جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

Anti-Malware Policy

Version: 2.0

CODE: DICT.I.06-30.CS.E.V2.0

1 Table of Contents

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
ANTI-MALWARE POLICY	RESTRICTED	V2.0	ACTIVE

3.2 Revision History

Version	Author(s)	Issue Date	Changes
V1.0	DR. BASHAR ALDEEB	07/01/2021	CREATION
V1.1	DR. SAMER BANI AWWAD	02/03/2022	REVIEW AND UPDATE
V2.0	BAHA NAWAFLEH	30/12/2023	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

Information and information technology asset protection is essential for the success of the university. To achieve this goal, the Cybersecurity Management develops, establishes, and organizes the required security processes to safeguard information and technological assets. This document defines the security requirements for protection against malware based on international best practices and relevant legislative and regulatory requirements.

This policy falls within the scope of the university's policy and is executed under the authority granted by the responsible entity, starting from its date of approval.

5 Policy Objective

The objective of this policy is to establish procedures and requirements for identifying, assessing, mitigating, and neutralizing malware attacks against the university. The Cybersecurity Management develops a set of tools to protect the information and technological assets of the university, which will be implemented accordingly.

6 Applicability and Scope

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

7 Policy

7.1 General Policy Requirements

7.1.1 Install antimalware software on all servers, computers, and network-connected mobile devices, and centrally manage it securely.

7.1.2 Enable antimalware software at all times.

7.1.3 Ensure that protection technologies and mechanisms can detect and remove all known types of malwares, such as viruses, Trojan horses, worms, spyware, adware, and rootkits.

7.1.4 Choose protection technologies and mechanisms suitable for the university's operating systems, such as Windows, UNIX, Linux, macOS, and others.

7.1.5 If updates to protection technologies cause harm to systems or business requirements, ensure that the protection technologies can be rolled back to the previous version.

7.1.6 Restrict permissions to disable, uninstall, or modify settings of antimalware protection software and grant these permissions only to system security administrators.

7.2 Configuration of Antimalware Protection Technologies and Mechanisms

7.2.1 Configure the settings of protection technologies and mechanisms according to the university's approved security standards, taking into consideration vendor guidelines and recommendations.

7.2.2 External parties' personnel are not allowed to connect to the university's network.

7.2.3 Configure protection technology settings to allow only a specific list of whitelisted application and program executable files to operate on servers dedicated to sensitive systems.

7.2.4 Prevent access to websites and other online sources known to host malware using a web content filtering mechanism.

7.2.5 Centralize and synchronize timing (Clock Synchronization) accurately from a reliable source to all university assets, as well as all antimalware protection technologies and mechanisms.

7.2.6 Protect servers on all systems, especially sensitive ones, using approved endpoint protection techniques.

7.2.7 Configure antimalware software on servers/user devices to automatically update virus definitions. Servers and computers should download virus definition updates from the central management server using the primary client mechanism. In case of central management server failure, the client device should be configured to directly download virus definition updates from a trusted source.

7.2.8 Configure antimalware software to automatically scan all removable assets before use.

7.2.9 Protect antimalware software with a password to prevent users from changing settings or disabling it.

7.2.10 Generate periodic reports on antimalware protection status, indicating the number of devices and servers connected to protection technologies and their status (e.g., updated, not updated, disconnected, etc.), and submit them to the Head of Cybersecurity Management in the university.

7.2.11 All applications supporting file upload or transfer must have antimalware protection technologies.

7.2.12 Perform periodic scanning of user devices and servers to ensure they are free of malware.

Add point related to quick scan policy

7.2.13 Configure antimalware protection technology settings to perform suspicious content verification in isolated sources like a Sandbox.

7.2.14 When malware is discovered in the university information and technology assets, the cybersecurity management should scan the infected servers/computers.

7.2.15 In the event of malware spread, the cybersecurity management takes immediate measures to minimize damage.

7.2.16 Verify incoming data to the university network, including email, to ensure it is free of malware.

7.2.17 Users must report incidents of malware to the cybersecurity management.

7.2.18 The university must prohibit the use of unauthorized and unlicensed software and utilities on all information and technology assets.

