


King AbdulAziz University
Cyber-Security Center

Penetration Test Policy

Restricted-Internal

Document Authorization:

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

Document Versions:

Version	Date	Editor	Reasons for Revision
1.0	15/11/2021 CE	Shuruq bint Khalid Banafi	
1.1	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, for evaluating and testing the effectiveness of cyber-security enhancement capabilities at King AbdulAziz University by means of imitating real cyber-attack techniques and methods, and to detect unrecognized security weak-points that could lead to cyber-penetration of King AbdulAziz University, through focus on 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 requirement of Control 2-11-1 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 critical systems and their technical components, and all externally-provided (over the Internet) services and their technical components, including but not limited to: Internet sites, Web applications, smart-phone and smart-tablet applications, email, and remote connection to King AbdulAziz University. This policy applies to all King AbdulAziz University employees.

Policy Clauses

1– General Requirements

1-1 King AbdulAziz University must carry out penetration testing periodically, to evaluate and test the effectiveness of cyber-security enhancement capabilities.

1-2 The Cyber-Security Center will identify the systems, services, and technical components that require penetration testing, in accordance with the relevant legislative and regulatory requirements.

1-3 King AbdulAziz University must carry out penetration tests upon all externally-provided services and technical components on a periodic basis. (ECC-2-11-3-1)

1-4 It must be ensured that penetration tests do not affect the systems and services provided at King AbdulAziz University.

1-5 King AbdulAziz University must carry out penetration tests on critical systems and technical components at least once a year. (CSCC-2-10-2)

1-6 Penetration tests must be carried out to detect security weak-points in all their forms, including weak points that often produce application development errors, configurations faults, and exploitability of identified vulnerabilities.

1-7 Special procedures for penetration testing must be developed, approved, and disseminated, with consideration being given to ensuring that penetration tests do not affect the workflow of King AbdulAziz University.

1-8 The Cyber-Security Center must define or approve the penetration test methods, tools, and techniques used by internal or external penetration test teams prior to the initiation of penetration test operations.

1-9 In the event that an external party carries out penetration testing on behalf of King AbdulAziz University, the application of all cyber-security requirements for external parties must be verified and in accordance with the Cyber-Security Policy for External Parties adopted by King AbdulAziz University.

1-10 The results of penetration tests must be classified based on their importance, and must be addressed according to the cyber-risks potentially consequent upon them and the risk-management methodology adopted by King AbdulAziz University.

1-11 An action plan must be established to address the results of penetration tests, which explains the impact of risks detected, as well as the mechanisms for addressing them, the responsibilities for applying them, and the time period within which they must be implemented.

2– Other Requirements

2-1 Key Performance Indicators (KPI) must be employed to ensure the continual development of penetration test operations.

2-2 The application of the cyber-security requirements for King AbdulAziz University penetration test operations must be reviewed periodically.

2-3 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.