


King AbdulAziz University
Cyber-Security Center

General Cyber-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	Khalid ibn Atiyyah Allah al-Subhi	
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>	<i>4</i>
<i>Scope and Applicability of the Work.....</i>	<i>4</i>
<i>Elements of the Policy.....</i>	<i>4</i>
<i>Roles and Responsibilities.....</i>	<i>8</i>
<i>Compliance with the Policy.....</i>	<i>9</i>
<i>Exceptions.....</i>	<i>9</i>

Objectives

The objective of this policy is to provide and fulfill cyber-security requirements, based on best practices and standards, relating to the documentation of cyber-security requirements and King AbdulAziz University's compliance with them, so as to reduce cyber-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 the regulatory operations requirements pertaining to King AbdulAziz University and relevant legislative and regulatory requirements, which is itself a regulatory requirement expressed in Control 1-3-1 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 informational and technical assets of King AbdulAziz University, and applies to all King AbdulAziz University employees.

This policy represents the main driver behind all cyber-security policies, procedures, and standards pertaining to various subjects, and also is one of the inputs for internal operations at King AbdulAziz University, such as human resources operations, supplier management operations, project management operations, and change management operations, among others.

Elements of the Policy

1– The Cyber-Security Center must define cyber-security standards, and document its policies, programs, and plans, based on the results of risk-assessments, in a way that ensures the publication of cyber-security requirements and the compliance of King AbdulAziz University with them, and in accordance with the regulatory operational requirements of King AbdulAziz University and relevant legislative and regulatory requirements, subject to approval by King AbdulAziz University. King AbdulAziz University employees whom this policy affects and relevant parties must be informed concerning it.

2– The Cyber-Security Center must develop and apply cyber-security policies, programs, standards, as represented in the following clauses:

2-1 The Cyber-Security Strategy, as a requirement of Control 1-1:

To ensure cyber-security action plans, objectives, initiatives, and projects and their effectiveness in realizing the legislative and regulatory requirements relevant to King AbdulAziz University.

2-2 Cyber-Security Roles and Responsibilities, as a requirement of Control 1-4:

To ensure that tasks and responsibilities are clearly defined for all participating parties as they concern the application of the Cyber-Security Controls at King AbdulAziz University.

2-3 Cyber-Security Risk-Management, as a requirement of Control 1-5:

The field of cyber-security includes the ensuring of cyber-security risk-management in a systematic manner, aiming at the protection of informational and technical assets, in accordance with King AbdulAziz University, the University's regulatory procedures, and the relevant legislative and regulatory requirements.

Inclusive of: (Risk-Management Policy; Risk-Management Guidelines).

2-4 Cyber-Security in Information Technology Projects, as a requirement of Control 1-6:

To ensure that cyber-security requirements are included in King AbdulAziz University project management methodology and procedures to protect the confidentiality of information, as well as to ensure the integrity of King AbdulAziz University informational and technical assets and their accuracy and availability, and also to ensure the application of cyber-security standards in application development operations and programs, in accordance with University regulatory policies and procedures and relevant legislative and regulatory requirements.

Inclusive of: (Configuration and Fortification Policy; Standards for the Secure Development of Applications; the Project Management Plan; Change Management Process).

2-5 Cyber-Security Legislative, Regulatory, and Standards Compliance as a requirement of Control 1-7:

To ensure that the Cyber-Security Program at King AbdulAziz University is in accordance with the relevant legislative and regulatory requirements.

Inclusive of: (Cyber-Security Legislative, Regulatory, and Standards Compliance Policy).

2-6 Periodical Cyber-Security Assessment and Audit as a requirement of Control 1-8:

To ensure that King AbdulAziz University cyber-security controls are applied and operate in accordance with the regulatory policies and procedures of the University, the relevant national legislative and regulatory requirements, and international requirements regulatorily-approved by King AbdulAziz University.

Inclusive of: (Periodical Cyber-Security Assessment and Audit Policy; Periodical Cyber-Security Assessment and Audit Plan).

2-7 Cyber-Security in Human Resources as a requirement of Control 1-9:

To ensure that cyber-security risks and requirements related to employees (staff and contractors) at King AbdulAziz University are addressed prior to, during, and at the end of their employment, in accordance with the University's regulatory policies and procedures and the relevant legislative and regulatory requirements.

Inclusive of: (Human Resources Cyber-Security Policy; Cyber-Security Standards for Human Resources).

2-8 Cyber-Security Awareness and Training Program as a requirement of Control 1-10:

To ensure that King AbdulAziz University employees have the necessary security awareness, and are aware of their responsibilities in the field of cyber-security, while ensuring University employees are provided with the required skills, qualifications, and training courses in the field of cyber-security, in order to protect the University's informational and technical assets, and to carry out their responsibilities in regard to cyber-security.

