


King AbdulAziz University
Cyber-Security Center

Cryptography 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

<i>Objectives</i>	4
<i>Scope and Applicability of the Work</i>	5
<i>Policy Clauses</i>	5
<i>Roles and Responsibilities</i>	7
<i>Compliance with the Policy</i>	7

Objectives

The purpose of this policy is to provide and fulfill cyber-security requirements, based on best practices and standards, to ensure the proper and effective use of cryptography, so as to protect King AbdulAziz University electronic informational assets and to reduce internal and external cyber-risks and cyber-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 2-8-1 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 electronic informational assets, and applies to all King AbdulAziz University employees, including external entities and parties that interact with the University.

Policy Clauses

1-1 King AbdulAziz University must develop, document, and approve cryptography procedures and standards with reference to operational necessities and risk analysis for King AbdulAziz University, so as to bring the University's security level into conformity with the National Cryptography Standards promulgated by the National Cyber-Security Authority. These procedures must include approved cryptography solutions, the restrictions applied to them (technical and regulatory), their means of use, and mechanisms for issuing, disseminating, and restoring keys, as well as key backup management and key destruction procedures. (ECC-2-8-3-1)

1-2 Data must be encrypted during transmission and storage based on its level of classification, and according to King AbdulAziz University regulatory policies and procedures and the relevant legislative and regulatory requirements.

1-3 Up-to-date cryptography solutions, algorithms, keys, and devices must be employed, in accordance with the Authority's pronouncements on the matter. (CSCC-2-7-1-3)

1-4 All data pertaining to critical systems must be encrypted during transmission (data-in-transit). (CSCC-2-7-1-1)

1-5 All data pertaining to critical systems must be encrypted during storage (data-at-rest) at the level of files, databases, or specific columns within the database. (CSCC-2-7-1-2)

1-6 Roles and responsibilities relating to Key Management Infrastructure (KMI) must be defined and documented, for the following roles at a minimum:

1-6-1 The Keying Material Manager, an office considered to be occupied by the Director of the Cyber-Security Center.

1-6-2 Key Custodians, responsible for encryption key protection.

1-6-3 Certification Authorities (CAs), offices concerned with issuing certificates in such a way as to ensure that they are reliable and secure.

1-6-4 Registration Authorities (RAs), offices concerned with registering certificates in such a way as to ensure that they are reliable and secure.

2– Secure Use of Cryptography

2-1 All encryption solutions employed (including algorithms, programs, modules, libraries, and other encryption components) must be documented, assessed, and approved by the Cyber-Security Center prior to their implementation at King AbdulAziz University.

2-2 The implementation of encryption in accordance with the cryptography solutions approved by King AbdulAziz University must be ensured.

2-3 The use of internally-developed encryption algorithms is prohibited, in accordance with the cryptographic guide of the Open Web Application Security Project.

2-4 Secure verification methods (such as the use of public encryption keys, digital signatures, and digital certificates) must be employed to limit cyber-risks and in accordance with the cryptography solutions adopted by King AbdulAziz University.

2-5 User identity verification must be employed for the transfer of top secret data to external parties through the use of approved digital encryption certificates, and in accordance with the Data and Information Protection Policy adopted by King AbdulAziz University.

2-6 Multi-factor authentication methods must be used to verify user access privileges to critical systems, in accordance with the Data and Information Protection Policy adopted by King AbdulAziz University.

3– Encryption Key Management

3-1 The management of encryption keys must be secured by means of key lifecycle management operations, the proper and secure use of which must be ensured.

3-2 Encryption certificates for local services must be issued through certificate issuance offices within King AbdulAziz University, or by a reliable external office.

3-3 Private key information must be kept in a secure place (especially when used for electronic signatures), and unauthorized access to it, including by certificate issuance offices, must be prevented.

3-4 Technologies and techniques for protecting encryption keys during storage (in a tamper-resistant safe) must be provided.

3-5 Private keys must be protected and secured by means of passwords, or by storing them using secure media, in accordance with the approved cryptography procedures.

3-6 Private encryption keys must be classified as containing “top secret” information, in accordance with the Data Classification Policy adopted by King AbdulAziz University.

3-7 Events logs for encryption key management solutions must be activated and periodically monitored.

3-8 Encryption key use periods, creation dates, and expiration dates must be specified for all keys.

3-9 Encryption keys must be renewed prior to their expiration.

3-10 Up-to-date encryption certificate revocation lists must be employed, to ensure that encryption certificates that have expired or that have been subjected to security breaches are not used in future operations.

3-11 In the event that a private encryption key used by King AbdulAziz University is subjected to a security breach, or in the event that a key is not available (due to damage of key storage media), the certification office must be notified immediately to cancel and re-issue the private encryption key.

3-12 The certification issuance office must be required, in the event that private encryption keys are subjected to security breaches, to inform King AbdulAziz University, to immediately revoke all certificates, and to replace the certificate issuance office’s key.

3-13 In the event that it is not possible to replace keys in a secure and reliable manner over telecommunications networks, encryption keys must be sent using alternative secure and independent channels (out-of-band channels).

3-14 Cryptographic key length requirements must be reviewed and updated based on the latest technical requirements once a year at least, and in accordance with national cryptography standards.

3-15 Key Custodians are the responsible administrators for protecting encryption keys, and are solely responsible for replacing keys when to do so is necessary.

3-16 It is forbidden to save keys on the primary memory, or on the same systems to which the encryption they represent is applied. Instead, it is advised to save encryption keys on peripheral hardware devices, such as hardware security modules (HSM), key loader systems, or any other device intended for this purpose.

4– Other Requirements

4-1 Key Performance Indicators (KPI) must be employed to ensure the continual development of the proper and effective use of cryptography.

4-2 All cyber-security requirements pertaining to cryptography must be reviewed periodically. (ECC-2-8-4)

4-3 This policy must be reviewed at least once a year.

5– Policy Review and Application Clause

1-1 Cyber-security requirements and the implementation 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 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.