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

Acceptable Use Policy

Version: 2.0

CODE: DICT.I.06-27.CS.E.V2.0

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

1 Table of Con.

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
ACCEPTABLE USE POLICY	RESTRICTED	V2.0	ACTIVE

3.2 Revision History

Version	Author(s)	Issue Date	Changes
V1.0	DR. BASHAR ALDEEB	04/01/2021	CREATION
V1.1	DR. SAMER BANI AWWAD	02/04/2022	REVIEW AND UPDATE
V2.0	BAHA NAWAFLEH	27/12/2023	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, informational, and technological assets is essential for the success of the IAU to achieve this goal, the Cybersecurity Management develops, establishes, and organizes the necessary security operations to safeguard information and technological assets. This document outlines the Acceptable Use Policy for assets within the organization, along with the security requirements based on global best practices and relevant legislative and regulatory requirements.

This policy is included within the framework of the IAU's policies and falls under the authority granted by the policy owner, effective from the date of its adoption.

5 Objective of the Policy

The purpose of this policy is to define the acceptable use of assets, such as equipment, software, networks, information, and communication systems operated by the IAU. It aims to raise awareness among all affiliates, contractors, and authorized users of the organization's systems about their responsibilities and duties regarding the utilization of information systems and services. The intention of this policy is to safeguard information and assets embedded in the IT infrastructure and other documents. This is achieved through controlling the use of information systems and data at an acceptable level that aligns with the operational and security requirements of the IAU.

6 Applicability and Scope

The provisions of this policy apply to all affiliates or individuals engaged in work within the IAU, whether on permanent or temporary contracts, whether directly or indirectly involved. This includes suppliers, external contractors, and any individual with permanent or temporary access rights to the IAU's data, regardless of the source, form, or nature of the data, as well as to the IAU's systems, devices, and databases.

7 Policy

7.1 General Policy Requirements

7.1.1 All information must be treated according to the specified classification, in alignment with the data classification policy and data protection policy of the IAU. This ensures the confidentiality, integrity, and availability of information.

7.1.2 All affiliates, contractors, and external parties are prohibited from attempting to access data, electronic documents, emails, and software within the IAU's information technology systems without authorization.

7.1.3 All affiliates must recognize that any data stored in the IAU's systems is owned by the IAU. Therefore, any transfer of this information requires proper authorization and necessary actions.

7.1.4 Affiliates are prohibited from disclosing any information related to the IAU or its work to unauthorized individuals, both internally and externally.

7.1.5 Systems administrators and authorized personnel must not disclose details about systems and networks, including remote access to or communication with the IAU's information technology resources, to unauthorized individuals.

7.1.6 Printouts should not be left unattended on shared printers.

7.1.7 All affiliates should use assigned information technology systems and assets with care, as their security and integrity are their responsibility.

7.1.8 Affiliates and external contractors are prohibited from copying documents with restricted rights or proprietary software and information owned by the IAU.

7.1.9 All affiliates and contractors must not install unauthorized software (such as freeware or shareware) without approval from the IT management.

7.1.10 Affiliates should avoid activities that negatively impact the efficiency of the IAU's IT resources and refrain from engaging in activities that could result in revocation of privileges.

7.1.11 Affiliates must take adequate steps to prevent unauthorized access to IAU information, including avoiding information leakage.

7.1.12 Personal use of IAU resources, including storing personal data, is prohibited. The IAU does not guarantee the privacy of personal information stored on its assets used specifically for work purposes.

7.1.13 Sharing user account data (passwords) with others is prohibited, and users are fully responsible for their accounts. Failure to comply may lead to disciplinary action.

7.1.14 Laptops, company-owned mobile devices, and other IT systems must be used in a manner that preserves their confidentiality and protects stored information.

7.1.15 Disabling or bypassing antivirus protection or security features on IT resources is prohibited.

7.1.16 Copying or transferring any classified information is prohibited, including but not limited to CDs, USB drives, and email attachments, without following cybersecurity guidelines.

7.1.17 External storage media should be securely stored, considering factors like temperature and isolation.

7.1.18 Use of portable media for storing or transferring IAU data is only allowed for work purposes with prior authorization from cybersecurity management. Encrypted and protected storage media should be used.

7.1.19 Cybersecurity management retains the right to monitor and review user accounts, networks, systems, and infrastructure periodically to ensure compliance with this policy.

7.1.20 Users are prohibited from engaging in illegal activities, such as unauthorized access, hacking, or actions that could disrupt asset use.

