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

Cybersecurity compliance policy

Version: 2.0

CODE: DICT.I.06-02.CS.E.V2.0

1 Table of Content

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
CYBERSECURITY COMPLIANCE POLICY	RESTRICTED	V2.0	ACTIVE

3.2 Revision History

Version	Author(s)	Issue Date	Changes
V1.0	DR. BASHAR ALDEEB	02/03/2021	CREATION
V1.1	DR. SAMER BANI AWWAD	02/06/2022	REVIEW AND UPDATE
V2.0	BAHA NAWAFLEH	15/12/2023	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

Safeguarding information and technology assets are imperative for the success of the IAU. To this end, the Cybersecurity Management is dedicated to developing information security governance and overseeing the necessary security operations to protect its data, assets, and personal information. This is crucial for the sustained success of the IAU. This document outlines the Cybersecurity Compliance Policy, following global best practices, standards, and regulations.

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

5 Objective of the Policy

The aim of the Cybersecurity Compliance Policy is to ensure the IAU's adherence to regulatory and contractual obligations concerning cybersecurity, intellectual property rights, and copyright for the use of information technology systems, all types of data, and the IAU's technology assets.

6 Applicability and Scope

The provisions of this policy apply to all affiliates or contractors working within the IAU, whether on a permanent or temporary basis, and whether directly or indirectly involved. This includes suppliers, external contractors, and any individuals with permanent or temporary access rights to the IAU's data, regardless of its source, form, nature, and to the IAU's systems, devices, and databases.

7 Policy

7.1 Policy Clauses

7.1.1 Cybersecurity policies must be periodically defined and reviewed based on a specific and approved timeline, with continuous monitoring of their implementation.

7.1.2 The responsibilities of the IAU and the authorized representatives concerning compliance matters, reporting, and resolution should be clearly defined and communicated.

7.1.3 The upper management and the Cybersecurity Management within the IAU should collaborate with the internal audit management to ensure the achievement of required compliance levels.

7.1.4 Full compliance with all regulatory requirements, statutory provisions, relevant regulations, IAU's activities, policies, regulations, directives, instructions, and national-level requirements issued and published by the Government of the Kingdom of Saudi Arabia is required.

7.1.5 Identification and compilation of systems, regulations, organizational and legislative documents related to cybersecurity and related requirements are necessary.

7.1.6 Adequate technologies and competencies must be provided to verify compliance with legal and regulatory requirements and the IAU's requirements related to cybersecurity.

7.1.7 Regular enforcement of cybersecurity policies and procedures should occur based on a defined and approved timeline by the authorized entity within the IAU. This should be facilitated using appropriate tools such as:

- Cybersecurity Risk Assessment activities.
- Vulnerabilities Management activities.
- Penetration Test activities.
- Review of cybersecurity standards.
- Security Source Code Review.
- User surveys.
- System and network permissions review.
- Review of cybersecurity logs and incidents.

7.1.8 Necessary corrective actions should be identified and implemented to rectify vulnerabilities for all compliance requirements by the Cybersecurity Management.

7.1.9 A disclaimer notice, confidentiality, and privacy statement should be attached to all published information through email, memos, notifications, and all other forms of communication to ensure recipients are aware of the constraints imposed on the transmitted data.

7.1.10 Appropriate measures must be undertaken to comply with legislative and regulatory requirements concerning data confidentiality, privacy, intellectual property rights, and software usage.

7.1.11 Key Performance Indicators (KPIs) should be employed to ensure continuous improvement in cybersecurity compliance.

7.2 Intellectual Property Rights

7.2.1 Compliance with regulatory constraints imposed on intellectual property rights (such as copyright, trademarks, software applications, and others) is mandatory based on regulatory requirements.

7.2.2 The use of pirated software within the IAU is strictly prohibited.

7.2.3 The IAU should educate various departments/stakeholders to protect intellectual property rights and inform them about taking disciplinary actions against individuals violating these rights.

7.2.4 All IT assets requiring protection of intellectual property rights must be identified.

7.2.5 The IAU should retain evidence and documentation of ownership of licenses, master disks, and guidance materials containing intellectual property rights-related content, in accordance with data storage and retention policy provisions.

