


King AbdulAziz University
Cyber-Security Center

Server 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 | |
| 1.1 | 14/11/2022 CE | Daniyal ibn Muhammad al-Ghazzawi | 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>6</i> |
| <i>Compliance with the Policy.....</i> | <i>7</i> |

Objectives

The purpose of this policy is to provide and fulfill cyber-security requirements, based on best practices and standards, for servers belonging to King AbdulAziz University, so as to reduce cyber-security risks, 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 2-3-1 of the Essential Cyber-Security Control (ECC-1:2018) promulgated by the National Cyber-Security Authority.

Scope and Applicability of the Work

This policy covers all King AbdulAziz University servers, and applies to all King AbdulAziz University employees.

Policy Clauses

1– General Clauses

1-1 All King AbdulAziz University servers must be identified and documented, and server software must be updated and certified.

1-2 Technical security standards must be developed and applied for King AbdulAziz University servers used internally, employing best international standards.

1-3 Server settings must be set according to the approved technical security standards prior to the operation of servers in the production environment.

1-4 The necessary protection must be provided for all servers, in order to control related cyber-security risks.

1-5 Regular backup copies of servers must be made in accordance with the Backup Management Policy adopted by King AbdulAziz University, to ensure the ability to restore them in the event that they are subjected to unintentional deletion or accident. (The Authority advises that backup copies be made for critical systems on a daily basis.)

1-6 Server software, including operating systems and application software must be updated and provided with the latest security patches, in accordance with the Patch Management Policy adopted by King AbdulAziz University.

2– Server Settings

2-1 An image of the settings and fortification of King AbdulAziz University server operating systems must be made available, approved, and stored in a secure location, in accordance with the adopted technical security standards.

2-2 An approved image must be used to install or update server operating systems.

2-3 Server settings and fortification must be approved, reviewed, and updated periodically, and at least once every six months for critical systems servers. (CSCC-6-1-3-2)

3– Access and Management

3-1 Access to King AbdulAziz University servers must be restricted, so as to make access available to authorized users only, and only when needed.

3-2 Access to servers must be restricted and limited to system administrator accounts, and administrator accounts and privileges must be reviewed periodically.

3-3 Access to servers pertaining to critical systems must be restricted and limited to technical teams holding important privileges, and should be granted through computing workstations. It is also necessary to isolate these workstation devices in a systems management network, and to prevent their being linked to any other network or server (such as email servers or the Internet).

3-4 Multi-factor identity authentication must be put into effect for access to servers pertaining to critical systems. (CSCC-3-1-2-2)

3-5 Factory and automated accounts must be suspended or changed, and unused servers and unused network ports on the operating system must be suspended.

3-6 Data stored on servers must be protected and encrypted, in accordance with the approved Cryptography Controls, based on their classification and according to the relevant legislative and regulatory requirements. (ECC-2-8-3-3)

4– Server Protection

4-1 Unreliable or un-updated servers must be prevented from connecting to the King AbdulAziz University network, and must be placed in an isolated network so that the necessary updates may be undertaken, in order to reduce related cyber-security risks that may lead to unauthorized access, malware entry, or data leakage.

4-2 Up-to-date and advanced techniques and tools for protection against viruses, suspicious activities, and malware must be employed and managed securely.

4-3 Only a specified list of whitelisted applications and software files must be permitted to run on servers pertaining to critical systems. (CSCC-2-3-1-1)

4-4 The use of external storage media on servers must be restricted, prior permission must be obtained from the Cyber-Security Center prior to their use, and their secure use must be ensured.

4-5 Servers must be installed in the appropriate area of the network structure/plan, according to operational and legislative requirements, to ensure their management and the application of the necessary protections to them in an effective manner.

5– Operations Requirements for Server Management

5-1 Servers must be centrally-managed at King AbdulAziz University, in order to enable faster detection of risks, and to enable the management and monitoring of servers, such as access restriction, installation of update packages, etc.

5-2 The necessary protection must be provided for servers operating in the virtual systems environment, which must be managed in a secure manner that accords with risk assessment.

5-3 Server settings should be set precisely, and the sending of events logs to the Security Information and Event Management (SIEM) system should be enabled, in accordance with the Cyber-Security Events Logs and Monitoring Policy.

5-4 Clock synchronization for all servers must be set centrally with reference to an accurate, reliable, and approved source.

5-5 Necessary requirements for server operation must be fulfilled in a secure and appropriate manner, such as the provision of a suitable and secure environment, and the monitoring of physical access to the server area, which must be restricted to authorized employees.

5-6 The Deanship of Information Technology must monitor the operational components of servers, and ensure their effective performance, availability, adequate storage capacity, and the like.

6– Vulnerabilities and Penetration Test Management

6-1 Servers must be checked, and vulnerabilities present in them must be detected and addressed based on the classification of the vulnerabilities detected and the potential cyber-risks they represent, on a periodic basis, and once monthly at least for critical systems servers. (CSCC-2-9-1-2)

6-2 Penetration test operations must be carried out on servers on a periodic basis, and at least once every three months on critical systems servers. (CSCC-2-10-2)

6-3 Security update and repair packages must be installed in order to address vulnerabilities and to raise the efficiency and security levels of servers, in accordance with the Patch Management Policy.

7– Physical and Environmental Protection for Servers

7-1 Entry and exit from King AbdulAziz University facilities, for example doors and locks, must be monitored and controlled.

7-2 Environmental factors, such as heating, air conditioning, smoke and fire alarms, and fire suppression systems must be monitored and controlled.

7-3 Appropriate physical security controls must be put in place (such as observation cameras exterior and interior to the King AbdulAziz University data center, security guards, cable protection systems, etc).

8– Other Requirements

8-1 Key Performance Indicators (KPI) must be used to ensure the continual development of server protection.

8-2 Cyber-security requirements relating to servers management must be reviewed once a year at least, or in the event that changes are made to the relevant legislative or regulatory requirements or standards.

9– Review and Application of Policies

9-1 Cyber-security requirements, and the application of cyber-security requirements, must be reviewed on a yearly basis.

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 Servers 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 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.