7.1.21 Immediate reporting to IT management is required in case of equipment damage, loss, or theft.

7.1.22 Unauthorized individuals must not enter restricted areas within the IAU.

7.1.23 Capturing photos or videos within the IAU is prohibited.

7.1.24 Unauthorized individuals must not be hosted in sensitive areas without prior permission.

7.1.25 Identification badges must be worn at all times within the IAU.

7.1.26 IT Security Management should be notified in case of information loss, theft, leakage, or suspected cyber threats.

7.2 Protection of User Devices

7.2.1 All users must ensure they log out of information systems before leaving the IAU at the end of working hours. Additionally, they should lock the system during their short breaks before leaving their workstations.

7.2.2 All users are prohibited from leaving any confidential information on their desks where it could be read, copied, or manipulated without their knowledge. This information should be secured, stored in lockable cabinets, or securely disposed of, such as using a paper shredder.

7.2.3 All users must ensure that screen savers are password-protected. The IT management should set a password-protected screen saver to activate after 5 minutes of device inactivity.

7.2.4 All users should install privacy screens to support the confidentiality of all users in the IAU.

7.2.5 All users are prohibited from installing new equipment on laptops or IAU devices without permission from the IT management.

7.2.6 All users must ensure that there is no pirated or unauthorized software installed on laptops or IAU devices. Only approved and authorized software is allowed to be installed.

7.2.7 Users are only allowed to use equipment that is approved and owned by the IAU.

7.2.8 The use of gaming software on any IAU systems is not allowed, and it is prohibited to install or transfer such software within the IAU's network.

7.2.9 High-level privileges (Admin Privileges) must be securely controlled on all IAU devices, and they should not be assigned for regular user usage within the IAU.

7.3 Acceptable Use of Internet and Software

7.3.1 Internet usage should be limited to work-related purposes only.

7.3.2 Users are prohibited from downloading non-work-related media, such as:

- Peer-to-peer software and file-sharing software.
- Movies, games, music, software, scripts, etc.

7.3.3 Technical staff, contractors, and other parties responsible for technical troubleshooting and operations must obtain permission from the cybersecurity management before installing and using software on work devices, such as instant messaging or data access control software.

7.3.4 Users must notify the IT management if they suspect security warning messages appearing during usage.

7.3.5 Unlicensed software or other forms of intellectual property are prohibited.

7.3.6 Techniques that bypass proxies or firewalls to access the Internet are prohibited.

7.3.7 Downloading or installing software and tools on IAU assets requires prior permission from the cybersecurity management.

7.3.8 Conducting security assessments to discover vulnerabilities, including penetration testing, monitoring IAU networks and systems, external networks and systems, such as port scanning, network reconnaissance, deception, vulnerability scanning, and network monitoring, is prohibited without prior permission from the cybersecurity management.

7.3.9 Internet users are not allowed to visit pages related to hacking, phishing, peer-to-peer networks, or proxies. Services and known malicious sites should be blocked by the IAU.

7.4 Acceptable Use of Email

7.4.1 The email system is primarily available for work-related use. Email should be used responsibly in accordance with the email security policy.

7.4.2 The exchange of inappropriate or unacceptable content via the IAU's email, whether internal or to external recipients, is not allowed.

7.4.3 All users must report any phishing or malicious email messages to the cybersecurity management.

7.4.4 All email correspondence should take place within the approved and closed network.

7.4.5 The IAU has the right to access or disclose any email communication upon specific request, with necessary authorization from the concerned party within the IAU and cybersecurity management. This is in line with relevant regulations and legislation.

7.4.6 The use of the IAU's systems for generating or distributing chain emails is prohibited.

7.4.7 The circulation of cybersecurity warning email messages is restricted to the relevant authority only, which is the cybersecurity management, or sending an urgent warning about a non-existent virus.

7.4.8 The IT management must ensure that all incoming and outgoing email messages include a disclaimer about the IAU.

7.4.9 Users should not open suspicious emails, links, attachments, or any unexpected emails, even from a trusted source.

7.4.10 The cybersecurity management should be notified if there is suspicion of email messages containing content that may harm the IAU's systems or assets.

7.4.11 The IAU's email address should not be registered on any non-work-related websites.

7.4.12 Encryption techniques should be used when sending sensitive information through email or communication systems.

7.5 Online Communications and Video Conferencing

7.5.1 All users must ensure they use approved equipment from the IAU for their online communications and video conferencing.