Inclusive of: (Cyber-Security Awareness and Training Plan).

2-9 Asset Management as a requirement of Control 1-2:

To ensure that King AbdulAziz University has an accurate and up-to-date inventory of assets that includes the details of all informational and technical assets available to the University, in order to support the University's operational processes and cyber-security requirements, so as to achieve the confidentiality, integrity, accuracy, and availability of the University's informational and technical assets.

Inclusive of: (Assets Management Policy; Acceptable Use of Assets Policy).

2-10 Identity and Access Management as a requirement of Control 2-2:

To ensure the cyber-security protection of logical access to the informational and technical assets of King AbdulAziz University, in order to prevent unauthorized access, and to restrict access beyond what is necessary to accomplish University-related work.

Inclusive of: (Identity and Access Management Policy).

2-11 Information System and Processing Facilities Protection as a requirement of Control 2-3:

To ensure the protection of systems, information processing facilities, including user devices, and University infrastructure from cyber-risks.

Inclusive of: (Server Security Policy; Database Security Policy; User Devices, Mobile Devices, and Personal Devices Policy; Patches Policy; Protection from Malware Policy; Server Security Standards; Database Security Standards; User Devices Security Standards; Protection from Malware Standards).

2-12 Email Protection as a requirement of Control 2-4:

To ensure the protection of King AbdulAziz University email from cyber-risks.

Inclusive of: (Email Security Policy; Email Protection Standards).

2-13 Networks Security Management as a requirement of Control 2-5:

To ensure the protection of King AbdulAziz University networks from cyber-risks.

Inclusive of: (Networks Security Policy; Networks Security Standards; Secure Wireless Networks Standards).

2-14 Mobile Devices Security as a requirement of Control 2-6:

To ensure the protection of King AbdulAziz University mobile devices (including mobile computing devices, smart phones, and smart tablets) from cyber-risks, and to ensure the safe handling and protection of sensitive information and information pertaining to the work of King AbdulAziz University, during transfer and storage, and in the use of University employees' personal devices (BYOD principle).

Inclusive of: (Mobile Device Security Standards).

2-15 Data and Information Protection as a requirement of Control 2-7:

To ensure the protection of confidentiality, integrity, accuracy, and availability of King AbdulAziz University data and information, in accordance with the University's regulatory policies and procedures and relevant legislative and regulatory requirements.

Inclusive of: (Privacy and Personal Data Protection Policy).

2-16 Cryptography as a requirement of Control 2-8:

To ensure proper and effective use of cryptography, to protect King AbdulAziz University informational assets, in accordance with the University's regulatory policies and procedures relevant legislative and regulatory requirements.

Inclusive of: (Cryptography Policy, Cryptography Standards).

2-17 Backup and Recovery Management as a requirement of Control 2-9:

To ensure the protection of King AbdulAziz University data and information, and also the technical settings of University systems and applications from harms arising from cyber-risks, in accordance with the University's regulatory policies and procedures and relevant legislative and regulatory requirements.

Inclusive of: (Backup and Recovery Policy).

2-18 Vulnerabilities Management as a requirement of Control 2-10:

To ensure that technical vulnerabilities are discovered in a timely manner and addressed effectively, so as to prevent and reduce the possibility that such vulnerabilities will be exploited by cyber-attacks, and also to reduce resulting effects on King AbdulAziz University operations. Inclusive of: (Vulnerabilities Management Policy; Vulnerabilities Management Standards).

2-19 Penetration Testing as a requirement of Control 2-11:

To assess the extent and test the effectiveness of capabilities for enhancing cyber-security at King AbdulAziz University, by simulating actual cyber-attack techniques and approaches, and to locate unrecognized points of security weakness which could lead to cyber-penetration of the University, in accordance with relevant legislative and regulatory requirements.

Inclusive of: (Penetration Testing Policy; Penetration Testing Standards; Penetration Testing Plan).

2-20 Cyber-Security Event Logs and Monitoring Management as a requirement of Control 2-12:

To ensure the collection, analysis, and monitoring of cyber-security event logs in a timely manner, for the purpose of proactive discovery of cyber-attacks, and to manage effectively their risks, so as to prevent or reduce potential negative effects upon King AbdulAziz University operations.

Inclusive of: (Cyber-Security Event Logs and Monitoring Management Policy; Cyber-Security Event Logs and Monitoring Management Standards).

2-21 Cyber-Security Event and Threat Management as a requirement of Control 2-13:

To ensure the discovery, identification, and effective management of cyber-security events in a timely manner, and to deal with cyber-security threats proactively, in order to prevent or reduce negative effects upon King AbdulAziz University operations, taking into account the provisions of Noble Royal Decree no. 37140, dated 14/8/1438 AH.

