King AbdulAziz University
Cyber-Security Center

Cyber-Security Policy for Physical Security

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, based on best practices, to ensure that cyber-security risks and requirements relating to physical security at King AbdulAziz University are effectively addressed.

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 2-14-1 of the Essential Cyber-Security Controls (ECC-1:2018) promulgated by the National Cyber-Security Authority. The authorities have required the protection of informational and technical assets from unauthorized access, loss, theft, and sabotage, so as to ensure effectively the integrity, availability, and protection of information and data.

Scope and Applicability of the Work

This policy covers all King AbdulAziz University information systems, assets, equipment, and devices, and applies to all King AbdulAziz University employees.

Policy Clauses

1– Cyber-security requirements pertaining to the protection of informational and technical assets from unauthorized physical access must be defined, documented, and approved, and must include at a minimum the following:

1-1 Control over access to critical sites, such as data centers, recovery centers, information processing sites, monitoring sites, network communication rooms, and device and technical component supply areas.

1-2 Monitoring and review of entry and exit records, such as CCTV recordings.

1-3 Protection of records and information sources from unauthorized access.

1-4 Securing, destroying, and reusing physical assets that contain classified information, including paper documents and saving and storage media.

1-5 Securing devices and equipment both inside and outside of buildings.

1-6 Developing and implementing emergency response procedures and University building and facility evacuation plans, in anticipation of any suspected or actual physical or environmental accidents.

1-7 Preventing the introduction of dangerous liquids or substances to critical sites.

1-8 Controlling the temperature of critical sites to maintain the efficiency of systems.

1-9 Preventing unauthorized individuals to access classified halls and rooms, with authorization being granted on the basis of the “need-to-know” and “minimum privileges” principles.

1-10 Regular maintenance of devices inside and outside of buildings.

2– Controls for protecting audio, communications, network, and power cables must be implemented, subsequent to study of potential risks. These controls must also cover the following, at a minimum:

2-1 Protection of communications and data network cables from wiretapping.

2-2 Not extending communications and data network cables through areas in which external parties could potentially access them.

2-3 Efficient protection and isolation of communications and data network cables from harm and unauthorized interception, and ensuring that they are extended through safe and protected areas.

2-4 Isolation of electricity and power cables from communications and data network cables.

2-5 Use of multiple and uninterrupted power sources to support continuity of operations for critical systems and facilities (such as data centers).

3– Physical security risk assessments must be carried out by the offices responsible for physical security in order to analyze the physical environment and surrounding areas, so as to monitor security threats and safety threats and identify and address weak points, to protect information assets from being subjected to threats.

4– The Deanship of Information Technology, together with the General Office for Educational Affairs, must develop and adopt regulations and procedures for physical safety and security at King AbdulAziz University and for any events or activities in which the University participates in organizing. These must include a strict and accurate delineation of duties and tasks, to serve as a general framework for safety, prevention, rescue, firefighting, and first aid services, as well as a guide concerning the protection of lives, assets, and information.

5– Security scans and attendance inspections for classified meetings must be carried out, for which purpose metal and dangerous substance detection devices must be provided.

6– All office facilities must be classified on the basis of the classification of the information circulated and processed within them.

7– External parties must not be granted physical access privileges to office facilities until security requirements have been fulfilled; their access must be monitored, and escorts must be provided for them where required.

8– Administrative privileges to physical access systems must be restricted to individuals with specific privileges that can be assessed and reviewed.

9– Review and updating of physical access privileges to critical areas must be carried out periodically.

10– Office staff must be instructed concerning best practices relating to physical security, such as the Clean Desk Policy, and their compliance with them must be ensured.

11– Key Performance Indicators must be used to ensure continual development of cyber-security requirements for physical security.

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, with the assistance of the General Office for Educational Affairs.

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.