless they fulfil with the network access control requirements as follows:
   a. Security policies of operating system.
   b. Updated antivirus definitions.
   c. Firewall security rules.

3. Access to IAU wired and wireless network shall be provided for employees, students and guests as per the following security requirements:

Group	Security Requirements	
	Wired Network	**Wireless Network**
Employees	• Check for antivirus Symantec endpoint, Antispyware and Antivirus definitions for an update not older than 5 days. • Compliant machines shall get full access to IAU network based on the Port VLAN membership. • Non-compliant domain machines and users shall be denied to access the IAU network (i.e., network resources and Internet access).	• Web redirection to Cisco Web NAC agent to check for an antivirus update not older than 5 days. • Compliant users shall be granting access to UC services using their mobile devices after profiling. • Compliant users shall be granting a limited access to only Internet connection without accessing internal network resources. • Non-compliant users shall be totally blocked from accessing network resources (including Internet access).
Students	• Check for antivirus Symantec endpoint, Antispyware and Antivirus definitions for an update not older than 5 days. • Compliant machines shall be granting a limited access to only SIS servers and Internet connection. • Non-compliant domain machines and users shall be blocked from accessing SIS servers (i.e., SIS resources and Internet access).	• Web redirection to Cisco Web NAC agent to check for an antivirus update not older than 5 days. • Compliant users shall be granting access to Internet and internal SIS servers. • Non-compliant users shall be totally blocked from accessing network resources (including Internet access).
Guests	No access at all	• Guest shall login to Open SSID for accessing wireless connection.

		• Enforce redirect to web page to submit required information. • Allowed for Self-registration by submitting First Name, Last Name and Mobile Number. • Users shall be receiving a valid One Time Password (OTP) through SMS (i.e., login with credentials sent by SMS and mapped to Active Directory). • Compliant users shall be granting a limited access to Internet only.

Caption , and reference that this came from IAU

4. Access to shared folders shall consider the followings:
    a. Only authorized for specific employees.
    b. Only used for IAU's business purpose.
    c. Sharing any non-related business materials (e.g., photos, videos, audio files, etc.) shall not be permitted.

Ref:[ISO/IEC 27001: A.9.1.2]

5.3. User Registration and De-Registration

1. ICT Deanship shall define a formal access control procedure that includes clear steps in relation to requesting, creating, modifying, suspending and revoking user accounts.
2. The granting of user access, changes to existing user access rights and removal of user access shall be authorized by Owner taking into account the following:
    a. Least privilege ('need-to-know' principle).
    b. Segregation of duties.
    c. Level of access required.
3. The process for managing user IDs shall address the following:

a. All IAU's employees shall be identified with a unique ID that establishes identity. User ID shall require at least one factor of authentication (e.g., password, token number or biometric devices).

b. All IAU's employees shall be registered by IAU's formal approved user registration procedure.

c. Redundant, shared or group user IDs shall not be allowed.

d. Redundant user shall be removed or disabled.

e. The number of privileged user IDs shall be strictly limited to those individuals who shall have such privileges for authorized business purposes.

f. Multi-user systems administrators shall have at least two user-IDs to separate their privileged access from their ordinary day-to-day access.

g. Consistent access control across different types of IAU's systems shall be achieved by supporting standard user ID codes, production programs and file names, and system names.

[ISO/IEC 27001: A.9.2.1]

5.4. User Access Provisioning

1. All authorized user accessing IAU's assets shall be defined and documented. Authorizations process shall be tracked and logged as follows:

    a. Date of authorization.

    b. Identification of individual approving access.

    c. Description of access privileges granted.

    d. Description of why access privileges granted.

2. The provisioning process for assigning or revoking access rights for users shall consider the followings:

    a. Obtaining a proper authorization from the system or service's owner.

    b. Segregation of duties to ensure a proper access level is given.

    c. Access rights are not activated until an authorization process is completed.

    d. Records reflecting all user access rights are centrally kept up-to-date.

e. Updating users access rights based on IAU's employees roles and responsibilities.

f. Reviewing users access rights in a regular basis

3. ICT Deanship shall grant users access to IAU's systems and services in accordance with their business role and job description (i.e., access right profiles).

[ISO/IEC 27001: A.9.2.2]

5.5. Management of Privileged Access Rights

1. The allocation and use of privileges access rights shall be managed as follows:

   a. Identification of access rights required for each system or process (e.g., operation system, database, application and network).

   b. Granting access rights based on a need-to-use and event-by-event principles.

   c. Defining expiry requirements for all access rights.

   d. Providing access rights in accordance with system's configuration capabilities.

2. Users shall not have access to administration account or privileges on their local machines.

[ISO/IEC 27001: A.9.2.3]

5.6. Management of Secret Authentication Information of Users

1. All IAU's systems shall require identification and authentication through a proper secret authentication information method (e.g., passwords, token IDs, smart cards or biometrics).

2. Prior to allowing user access to any IAU's system or application, a password authentication method shall be implemented as follows:

   a. Password shall be a minimum of 8 characters length for normal users and 12 characters for IT administrators (e.g., system admin, application admin, DB admin and network admin).

   b. Password shall be combination of at least three of the four followings:

      - At least one lower case alphabetic character (a-z)

      - At least one upper case alphabetic character (A-Z)

- At least one number (0-9)
- At least one special character (e.g., @#$%^&*()_+|~-=\`{}[]:";'<>/)

c. Passwords shall not contain user ID.

d. Passwords shall contain no more than two identical characters in a row and not made up of all numeric or alpha characters.

e. Blank password shall not be allowed.

f. Users shall be required to change their password immediately after their first login to any system (i.e., It shall be configured to prompt a user to choose another password before continuing with his session).

g. User account shall be locked fort 3 minutes after 3 unsuccessful attempts:

h. Password change shall be enforced (by the operating system or the application) at least every 90 days. Re-use of the same password shall not be allowed.

i. Initial password shall be only used one time (i.e., it shall be valid only for the involved user's first login) and shall be expired at 23:59:59 of the date issued.

j. Password shall be stored and transmitted in protected (e.g., encrypted or hashed) form, if possible.