Inclusive of: (Cyber-Security Event and Threat Management Policy; Cyber-Security Event and Threat Management Standards; Cyber-Security Event Response Plan; Cyber-Security Event Recovery Plan).

2-22 Physical Security as a requirement of Control 2-14:

To ensure the protection of King AbdulAziz University technical and informational assets from unauthorized physical access, loss, theft, and sabotage.

Inclusive of: (Cyber-Security Physical Security Policy).

2-23 Web Application Security as a requirement of Control 2-15:

To ensure the protection of web applications internal and external to King AbdulAziz University from cyber-risks.

Inclusive of: (Web Application Security Policy; Web Application Security Standards).

2-24 Cyber-Security Resilience in Operations Continuity Management as a requirement of Control 3-1:

To ensure the availability of cyber-security resilience requirements in King AbdulAziz University operations continuity management, and to ensure that effects upon the University's critical electronic services and information processing systems and devices caused by disturbances resulting from catastrophic events induced by cyber-risks are addressed and reduced.

Inclusive of: (Cyber-Security Operations Continuity Policy; Service Availability Management Policy; Crisis Management Policy; Disaster Recovery Policy).

2-25 Third-Party and Cloud Computing Cyber-Security as a requirement of Control 1-4:

To ensure the protection of King AbdulAziz University assets from cyber-security risks relating to third parties (including information technology outsourcing services and managed services), in accordance with the University's regulatory policies and procedures and relevant legislative and regulatory requirements.

Inclusive of: (External Party Policy; Cloud Computing Cyber-Security Policy).

2-26 Cloud Computing and Hosting Cyber-Security as a requirement of Control 4-2:

To ensure that cloud computing and hosting cyber-risks are addressed and cloud-hosting cyber-security requirements are implemented in an appropriate and effective manner, in accordance with the regulatory policies and procedures of King AbdulAziz University and relevant legislative and regulatory requirements, orders, and decisions, and to ensure the protection of King AbdulAziz University informational and technical assets maintained on cloud computing services that are hosted, processed, or managed by third parties.

Inclusive of: (Cloud Computing and Hosting Cyber-Security Policy).

3– The Cyber-Security Center has the right to access information and to collect evidence necessary for ensuring compliance with relevant legislative and regulatory requirements relating to cyber-security.

Roles and Responsibilities

1– The following list represents the set of roles and responsibilities necessary for the approval and implementation of and compliance with the Cyber-Security Policies, Procedures, Standards, and Programs:

1-1 The responsibilities of the President of the University, being the Responsible Authority, or his deputy, are, for example:

1-1-1 Establishment of the Supervisory Committee for Cyber-Security, one of the members of which is the Director of the Cyber-Security Center.

1-2 The responsibilities of the General Office for Legal Affairs are, for example:

1-2-1 Ensuring that cyber-security and Non-Disclosure Agreement conditions and responsibilities contained in King AbdulAziz University employment and external party contracts are legally binding.

1-3 The responsibilities of the Deanship for Quality and Information Technology are, for example:

1-3-1 Reviewing the Cyber-Security Controls and auditing their application in accordance with generally accepted standards for assessment and audit and relevant legislative and regulatory requirements.

1-4 The responsibilities of the General Office of Human Resources are, for example:

1-4-1 Application of cyber-security requirements relating to King AbdulAziz University employees.

1-5 The responsibilities of the Cyber-Security Center are, for example:

1-5-1 Obtaining the approval of the President of King AbdulAziz University or his deputy for the Cyber-Security Policies, ensuring that the parties the Policies concern are aware of them and apply them, and periodic review and updating of the Policies.

1-6 The responsibilities of the heads of other offices are, for example:

1-6-1 Supporting the Cyber-Security Policies, Procedures, Standards, and Programs, and providing the necessary resources, so as to achieve the desired objectives in a way that serves the general interest of King AbdulAziz University.

1-7 The responsibilities of employees are, for example:

1-7-1 Understanding of and compliance with the cyber-security requirements that relate to employees of King AbdulAziz University.

Compliance with the Policy

1– The Responsible Authority of King AbdulAziz University must ensure compliance with the Cyber-Security Policy and Standards.

2– The Director of the Cyber-Security Center must ensure the compliance of King AbdulAziz University with the Cyber-Security Policies and Standards on a periodic basis.

3– All King AbdulAziz University employees must comply with this policy.

4– Any violation of policies relating to cyber-security may subject the offender to disciplinary action, in accordance with the procedures followed by King AbdulAziz University.

Exceptions

It is forbidden to disregard the Cyber-Security Policies and Standards without obtaining prior permission from the Director of the Cyber-Security Center of the Supervisory Committee for Cyber-Security, unless to do so would conflict with relevant legislative and regulatory requirements.