King AbdulAziz University
Cyber-Security Center

Network Security 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	ISO27001
2.0	14/11/2022 CE	Daniyal ibn Muhammad al-Ghazzawi	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 on the basis of best practices and standards relating to network security at King AbdulAziz University, so as to reduce cyber-risks and to protect the University from internal and threats, through focus on the essential objectives of protection, which are: Confidentiality, integrity, and availability of information.

This policy aims to comply with relevant legislative and regulatory cyber-security requirements, which is itself a legislative requirement expressed in Control 2-5-1 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 technical networks, and applies to all King AbdulAziz University employees.

Policy Clauses

1– **General Clauses**

1-1 All network devices within King AbdulAziz University must be identified, documented, and ensured to be updated and approved.

1-2 Technical security standards for all network devices used within King AbdulAziz University must be documented and approved.

1-3 Access privileges to all King AbdulAziz University networks must be managed in accordance with the Identity and Access Management Policy, such that access to King AbdulAziz University networks is allowed only when necessary, and only to authorized users.

2– **Network Access Requirements**

2-1 Procedures for providing and revoking network access privileges must be developed and approved, in accordance with the King AbdulAziz University Identity and Access Management Policy.

2-2 To obtain network access privileges, users must submit a request to the Deanship of Information Technology that specifies the type of access requested, the timeframe for the privileges requested, and the reasons for the request.

2-3 In the event that firewall rules are added or modified, the network administrator must document in the firewall system the operational requirements and information pertaining to the request.

2-4 A username and password must be used to access the King AbdulAziz University network, in accordance with the Identity and Access Management Policy.

2-5 Firewall settings and rules must be reviewed periodically, and at least every six months for critical systems. (CSCC-2-4-1-2).

2-6 The necessary protection must be provided for Internet browsing and connection, and access to suspicious websites, file-sharing sites, and remote access sites must be restricted.

2-7 The King AbdulAziz University wireless network should not be connected to the University's internal network except on the basis of a complete study of the risks involved in doing so. Such connection must proceed in a way that ensures the protection of personal technical assets, the confidentiality and integrity of data, and the protection of King AbdulAziz University systems and applications.

2-8 Critical systems must be prevented from connecting to the King AbdulAziz University wireless network.

2-9 Technologies necessary for setting restrictions and managing network ports, protocols, and services must be made available.

2-10 Direct connection to any local network devices pertaining to critical systems must be prevented in advance of assessment, and the availability of the elements necessary to achieve acceptable levels of protection for critical systems must be ensured. (CSCC-2-4-1-3)

3– **Requirements for External-Party Access to the Network**

3-1 The granting to external parties of access privileges to the King AbdulAziz University network must be subject to the cyber-security requirements laid out in the Cyber-Security Policy for External Parties.

3-2 Secure encryption and verification techniques must be employed in the transfer of data to or from external parties.

3-3 Specific timeframes for external-party access to the King AbdulAziz University network must be defined.

3-4 User and third-party access privileges must be reviewed periodically, in accordance with the cyber-security policies adopted by King AbdulAziz University.

4– **Protection of Networks**

4-1 Networks must be isolated and separated from one another both physically and logically using firewalls and the defense-in-depth principle. (ECC-2-5-3-1)

4-2 Logical isolation must be applied to networks pertaining to critical systems (VLAN).

4-3 Logical isolation must be applied between the production environment network, the test environment network, and other networks.

4-4 Connection of critical systems to the Internet must be prevented in the event that such systems are providing internal service to King AbdulAziz University and there is no absolutely necessary purpose for access to the service from outside of King AbdulAziz University. (CSCC-2-4-1-6)

4-5 Logical isolation must be applied between the Voice Over IP (VOIP) network and the data network.

4-6 The use of physical network ports in all King AbdulAziz University facilities must be restricted using the port security feature or port-based authentication techniques, to protect the network from potential undetected connections by unauthorized or suspicious devices.

4-7 Protection systems for Internet browsing channels must be provided and securely managed, so as to protect against advanced persistent threats (APT protection), which usually use viruses and zero-day malware.

4-8 Direct connection of the internal network to the Internet must be prevented. Connections must be made using Internet connection distributors (proxies), in order to allow for the analysis and filtering of data transferred to and from King AbdulAziz University.

4-9 Firewall rules settings must be set so that all types of connections between parts of the network are explicitly and automatically prohibited. Firewall rules may be made available as per user requests and operational requirements.

4-10 The technologies necessary for secure Domain Name Systems (DNS) must be made available.

4-11 Advanced intrusion detection and prevention systems must be made available for all parts of the network, and must be updated periodically.

4-12 Systems for protection from advanced persistent threats at the network level (Network APT) must be made available for networks pertaining to critical systems.

4-13 Tools for protecting Internet browsing channels from advanced persistent threats and unrecognized malware must be put into operation proactively, and securely managed. (ECC-2-5-3-8)

4-14 Systems for protection from Distributed Denial-of-Service (DDOS) attacks must be provided for critical external systems. (CSCC-2-4-1-8)

5– **Physical and Environmental Security**

5-1 Network devices must be maintained in a safe and appropriate environment, in which the degree of heat and moisture must be set and controlled, and for which backup sources of power are provided, such as an Uninterruptible Power Supply (UPS).

5-2 Physical access to networks devices must be restricted to authorized persons only, in order to preserve and protect devices from theft or tampering.

5-3 Access and monitoring (CCTV) records of network device areas pertaining to critical systems must be maintained and periodically reviewed.

6– **Other Requirements**

6-1 Key Performance Indicators (KPI) must be used to ensure the continual development of network security.

6-2 Review of cyber-security requirements relating to network security must be undertaken at least once a year, or in the event that changes are made to relevant legislative or regulatory requirements or standards.

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 Networks Office in the Deanship of Information Technology and the Cyber-Security Center.

Compliance with the Policy

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

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.