


King AbdulAziz University
Cyber-Security Center

Penetration Test Plan

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	14/10/2022 CE	Ashwaq bint Samir Abd al-Jawad	

Objectives

The objective of this plan is to provide and fulfill cyber-security requirements, based on best practices and standards, for testing and evaluating the effectiveness of cyber-security enhancement capabilities at King AbdulAziz University and for detecting unrecognized security weak points that could allow for cyber-penetration of the University by imitating actual cyber-attack techniques and methods, through focus on the essential objectives of protection, which are: Confidentiality, integrity, and availability of information.

Implementation

This plan aims to comply with cyber-security requirements and the relevant legislative and regulatory requirements, which is itself a legislative requirement expressed in Control 2-11-3-2 of the Essential Cyber-Security Controls (ECC-1:2018) promulgated by the National Cyber-Security Authority.

Penetration Test Plan

In accordance with Control 2-11-3-2, which stipulates that the plan must include all externally-provided (over the Internet) services and technical components, including:

- Infrastructure
- Websites
- Web applications
- Smart phone and tablet applications
- Email and remote access
- The plan below has been laid out so that penetration tests will be carried out for all services provided externally over the Internet once a month, as follows:
- Active hosts as per scan report: 2513.
- Total hosts configured: 3006.
- Estimated hosts plan: 2750

[illegible]

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 Cyber-Security Center.