7.3 Protection of IAU's Documents

7.3.1 Procedures for handling IAU's data, retention, and disposal mechanisms must be defined and implemented in accordance with relevant legal, legislative, regulatory, contractual requirements, as well as the IAU's data governance policy and data protection policy.

7.3.2 IAU's documents should be retained and stored according to the data storage and retention policy.

7.3.3 Classification of IAU's documents should be conducted based on their type, importance, and confidentiality, in accordance with the data classification policy.

7.4 Protection of Personal Data

7.4.1 Protection of personal data must be considered in accordance with regulatory and legislative requirements, and the Cybersecurity Management should propose necessary clauses to be added to contractual documents and other relevant IAU's documents.

7.4.2 Security controls for protecting personal data should be applied based on data classification level and impact level, as defined by the data classification policy of the IAU.

7.4.3 Awareness training for users should be conducted to familiarize them with the implemented personal data protection systems.

7.4.4 Personal data should be safeguarded against leakage, damage, loss, theft, transfer, copying, quoting, misuse, alteration, and unauthorized access, following the approved IAU's policies and guidelines set forth by the National Data Management Office (NDMO), the National Cybersecurity Authority (NCA), the Personal Data Protection System, and relevant authorities.

7.5 Preventing Misuse of Information Processing Facilities

7.5.1 Use of information processing facilities of the IAU for unauthorized purposes is strictly prohibited.

7.5.2 Necessary measures should be taken to ensure that information technology facilities receive adequate protection in accordance with relevant regulations, including at a minimum:

- Conducting awareness campaigns for users regarding compliance issues and encouraging them to report non-compliance.
- Monitoring data and information systems to detect unauthorized usage.

7.6 Compliance with Polices and Security Standards

7.6.1 All affiliates must be informed about and provided with access to the Cybersecurity policies. Contractors and external parties should also have access to these policies.

7.6.2 All Cybersecurity policies should be made available on the internal network of the IAU for reference.

7.6.3 Ensuring that affiliates carry out all procedures and guidelines related to their responsibilities is essential.

7.6.4 Regularly verify the implementation of Cybersecurity policies and their procedures according to a specified timeline.

7.6.5 Appropriate corrective measures and preventive controls should be established, their priorities determined, and timely execution ensured to address identified security weaknesses by the Cybersecurity Management.

7.6.6 Necessary metrics and tools should be established to assist in the evaluation and improvement of the compliance program.

7.6.7 Continuous improvement processes must be ensured through the activation of monitoring and follow-up activities.

7.6.8 Regular updates of the Cybersecurity Risk Assessment records should be conducted to include new threats and vulnerabilities.

7.7 Technical Compliance Assessments

7.7.1 The Cybersecurity Management must conduct regular technical assessments of compliance. This should include examining operating systems to ensure correct implementation of hardware and software controls.

7.7.2 The technical assessment should encompass penetration testing and security vulnerability assessments, which can be conducted internally or by independent experts specifically contracted for this purpose.

7.7.3 Regular technical assessments should be conducted to ensure compliance with security standards within the IAU, in alignment with the Minimum-Security Baseline.

7.8 Legal Responsibilities Awareness

7.8.1 All affiliates must be aware of their responsibilities regarding the use of data, technical assets, and information to avoid legal issues in case of violations.

7.8.2 Non-compliance by affiliates with legal aspects of data usage and IT assets may result in disciplinary actions as stipulated in relevant regulations and policies. Additional penalties as defined by related systems or regulations, including penalties related to the dissemination of classified documents and information, might also apply.

7.9 Compliance with General Copyright Laws

7.9.1 Making copies of materials protected by copyright constitutes a violation of relevant regulations and laws, and infringing on the rights of authors is considered a criminal offense.

7.9.2 Unintentional violations of copyright laws due to lack of awareness necessitate taking necessary legal actions in accordance with regulatory provisions and relevant laws.

7.9.3 Failure to comply with legal requirements related to software licenses results in taking regulatory actions against the user.

7.9.4 This policy also extends to protecting the copyright of information related to databases.

7.10Copyright and Software Licensing Regulations

7.10.1 Copying and distributing software is not allowed unless explicitly authorized by the person responsible for Cybersecurity Management.