8 Roles and Responsibilities

The Cybersecurity Management responsibilities:

8.1.1 The Head of Cybersecurity Management is responsible for endorsing the policy on behalf of the authority and ensuring its implementation.

8.1.2 The Head of Cybersecurity Management is responsible for endorsing standards, procedures, and guidelines to ensure necessary compliance with the university operation security requirements.

8.1.3 The Head of Cybersecurity Management must ensure the alignment of this policy with the university's operations.

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

8.1.5 The Head of Cybersecurity Management must provide the necessary resources for identifying, purchasing, and implementing technical solutions to meet the policy's requirements wherever possible.

8.1.6 The Head of Cybersecurity Management must establish mechanisms or processes for monitoring antimalware solutions to ensure appropriate usage and that activities are limited to authorized personnel who require the program for their designated tasks.

8.1.7 The Cybersecurity Management must disseminate the cybersecurity compliance policy to all departments, affiliates, and users authorized or to be authorized access to technological and information assets.

8.1.8 The Cybersecurity Management must coordinate with relevant departments to monitor compliance and implementation.

8.1.9 The Cybersecurity Management must establish a security baseline from which malicious and suspicious activities can be measured.

8.1.10 The Cybersecurity Management must detect unusual activities of the university personnel through electronic monitoring and other indicators. Based on these suspicious cases, risks of malicious behavior must be evaluated.

8.1.11 The Cybersecurity Management must define the necessary actions to be taken when responding to virus alerts on computers/servers.

8.1.12 The Cybersecurity Management must periodically review the policy according to the defined timeline.

The Deanship of Information and Communication Technology shall:

8.1.13 Comply with this policy, implement the controls outlined in this policy, and report any security incidents to the General Management of Cybersecurity Management.

8.1.14 Support the initiatives of the malicious software management program within the university, including investigating suspected users or those who pose a risk to the university's information.

8.1.15 Provide the necessary support for raising awareness and training users within the university.

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

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

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

8.1.18 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.

9 Ownership of the Policy

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

10 Policy Changes

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

11 Compliance

All individuals within the university, including external parties or contractors, must adhere to the terms of this policy. The Head of Cybersecurity Management within the university must ensure continuous monitoring of compliance and regularly report on this matter to the authorized party.

Necessary measures should be taken to ensure compliance with this policy. This can be achieved through periodic reviews conducted by the Cybersecurity Management or related departments. 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 should be proportional to the severity of the incident as determined by the investigation, and may include, but are not limited to:

- Revoking access rights to data, IT assets, and connected systems of the university.
- Sending written warnings or terminating the employment of the staff member, or other appropriate actions as deemed by the university.

Non-compliance with any provisions of this policy, without prior approval from the Cybersecurity Management, will lead to appropriate actions in accordance with the university's policies and regulations, or as suitable, and as defined by contractual agreements 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.06-02.CS.E. V2.0- Cybersecurity Compliance Policy
- DICT.I.06-29.CS.E. V2.0- Encryption Policy
- DICT.I.06-09.CS.E. V2.0- Cybersecurity Incident Management Policy
- DICT.I.06-10.CS.E. V2.0- Security Event Logs and Monitoring Policy
- DICT.I.06-71.CS.E.V2.0 Encryption 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.04-37.CS.E.V2.0 Anti-Malware Procedures

13 References

Department Name	National Institute for Standards and Technology	ISO 27001:2013	Cybersecurity Controls for Cloud Computing	Cybersecurity Controls for Social Media Accounts for IAU	Cybersecurity Controls for Remote Work	Cybersecurity Controls for Sensitive Systems	Core Cybersecurity Controls
Protection against Malware		A12.2 ,A12.2.1					
Web Application Security	-	A.6.2.2	-	-	-	-	1-15-2
Protection of Information Processing Systems and Devices	-	-	-	-	-	1-3-2	3-3-2

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