جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

Policy for Teleworking

Version: 2.0

CODE: DICT.I.06-37.CS.E.V2.0

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

Table of Cont.

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

1.1 Information

Title	Classification	Version	Status
POLICY FOR TELEWORKING	RESTRICTED	V2.0	ACTIVE

1.2 Revision History

Version	Author(s)	Issue Date	Changes
V1.0	DR. BASHAR ALDEEB	27/01/2021	CREATION
V1.1	DR. SAMER BANI AWWAD	02/08/2022	REVIEW AND UPDATE
V2.0	BAHA NAWAFLEH	26/12/2023	REVIEW AND UPDATE

1.3 Document Review

Date of Next Scheduled Review
01/01/2025

1.4 Distribution List

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

1.5 Approval

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

3 Introduction

Protection of information, information assets, and technology is considered essential for the success of the IAU. To this end, the Cybersecurity Management develops, establishes, and organizes the necessary security operations to safeguard information and technological assets. This document defines the remote work policy within the university, in accordance with relevant IAU policies, regulatory procedures, legislative requirements, and regulations.

This policy is aligned within the framework of the university's policy and falls under the authority granted by the responsible entity, effective from the date of its approval.

4 Goal of the Policy

The purpose of the remote work policy is to provide guidance and security requirements to all users regarding their responsibilities and obligations concerning the remote use of the IAU's assets and data.

5 Applicability and Scope

The provisions of this policy apply to all affiliates or contractors working within the IAU, whether on permanent or temporary contracts, directly or indirectly. This includes external suppliers, contractors, and anyone who possesses permanent or temporary access privileges to the university's 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 Approval from the Cybersecurity Management within the university must be obtained for remote work access requests, following the submission of necessary justifications.

6.1.2 The Cybersecurity Management within the university must review remote work access requests, considering data classification and the sensitivity of technological and information assets during the review.

6.1.3 Designated classified data that can be accessed, utilized, or interacted with through remote work systems must be protected using necessary technical controls, such as Data Leakage Prevention, and other techniques through analysing cyber risks for the university.

6.1.4 In cases where personal devices are permitted for remote work, the device used for remote work must meet the security requirements set by the university.

6.1.5 Mobile devices and Bring Your Own Device (BYOD) devices must be centrally managed using Mobile Device Management (MDM) system.

6.1.6 All necessary security controls must be applied in accordance with the requirements for mobile devices as stated in the Mobile Device Security Policy and Personal Device Policy.

6.1.7 Affiliates must ensure adequate protection of mobile devices in public spaces.

6.1.8 Security packages for technological assets and remote access systems must be updated periodically, not less than once per year.

6.1.9 Factory default configurations for remote work systems must be reviewed and secured, including the removal of default passwords and backgrounds.

6.1.10 The implementation of secure management requirements for sessions must be ensured, including:

- Session authenticity
- Session lockout
- Session timeout

6.1.11 Activation of features and services in remote work systems must be restricted as needed, while analysing potential cyber risks in case of activation.

6.1.12 Network ports, protocols, and services used for remote access, especially on internal systems, must be restricted and opened as needed.

6.1.13 Firewall rules related to remote work systems must be regularly reviewed.

6.1.14 Protection against Distributed Denial of Service (DDoS) attacks must be provided for remote work systems to mitigate cyber risks resulting from service disruption attacks.

6.1.15 Continuous protection against Network Advanced Persistent Threats (Network APT) must be provided for remote work systems.

6.2 Protection of Data and Information

6.2.1 Hard drives of devices used for remote work must be fully encrypted.

6.2.2 Scheduled backups must be performed for remote work systems based on a planned timeline, considering the assessment of Cybersecurity risks for the university.

6.2.3 Regular assessments must be conducted to determine the effectiveness of the recovery of backup systems for remote work.

6.2.4 Updated and secure methods and algorithms for encryption must be used for the entire network communication used for remote work.

6.2.5 Information related to the university stored on devices used for remote work must be deleted in the following cases:

- Device loss or theft
- Suspected security threat on the device
- Termination of the affiliate's affiliation with the university

6.2.6 Protection against viruses, suspicious activities, and Malware on user devices and servers used for remote access must be ensured using modern and advanced protection techniques, and these should be securely managed.

6.3 Cybersecurity Risk Management

6.3.1 Regular assessment of cybersecurity risks for remote work systems must be conducted.

6.3.2 Cybersecurity risks must be assessed during planning and prior to allowing remote work for any service or system.

6.3.3 Cybersecurity risks specific to remote work systems, services, and authorized remote work systems must be included in the university's cybersecurity risk register.

6.4 Asset Management

6.4.1 Information and technological assets for remote work systems must be identified, documented, and updated regularly.

6.5 Access Control Management

6.5.1 User permissions for remote work must be managed based on work requirements, considering system sensitivity, permission levels, and the types of devices used by remote workers.