7.10.2 Sharing or distributing copies of software without proper licensing from the software owner is prohibited.

7.10.3 Copying and distributing software over the network or engaging in any illegal activities that threaten the university's security or could lead to legal actions against it are prohibited.

7.10.4 Unauthorized use of software by contractors and consultants within the university's premises entails taking necessary regulatory actions against them.

7.10.5 Software licenses must be kept in a secure location and should be readily available for inspection, as failing to do so could result in penalties for the user.

7.10.6 The Cybersecurity Management should seek legal advice regarding requirements and regulations governing intellectual property rights and software licenses.

7.10.7 In cases where transferring software installed on old or unnecessary computers might breach copyright law, all software on storage media must be erased, followed by necessary procedures for asset disposal as outlined by the General Department of Financial and Administrative Affairs.

7.10.8 Possession of software with unauthorized licenses or modifying it to alter its legal specifications is prohibited.

7.11Auditing and Review

7.11.1 The implementation of controls for protecting the confidentiality, integrity, availability, and privacy of information and personal data within the university should be audited by a different management/body than the Cybersecurity Management.

7.11.2 The results of the review, observations, and findings should be documented, and a report with these results should be generated and discussed with relevant parties.

7.11.3 The audit report should include the scope of the audit, observations, recommendations, corrective actions, and proposed remediation plan.

7.11.4 The results of the review and related observations should be presented to the Cybersecurity Oversight Committee.

7.11.5 Pre-emptive and corrective measures should be implemented based on the audit results and observations.

7.11.6 The elements that led to these results and observations should be identified, analysed, and the causes determined.

7.11.7 A number of measures should be identified to prevent or minimize the likelihood of recurrence of observations.

7.11.8 A timeline should be established for addressing reported non-compliant issues, and the application of proposed solutions should be continually monitored to ensure their effectiveness.

7.11.9 The access privileges for data and systems by the auditor should be granted according to the principle of "need to know" and "need to use".

8 Roles and Responsibilities

The Cybersecurity Management responsibilities:

8.1.1 The Head of the Cybersecurity Management shall approve the policy on behalf of the authorized entity and work on its implementation.

8.1.2 The Head of the Cybersecurity Management shall approve standards, procedures, and guidelines to ensure necessary compliance with the security requirements of the university operations.

8.1.3 The Head of the Cybersecurity Management shall ensure alignment between this policy and the operations of the university.

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

8.1.5 The Head of the Cybersecurity Management shall provide necessary resources to identify, acquire, and implement technical solutions, if feasible, to meet the policy requirements.

8.1.6 Staffs of the Cybersecurity Management shall ensure the dissemination of the Cybersecurity Compliance Policy to all departments, staff, and users authorized to access technical and information assets within the university or those who will be granted access.

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

8.1.8 Staffs of the Cybersecurity Management shall periodically review the policy according to the established timeline.

The Director of Legal Affairs responsibilities:

8.1.9 In the event of a violation of compliance with this policy based on the investigation by the Cybersecurity Management, take necessary actions.

The Director of Quality Assurance Department shall:

8.1.10 Review the cybersecurity controls, audit their implementation according to accepted general audit standards, and relevant legislative and regulatory requirements.

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

8.1.11 Ensure the dissemination of this policy to all affiliates within the university or unit.

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

University Affiliates shall:

8.1.13 Comply with the provisions of this policy and report any security incidents or non-compliance with any provisions of this policy to the Head of Cybersecurity Management.

9 Ownership of the Policy

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

10 Changes to the Policy

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

11 Compliance

All affiliates within the university and external parties/contractors must comply with the provisions of this policy. The Head of Cybersecurity Management within the university is responsible for continuous monitoring of compliance and for regularly reporting on this matter to the authorized entity.

Necessary actions must be taken to ensure compliance with the policy. The Cybersecurity Management or relevant departments should conduct periodic reviews and corrective actions should be taken by the authorized entity within the university, based on recommendations from the Head of Cybersecurity Management, regarding any violations of this policy. Disciplinary actions should be proportionate to the severity of the incident, as determined by the investigation. Disciplinary measures may include, but are not limited to, the following:

- Revoking access privileges to data, IT assets, and connected systems of the university.
- Issuing a written warning or terminating the employment of the affiliate, or taking appropriate measures as deemed fit by the university.

