King AbdulAziz University
Cyber-Security Center

Email 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 4

Scope and Applicability of the Work 4

Policy Clauses 4

Roles and Responsibilities 5

Compliance with the Policy 5

Objectives

The purpose of this document is to provide and fulfill cyber-security requirements, based on best practices and standards, relating to the protection of King AbdulAziz University email from internal and external cyber-risks and cyber-threats, through focus on the essential objectives of security, which are: Confidentiality, integrity, and availability of information.

This policy aims to comply with the relevant cyber-security requirements and legislative and regulatory requirements, which is itself a legislative requirement expressed in Control 2-4-1 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 email systems, and applies to all King AbdulAziz University employees.

Policy Clauses

1– Modern technologies and techniques must be provided to protect email, to analyze and filter email messages, and to block suspicious messages, such as spam emails and phishing emails.

2– Email systems must employ linked user identification numbers and passwords to ensure the isolation of communications of different users.

3– The technology necessary for encrypting email messages that contain classified information must be provided.

4– The multi-factor authentication feature must be applied for remote login and login via the webmail site webpage.

5– Email messages must be archived and backed up periodically.

6– Responsibility for email messages must be specified for generic and shared accounts.

7– The technologies necessary for protection from viruses and previously-unknown malware (zero-day protection) must be provided for email servers, and the scanning of messages prior to their arrival in email inboxes must be ensured.

8– The King AbdulAziz University email domain must be documented using the necessary means, such as Sender Policy Framework, to prevent email spoofing. It is also necessary to document incoming email message domains (incoming message DMARC verification).

9– Access to email messages must be limited to King AbdulAziz University employees.

10– The necessary measures must be taken to prevent the use of King AbdulAziz University email for purposes other than work.

11– The System Administrator may not access the email information pertaining to any member of staff without obtaining prior authorization.

12– The size of file attachments to ingoing and outgoing email and the volume of email storage must be determined for each user. Efforts to limit the ability to send group messages to large numbers of users must also be made.

13– Email messages sent out from King AbdulAziz University must have a notice disclaiming responsibility appended to them.

14– The necessary technologies and techniques must be applied to protect the confidentiality and integrity of email and its availability during transmission and storage, including the use of encryption and data-theft prevention techniques.

15– Key Performance Indicators (KPI) must be used to ensure the continual development of the email system.

16– The Open Mail Relay forwarding of email must be disabled at the server level.

17– Email cyber-security requirements and their application 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 Website 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.