King AbdulAziz University
Cyber-Security Center

# Web Application Protection 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 | 15/11/2021 CE | Shuruq bint Khalid Banafi | |
| 1.1 | 14/11/2022 CE | Nashat ibn Nail Mala | In accordance with the requirements of the Authority |

## Table of Contents

## Objectives

The purpose of this policy is to provide and fulfill cyber-security requirements, based on best practices and standards, for the protection of external Web applications at King AbdulAziz University, so as to reduce cyber-risks and to protect the University from internal and external threats, 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 legislative requirement expressed in Control 2-15-1 of the Essential Cyber-Security Controls promulgated by the National Cyber-Security Authority (ECC-1:2018).

## Scope and Applicability of the Work

This policy covers all external Web applications pertaining to King AbdulAziz University, and this policy applies to all King AbdulAziz University employees.

## Policy Clauses

1– **General Requirements**

1-1 External Web applications purchased or developed internally must follow the multi-tier architecture principle. (ECC-2-15-3-2)

1-2 The multi-tier architectural principle must be employed for external Web applications pertaining to critical systems, with the number of tiers not falling below at least that of 3-tier architecture.

1-3 The exclusive use of secure communications protocols must be ensured, such as Hypertext Transfer Protocol Secure (HTTPS), Secure File Transfer Protocol (SFTP), Transfer Layer Security (TLS), etc. (ECC-2-15-3-3)

1-4 A Web application firewall system must be employed to protect external Web applications from external threats. (ECC-2-15-3-1)

1-5 Logical isolation must be applied to the development environment, the testing environment, and the production environment.

1-6 Information and data protection technologies and techniques must be employed in external Web applications, in accordance with the Data and Information Protection Policy and the Classification Policy.

1-7 In the event that Web applications are purchased from an external party, it must be ensured that the supplier complies with King AbdulAziz University cyber-security policies and standards.

1-8 At least the Minimum Application Security and Protection Standards (OWASP Top Ten) must be applied to external Web applications pertaining to critical systems. (CSCC-2-12-1-2)

2– **Access Right Requirements**

2-1 Multi-factor authentication must be employed for user logins to external Web applications. (ECC-2-15-3-5)

2-2 Security standards for Web application development must be documented and approved, including at a minimum secure session management and session authenticity, lockout, and timeout. (CSCC-2-12-1-1)

2-3 Access rights to production systems must be limited, and must be controlled in accordance with job responsibilities.

2-4 The Secure Use Policy must be disseminated to all external Web application users. (ECC-2-15-3-4)

3– **Requirements for Web Application Development or Purchase**

3-1 Cyber-security risks must be assessed when planning to develop or purchase Web applications, and prior to the launch of Web applications in the production environment, in accordance with the Cyber-Security Risk Management Policy approved by King AbdulAziz University.

3-2 Prior to the use of protected information in the test environment, prior permission must be obtained from the Cyber-Security Center, and strict controls must be employed for the protection of this data, such as: Data scrambling and data masking techniques, and deletion directly after use.

3-3 Source code must be securely maintained, and access to it must be restricted to authorized users only.

3-4 Penetration tests must be carried out for Web applications in the test environment, results must be documented, and it must be ensured that all vulnerabilities are addressed prior to launch in the production environment.

3-5 Vulnerabilities in the technical components of Web applications must be examined, and it must be ensured that vulnerabilities are addressed by installing update and repair packages approved by King AbdulAziz University.

3-6 Web applications must be approved by the Change Approval Board (CAB) prior to their launch in the production environment.

4– **Other Requirements**

4-1 Cyber-security requirements relating to external Web application protection must be reviewed periodically. (ECC-2-15-4)

4-2 Key Performance Indicators (KPI) must be employed to ensure continual development of external Web application protection.

4-3 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 on a continual basis.

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.