Non-compliance with any provisions of this policy without obtaining prior exception from the Cybersecurity Management requires taking appropriate actions according to the policies and regulations in place within the university, or as deemed appropriate, and in accordance with contractual terms with any individuals or entities contracted with.

12 Related Policies, Standards and Procedures

- DICT.I.06-01.CS.E. V2.0 - General Cybersecurity Policy
- DICT.I.06-24.CS.E. V2.0 - Cybersecurity Risk Management Policy
- DICT.I.06-28.CS.E. V2.0 - Cybersecurity Continuity of Business Policy
- DICT.I.06-25.CS.E. V2.0 - Human Resources Security Policy
- DICT.I.06-41.CS.E. V2.0 - Third Party and Suppliers Security Policy
- DICT.I.06-32.CS.E. V2.0 - Physical and Environmental Security Policy
- DICT.I.06-03.CS.E. V2.0 - Data Protection Policy
- DICT.I.06-20.CS.E. V2.0 - Data Storage and Retention Policy
- DICT.I.06-21.CS.E. V2.0 - Data Classification Policy
- DICT.I.06-13.CS.E. V2.0 - Personal Data Protection Policy
- DICT.I.06-29.CS.E. V2.0 - Encryption Policy
- DICT.I.06-39.CS.E. V2.0 - Network Security Policy
- DICT.I.06-09.CS.E. V2.0 - Cybersecurity Incident Management Policy
- DICT.I.06-10.CS.E. V2.0 - Event Logs Management and Cybersecurity Monitoring Policy
- DICT.I.06-05.CS.E. V2.0 - Vulnerability Management and Penetration Testing Policy
- DICT.I.06-30.CS.E. V2.0 - Anti-Malware Policy
- DICT.I.06-42.CS.E. V2.0 - Workstations, Mobile Devices and BYOD Security Policy
- DICT.I.06-43.CS.E. V2.0 - Cloud Computing Security Policy
- DICT.I.06-22.CS.E. V2.0 - System Acquisition, Development, and Maintenance Policy
- DICT.I.06-07.CS.E. V2.0 - Backup Management Policy
- DICT.I.06-08.CS.E. V2.0 - Patch and Update Management Policy

- ❖ DICT.I.06-26.CS.E. V2.0 - Clear Desk and Clear Screen Policy
- ❖ DICT.I.06-04.CS.E. V2.0 - Asset Management Policy
- ❖ DICT.I.06-06.CS.E. V2.0 - Change Management Policy
- ❖ DICT.I.06-27.CS.E. V2.0 - Acceptable Use of Assets Policy
- ❖ DICT.I.06-33.CS.E. V2.0 - Access Control Policy
- ❖ DICT.I.06-44.CS.E. V2.0 - Email Security 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.06-12.CS.E. V2.0 - Cookie Policy
- ❖ DICT.I.06-38.CS.E. V2.0 - Configuration and Hardening Policy
- ❖ DICT.I.06-34.CS.E. V2.0 - Cybersecurity Policy for Project Management
- ❖ DICT.I.06-11.CS.E. V2.0 - Data Sharing Policy
- ❖ DICT.I.06-37.CS.E. V2.0 - Cybersecurity Policy for Teleworking
- ❖ DICT.I.06-40.CS.E. V2.0 - Operations Security Policy
- ❖ DICT.I.06-39s.CS.E. V2.0 - Network Security policy
- ❖ DICT.I.06-35.CS.E. V2.0 - Cybersecurity Policy for Social Media Accounts and Media
- ❖ DICT.I.06-36.CS.E. V2.0 - Cybersecurity Policy to Protect Printers, Scanners and Photocopiers
- ❖ DICT.I.06-45.CS.E.V2.0 Cybersecurity assessment and audit policy
- ❖ DICT.I.06-46.CS.E.V2.0 Storage Media Security Policy
- ❖ DICT.I.06-47.CS.E.V2.0 Secure Systems Development Life Cycle policy
- ❖ DICT.I.06-48.CS.E.V2.0 Privileged Access Workstations Standards
- ❖ DICT.I.06-49.CS.E.V2.0 Identity And Access Management Standards
- ❖ DICT.I.06-50.CS.E.V2.0 Physical Security Standards
- ❖ DICT.I.06-51.CS.E.V2.0 Secure Coding Standard
- ❖ DICT.I.06-52.CS.E.V2.0 Advanced Persistent Threats (APT) Standards
- ❖ DICT.I.06-53.CS.E.V2.0 Data Loss Prevention Standards
- ❖ DICT.I.06-54.CS.E.V2.0 Network Detection and Response Standards
- ❖ DICT.I.06-55.CS.E.V2.0 Email Protection Standards
- ❖ DICT.I.06-56.CS.E.V2.0 Data Cybersecurity Standards
- ❖ DICT.I.06-57.CS.E.V2.0 Standard Virtualization Security
- ❖ DICT.I.06-58.CS.E.V2.0 Database Security Standards