6.5.2 Concurrent logins from multiple devices for the same user must be restricted for remote access.

6.5.3 Secure standards must be used for managing identities and passwords used in remote work systems.

6.5.4 Multi-Factor Authentication must be implemented for remote login processes.

6.5.5 Regular review of remote work login identities and permissions must be conducted.

6.6 Vulnerability Management and Penetration Testing

6.6.1 Vulnerability scanning and discovery must be conducted on remote work systems, classifying them based on their severity at least once every three months.

6.6.2 Addressing vulnerabilities in remote work systems must be carried out at least once every three months.

6.6.3 Penetration testing must be conducted at least once a year on remote work systems, encompassing all technical components of remote work systems.

6.7 Cloud Computing and Hosting

6.7.1 The hosting location for remote work systems must be within the Kingdom of Saudi Arabia.

6.8 Awareness and Training

6.8.1 Necessary guidance must be provided to affiliates within the university to ensure they possess the required technical skills for applying cybersecurity requirements and practices when dealing with remote work systems.

6.9 Cybersecurity Monitoring, Incidents, and Threats

6.9.1 Cybersecurity event logs for technological assets and remote work systems must be enabled and continuously monitored around the clock.

6.9.2 User Behaviour Analytics (UBA) must be implemented to analyse and monitor the behaviour of remote work systems users.

6.9.3 Continuous update and implementation of 24/7 cybersecurity monitoring procedures must include monitoring remote login activities, especially logins from outside the Kingdom, and verification of their legitimacy.

6.9.4 Cybersecurity event logs for remote work systems must be retained for at least 12 months in accordance with relevant legislative and regulatory requirements.

6.9.5 Incident response plans and contact information within the IAU must be updated to align with the remote work situation, ensuring communication capability and incident response team readiness.

6.9.6 Periodic acquisition and handling of relevant Threat Intelligence for remote work systems must be conducted.

6.9.7 Recommendations and alerts regarding cybersecurity incidents and threats issued by the National Cybersecurity Authority must be executed and implemented.

7 Roles and Responsibilities

The Cybersecurity Management responsibilities:

7.1.1 The Head of Cybersecurity Management is responsible for approving the policy by the authorized entity and ensuring its implementation.

7.1.2 The Head of Cybersecurity Management shall endorse standards, procedures, and guidelines to ensure necessary compliance with the security requirements of the university's operations.

7.1.3 The Head of Cybersecurity Management must ensure alignment between this policy and the university's activities.

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

7.1.5 The Head of Cybersecurity Management shall provide necessary resources for identifying, procuring, and implementing technical solutions to fulfil policy requirements where possible.

7.1.6 The Cybersecurity Management shall disseminate the cybersecurity compliance policy to all departments, affiliates, and authorized users of the university or those who will be granted access to technological and informational assets.

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

7.1.8 The Cybersecurity Management shall periodically review the policy according to the defined schedule.

The Deanship of Information and Communication Technology shall:

7.1.9 Comply with this policy, implement the controls mentioned in this policy, and report any security incidents to the Cybersecurity Management.

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

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

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

7.1.12 Ensure that all affiliates within the university must adhere to 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.

8 Policy Ownership

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

9 Policy Changes

The policy must be reviewed annually at a minimum or when there are changes in legislative and regulatory requirements. Changes must be documented and endorsed by the authorized entity within the university.

10 Compliance

All individuals within the university, including external parties/contractors, must adhere to the provisions of this policy. The Head of Cybersecurity in the university must ensure continuous monitoring of compliance and provide periodic reports to the authorized entity.

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

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

Non-compliance with any provisions of this policy without prior authorization from the Cybersecurity Department requires appropriate actions to be taken according to the policies and regulations in place within the university. This also applies to contractual terms with individuals or entities contracting with the university.

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.06-24.CS.E. V2.0 - Cybersecurity Risk Management Policy
- DICT.I.06-32.CS.E. V2.0 - Physical and Environmental Security Policy
- DICT.I.06-21.CS.E. V2.0 - Data Classification 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 - Cybersecurity Event logs 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.06-04.CS.E. V2.0 - Asset Management Policy
- DICT.I.06-33.CS.E. V2.0 - Access Control Policy
- DICT.I.06-38.CS.E. V2.0 - Configuration and Hardening Policy
- 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.06-60.CS.E.V2.0 Asset Classification 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.06-67.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.06-71.CS.E.V2.0 Encryption Standards

- DICT.I.06-72.CS.E.V2.0 Anti-Malware Standards
- DICT.I.06-79.CS.E.V2.0 Workstations, Mobile Devices and BYOD Security Standards
- DICT.I.04-40.CS.E.V2.0 Cybersecurity Risk Management Procedures
- DICT.I.04-37.CS.E.V2.0 Anti-Malware Procedures

12 References

Department Name	The National Institute for Standards and Technology	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	Core Cybersecurity Controls
Distance working	-	A.6.2.2	-	-	2-1 3-1 1-2 2-2 3-2 4-2 5-2 6-2 7-2 8-2 9-2 10-2 11-2 12-2 1-3	1-3-1	1-3-1

---------- End of document ----------