


King AbdulAziz University
Cyber-Security Center

Database 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>5</i>
<i>Compliance with the Policy.....</i>	<i>6</i>

Objectives

The purpose of this policy is to provide and fulfill cyber security requirements, based on best practices and standards, relating to the protection of databases pertaining to 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 1-3-2 of the Essential Cyber-Security Controls promulgated by the National Cyber-Security Authority.

Scope and Applicability of the Work

This policy covers all database systems pertaining to King AbdulAziz University, and applies to all King AbdulAziz University employees.

Policy Clauses

1– General Clauses

1-1 All database systems used within King AbdulAziz University must be identified and documented, and efforts must be made to provide an environment suitable to their protection from environmental and operational risks.

1-2 Technical security standards for database systems within King AbdulAziz University must be developed, approved, and implemented by database administrators.

1-3 With the exception of database administrators, access or direct interaction with databases pertaining to critical systems is forbidden, and may only be obtained through applications. (CSCC-2-2-1-8)

1-4 Access rights to databases must be given in accordance with the Identity and Access Management Policy.

1-5 Copy or transfer of database systems pertaining to critical systems from the production environment to any other environment is forbidden. (CSCC-2-6-1-5)

2– Required Security Procedures for Database Hosting

2-1 Operational continuity and disaster recovery requirements pertaining to databases must be clearly defined in contracts with cloud services providers, to include mutual roles and responsibilities with regard to backup versions, incident response, disaster recovery plans, etc.

2-2 Logical isolation must be maintained between King AbdulAziz University databases and other hosted databases.

2-3 Hosting sites for cloud services must be located entirely within the geographical boundaries of the Kingdom of Saudi Arabia. (ECC-3-3-2-4)

2-4 Administrator access privileges to databases must be restricted using strong encryption methods, such as Secure Shell Protocol (SSH), Virtual Private Networks (VPN), and Secure Sockets Layer (SSL)/ Transport Layer Security (TLS), in accordance with the Cryptography Policy adopted by King AbdulAziz University.

3– Change Management Requirements for Database Systems

3-1 Changes to databases (such as database migration or transfer to the production environment) must be made in accordance with the change management process adopted by King AbdulAziz University.

3-2 Patches must be installed upon database systems in accordance with the Patch Management Policy adopted by King AbdulAziz University.

3-3 The use of reliable, approved, and licensed database systems must be ensured.

3-4 The existence of a clear disaster recovery plan for database systems must be ensured.

3-5 King AbdulAziz University must sign and authorize level of service support agreements with suppliers pertaining to systems for database management in the production environment.

3-6 Fragmentation and encryption must be implemented on stored databases in accordance with the Classification Policy and the Cryptography Policy adopted by King AbdulAziz University.

4– Monitoring Events Logs for Database Systems

4-1 Events logs for database systems must be activated and maintained, in accordance with the Events Logs Management and Monitoring Policy adopted by King AbdulAziz University.

4-2 The Cyber-Security Center must monitor events logs for databases pertaining to critical systems, as well as user behavior.

4-3 The Cyber-Security Center must monitor events logs for database administrators, monitor their behavior, and review these logs periodically.

5– Operational Requirements

5-1 The necessary requirements for operating databases must be fulfilled and provided in a secure and appropriate manner, such as providing a safe and secure environment and restricting physical access to systems, which may be granted only to authorized employees.

5-2 The Deanship of Information Technology must monitor operational database systems, and ensure the good quality of their performance, availability, the provision of adequate storage capacity, and the like.

5-3 Clock synchronization must be centrally-set, according to an accurate and reliable source, for all database systems. (ECC-2-3-3-4)

6– Other Requirements

6-1 Key Performance Indicators (KPI) must be employed to ensure continual development of database systems management.

6-2 The cyber-security requirements for database management must be reviewed yearly, at least, or in the event of changes 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 Systems and Database 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.