- DICT.I.06-59.CS.E.V2.0 Social Media Security Standard
- DICT.I.06-60.CS.E.V2.0 Asset Classification Standards
- DICT.I.06-61.CS.E.V2.0 Data Protection Standards
- DICT.I.06-62.CS.E.V2.0 Asset Management Standards
- DICT.I.06-63.CS.E.V2.0 Vulnerability Management and Penetration Testing Standards
- DICT.I.06-64.CS.E.V2.0 Change Management Standards
- DICT.I.06-65.CS.E.V2.0 Backup and Restoration Standards
- DICT.I.06-66.CS.E.V2.0 Patch Management Standards
- DICT.I.06-67.CS.E.V2.0 Cybersecurity Incident Management Standards
- DICT.I.06-68.CS.E.V2.0 Cybersecurity Events Logs and Monitoring Management standards
- DICT.I.06-69.CS.E.V2.0 Password Management standards
- DICT.I.06-70.CS.E.V2.0 System Acquisition, Development and Maintenance Standards
- DICT.I.06-71.CS.E.V2.0 Encryption Standards
- DICT.I.06-72.CS.E.V2.0 Anti-Malware Standards
- DICT.I.06-73.CS.E.V2.0 Web Application Security Standards
- DICT.I.06-74.CS.E.V2.0 Cybersecurity Policy for Project Management Standards
- DICT.I.06-75.CS.E.V2.0 Configuration and Hardening Standards
- DICT.I.06-76.CS.E.V2.0 Server Security Standards
- DICT.I.06-77.CS.E.V2.0 Network Security Standards
- DICT.I.06-78.CS.E.V2.0 Third Party and Suppliers Security Standards
- DICT.I.06-79.CS.E.V2.0 Workstations, Mobile Devices and BYOD Security Standards
- DICT.I.06-80.CS.E.V2.0 Proxy Security Standards
- DICT.I.06-81.CS.E.V2.0 Key Management Standards
- DICT.I.06-82.CS.E.V2.0 Protection against Distributed Denial of Service (DDOS) attacks
- DICT.I.06-83.CS.E.V2.0 Data Diode Standards
- DICT.I.04-34.CS.E.V2.0 Change Management Procedures
- DICT.I.04-35.CS.E.V2.0 Backup and Restoration Procedures
- DICT.I.04-36.CS.E.V2.0 System Acquisition, Development and Maintenance Procedures
- DICT.I.04-37.CS.E.V2.0 Anti-Malware Procedures
- DICT.I.04-38.CS.E.V2.0 Cybersecurity Audit Procedures
- DICT.I.04-39.CS.E.V2.0 Vulnerabilities Assessment Procedures
- DICT.I.04-41.CS.E.V2.0 Cybersecurity Documents Development Procedures

13 References

Department Name	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
Identifying Applicable Regulations	A.18.2.1	-	-	-	-	7-1
Intellectual Property Rights	A.18.2.2	-	-	-	-	-
Protection of IAU Records	A.18.2.3	-	-	-	-	-
Data Protection and Personal Data Privacy	A.18.2.4	-	-	-	7-2	3-7-2
Compliance with Security Policies and Standards	A.18.1.2	-	-	-	4-1	8-1
Technical Compliance	A.18.1.3	-	-	-	4-1	8-1

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