7.5.2 Online communications and video conferences should be conducted solely for work purposes.

7.5.3 Security measures for both physical and virtual meetings should be observed.

7.6 Password Usage

7.6.1 All users of the information system within the IAU must bear the responsibility of selecting and maintaining a secure password in accordance with the password policy of the IAU.

7.6.2 Users are prohibited from writing their passwords in email messages or electronic communications.

7.6.3 The information system within the IAU must not be used for the following purposes:

- Disclosing passwords over the phone to anyone.
- Disclosing passwords to anyone, including IT managers, family members, colleagues, or supervisors.
- Disclosing passwords over the internet.
- Writing passwords on paper or on a phone.
- Sharing passwords with anyone else.

7.6.4 Users of the information system within the IAU are responsible for any activity related to their access rights.

7.6.5 Users are not allowed to obtain or possess any passwords, decryption keys, or access mechanisms that may lead to unauthorized access. Users may be held accountable for any activities conducted through their accounts.

7.6.6 Users of the information system within the IAU should choose different passwords for their accounts within the IAU compared to their personal accounts, such as social media or personal email accounts (e.g., Yahoo, Gmail, Hotmail, etc.).

7.6.7 Users are required to change their password immediately upon receiving a temporary password from the system administrator.

8 Roles and Responsibilities

The cybersecurity management must undertake the following responsibilities:

8.1.1 The Head of Cybersecurity Management should endorse the policy from the appropriate authority and work towards its implementation.

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

8.1.3 The Head of Cybersecurity Management should ensure alignment between this policy and the IAU's operations.

8.1.4 The Head of Cybersecurity Management should resolve any conflicts arising from this policy.

8.1.5 The Head of Cybersecurity Management should provide the necessary resources to identify, purchase, and implement technical solutions to meet the policy's requirements for asset usage wherever possible.

8.1.6 Cybersecurity Management should disseminate the cybersecurity compliance policy to all departments, affiliates, and authorized users of the IAU or those who will be granted access to the technical and informational assets.

8.1.7 Cybersecurity Management should coordinate with relevant departments to monitor compliance and execution.

8.1.8 The Cybersecurity Management should periodically review the policy according to the established timeline.

The Deanship of Information and Communication Technology (DICT) should:

8.1.9 Adhere to this policy, implement the controls mentioned in this policy, and also report any security incidents to the Head of Cybersecurity Management.

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

8.1.10 Ensure the dissemination of this policy to all affiliates within the IAU or department.

8.1.11 Report any violations or non-compliance with this policy to the Head of Cybersecurity.

8.1.12 Ensure that all affiliates within the IAU 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.

9 Policy Ownership

The owner of this policy is the Head of the Cybersecurity Management in the IAU.

10 Policy Changes

The policy must 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 individuals within the IAU, including external parties/contractors, must comply with the provisions of this policy. The Head of Cybersecurity within the IAU is responsible for ensuring continuous compliance. Necessary reports regarding compliance should be submitted periodically to the authorized entity.

Necessary measures should be taken to ensure compliance with the provisions of this policy. This can be achieved through regular reviews conducted by the Cybersecurity Department or related departments. Corrective actions should be taken by the authorized entity within the IAU based on recommendations from the Head of Cybersecurity regarding any violations of this policy. Disciplinary actions should be proportionate to the severity of the incident as determined by the investigation. Disciplinary actions may include, but are not limited to:

- Revoking access privileges to data, information technology assets, and connected systems.
- Issuing a written warning or terminating the employment of the affiliate, as deemed appropriate by the IAU.

Non-compliance with any provisions of this policy without obtaining prior exceptions from the Cybersecurity Department requires appropriate actions in accordance with the existing policies and regulations within the IAU, as deemed suitable. Additionally, contractual terms with individuals or entities contracted with must also be followed.

12 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.06-44.CS.E. V2.0 - Email Security Policy
- DICT.I.06-15.CS.E. V2.0 - Password Policy
- DICT.I.06-69.CS.E.V2.0 Password Management standards
- DICT.I.06-49.CS.E.V2.0 Identity And Access Management Standards
- DICT.I.06-60.CS.E.V2.0 Asset Classification Standards

13 References

Department Name	National Institute for Standards and Technology	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	Key Cybersecurity Controls
Acceptable Use Policy for Assets.	AC-20, PL-4, PS-6	A.7.1.3	-	-	-	-	3-1-2
Use of Confidential Authentication Information	IA-5(1), IA-5(4), IA-2	A.9.3.1	-	-	-	-	2-2-3
Electronic Message Exchange	AU-10, SC-7, SC-8, SC-44	A.10.8.4	-	-	-	-	2-4

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