3. Passwords shall be immediately changed if there is any suspicion of password compromise; and this shall be reported immediately to ICT Deanship.
4. ICT Deanship shall change all IAU's systems and software default usernames and passwords upon installation.
5. ICT Deanship shall reset user passwords after getting a formal verification of user identity.

REF: [ISO/IEC 27001: A.9.2.4]

5.7. Review of User Access Rights

1. Upon detection of any misconduct of privileged access rights, ICT Deanship shall restrict such privileges.
2. All IAU's users' access rights shall be reviewed in accordance with the formally approved User Physical and Local Access Control Procedure.

3. ICT Deanship in cooperation with Asset Owner and Information Security Officer shall:
    a. Establish a user access rights review plan that includes:
        - IAU's systems to be reviewed.
        - The review frequency.
    b. Review the following access privileges:
        - Access profiles for high risk systems (mission critical systems) every three months
        - Access profiles for medium risk systems every six months.
        - Access profiles for normal risk systems on an annual basis.

REF:[ISO/IEC 27001: A.9.2.5]

5.8. Removal or Adjustment of Access Rights

1. Department Manager shall promptly report all significant changes in employees' duties and/or employment status to Human Resources Department / Administration Unit and ICT Deanship.
2. When an employee permanently leaves IAU:
    a. System administrators shall be notified.
    b. All IAU's access privileges shall be promptly terminated.
    c. ICT Deanship, unless notified to the contrary, shall purge all files held in the employee's directory one month after employment termination.

[ISO/IEC 27001: A.9.2.6]

5.9. Use of Secret Authentication Information

1. Users shall be accountable for any activity associated with their access rights.
2. Users shall not capture or otherwise obtain passwords, decryption keys or any other secret authentication method that could permit unauthorized access.
3. Users shall not do the following:
    a. Reveal a password over the phone to anyone.

b. Reveal a password in an email message.

c. Reveal or distribute a password to others even to ICT Administrators or his boss.

d. Talk about a password in front of other.

e. Hint at the format of a password:

- Name of family, friends and co-workers
- Birthday, address and phone number
- Patterns: "aaabbb" and "1112222"

f. Reveal a password on questionnaires or security forms.

g. Share a password with family members.

h. Reveal a password to co-workers while on vacation.

i. Write a password on a piece of paper and left in a place where unauthorized users are able to discover them.

4. ICT Deanship shall ensure that:

a. Passwords are always encrypted when held in storage or in system logs on any IAU's system.

b. Passwords are not be stored in internet browsers (i.e., cookie on user's workstations are not set for automatic password completion and login).

c. Systems are designed, tested and controlled to prevent the retrieval of and the unauthorized use of stored passwords.

REF: [ISO/IEC 27001: A.9.3.1]

5.10. Information Access Restriction

1. Appropriate controls shall be defined to control application systems functions as follows:

a. Limiting outputs information.

b. Restricting access to information based on a user access profile.

c. Defining proper access privileges required (e.g., read, write, delete and execute).

d. Implementing logical and physical access isolation between different critical IAU's systems.

[ISO/IEC 27001: A.9.4.1]

5.11. Secure Log-On Procedures

1. Login into IAU's operating systems shall be based on a formal secure logon procedure.
2. All systems shall display a general notice warning message that access to IAU's systems is granted to authorized users only.
3. The logon process on any system shall display only the limited information about the system and its purposed use.
4. When strong authentication and identification is required, authentication methods other than passwords (e.g., token IDs, smart cards or biometrics) shall be implemented.
5. All systems shall limit the number of unsuccessful logon attempts allowed; the following shall be considered:
    a. Recording both successful and unsuccessful attempts.
    b. Forcing a time delay before further logon attempts are allowed or rejecting any further attempts without specific authorization.
    c. Sending an alarm message to the system console if the maximum number of logon attempts is reached.
6. ICT Administrators (e.g., system admin, application admin, DB admin and network admin) shall review all unsuccessful log attempts in a periodically basis.

[ISO/IEC 27001: A.9.4.2]

5.12. Password Management System

1. ICT Deanship shall adopt an interactive system for managing passwords in order to:
    a. Enforce a quality of passwords.
    b. Enforce regular password changes as needed.
    c. Maintain a record of previously used passwords
    d. Hide passwords on the screen when being entered.

e. Isolate password files from application system data

f. Encrypt password when being stored and transmitted

REF: [ISO/IEC 27001: A.9.4.3]

5.13. Use of Privileged Utility Programs

1. System utilities shall be restricted from all users unless the user has received a written authorization from ICT Deanship.
2. All access to system utilities shall be logged and reviewed by the relevant ICT Deanship.
3. Access to and use of system programs shall be restricted and controlled.
4. All unnecessary system utilities and software shall be removed.

[ISO/IEC 27001: A.9.4.4]

5.14. Access Control to Program Source Code

1. Access to programs source codes, configurations and relevant items (e.g., designs, specifications, verification plans and validation plans) shall be documented and restricted to an authorized personnel.
2. ICT Deanship shall ensure that all source codes are compiled, controlled and maintained centrally.

REF: [ISO/IEC 27001: A.9.4.5]

---------- End of Document ----------