


King AbdulAziz University
Cyber-Security Center

Vulnerabilities Management Policy

Restricted-Internal

Document Authorization:

Role	Name	Date	Signature
Owner	Cyber-Security Center	14/11/2022 CE	

Document Versions:

Version	Date	Editor	Reasons for Revision
1.0	23/11/2021 CE	Shuruq bint Khalid Banafi	ISO27001
2.0	14/11/2022 CE	Ashwaq bint Samir Abd al-Jawad	In accordance with the requirements of the Authority

Table of Contents

<i>Objectives.....</i>	<i>4</i>
<i>Scope and Applicability of the Work.....</i>	<i>4</i>
<i>Policy Clauses</i>	<i>4</i>
<i>Roles and Responsibilities.....</i>	<i>5</i>
<i>Compliance with the Policy.....</i>	<i>5</i>

Objectives

The purpose of this policy is to provide and fulfill cyber-security requirements, based on best practices and standards, to ensure that technical vulnerabilities are discovered and addressed in a timely manner, so as to prevent or reduce the potential exploitation of such vulnerabilities through cyber-attacks, and likewise to reduce the consequences of such attacks for King AbdulAziz University, and to protect the University from internal and external threats, through focus upon the essential objectives of protection, which are: Confidentiality, integrity, and availability of information.

This policy aims to comply with cyber-security requirements and the relevant legislative and regulatory requirements, which is itself a legislative requirement expressed in Control 2-10-1 of the Essential Cyber-Security Controls (ECC-1:2018) promulgated by the National Cyber-Security Authority.

Scope and Applicability of the Work

This policy covers all King AbdulAziz University informational and technical assets, and this policy applies to all King AbdulAziz University employees.

Policy Clauses

1– General Requirements

1-1 King AbdulAziz University must periodically carry out vulnerabilities assessments, so as to detect, evaluate, and address effectively technical vulnerabilities in a timely manner.

1-2 The Cyber-Security Center will identify systems, servers, and technical components requiring vulnerabilities assessment, in accordance with relevant legislative and regulatory requirements.

1-3 The Cyber-Security Center must ensure the use of reliable methods and tools for detecting vulnerabilities.

1-4 Procedures for implementing vulnerabilities assessment and detection must be developed and adopted, in accordance with relevant legislative and regulatory requirements.

1-5 In the event that an external party is authorized to carry out vulnerabilities assessment and detection on behalf of King AbdulAziz University, the application of all cyber-security requirements related to third-parties must be verified, in accordance with the Third-Party Cyber-Security Policy adopted by King AbdulAziz University.

2– Vulnerabilities Assessment Requirements

2-1 Vulnerabilities assessment and detection is required prior to the publication of servers or systems over the Internet, or when change is made to any critical systems, in accordance with the Cyber-Security Policy of the Information and Technology Projects Office.

2-2 Vulnerabilities must be classified according to the danger that they pose, and must be addressed in accordance with the cyber-risks linked to them, in accordance with the risk-management methodology adopted by King AbdulAziz University.

2-3 King AbdulAziz University must carry out vulnerabilities assessments for all technical and informational assets on a periodic basis. (ECC-2-10-3-1)

2-4 King AbdulAziz University must carry out vulnerabilities assessments for all technical components of critical internal systems and address any detected vulnerabilities at least once every three months. (CSCC-2-9-1-3).

2-5 King AbdulAziz University must carry out vulnerabilities assessments for all technical components of critical external systems connected to the Internet once a month. (CSCC-2-9-1-2)

3– Requirements for Addressing Vulnerabilities

3-1 After the conclusion of vulnerabilities assessment, a report must be prepared that explains, classifies, and suggests advice for addressing the vulnerabilities detected.

3-2 After a vulnerabilities assessment and treatment report has been sent by the relevant parties, the detected vulnerabilities must be detected and assessed again to ensure that they have been addressed.

3-3 Update and repair packages from reliable sources and in accordance with the Patches Policy must be used.

3-4 Newly-discovered critical vulnerabilities must be repaired and closed, following the change management mechanisms used at King AbdulAziz University. (CSCC-2-9-1-3)

3-5 In the event that a security vulnerability cannot be repaired and closed for any reason, it is necessary to apply other controls, such as shutting down the server to which the vulnerability relates, or to implement a complementary protection control, such as controlling access using firewalls or other solutions. The vulnerability must be monitored for actual attacks, and the Events Response Team must be notified concerning the vulnerability and the potential for it to be exploited.

4– Other Requirements

4-1 King AbdulAziz University must communicate and partner with reliable cyber-security sources that provide proactive threat intelligence, private groups with common interests, and external specialists with expertise in the subjects concerned, in order to gather information on new threats and how to limit existing vulnerabilities. (ECC-2-10-3-5)

4-2 The application of cyber-security requirements must be assessed periodically to manage technical vulnerabilities at King AbdulAziz University.

4-3 Key Performance Indicators (KPI) must be used to ensure the continual development of vulnerabilities management.

4-4 This policy must be reviewed at least once a year.

Roles and Responsibilities

–Responsible Party and Owner of the Document: Director of the Cyber-Security Center.

–Updating and Review of the Document: The Cyber-Security Center.

–Implementation and Application of the Document: The Deanship of Information Technology and the Cyber-Security Center.

Compliance with the Policy

1- The Director of the Cyber-Security Center must ensure the compliance of King AbdulAziz University with this policy periodically.

2- All employees of King AbdulAziz University must comply with this policy.

3- Any violation of this policy may subject the offender to disciplinary action, in accordance with the procedures followed by King AbdulAziz University.