


King AbdulAziz University  
Cyber-Security Center

## **Cyber-Security Incident and Threat Management 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	Sultana bint Ahmad al-Ghamadi	In accordance with the requirements of the Authority

## Table of Contents

<b><i>Objectives</i></b> .....	<b>4</b>
<b><i>Scope and Applicability of the Work</i></b> .....	<b>4</b>
<b><i>Policy Clauses</i></b> .....	<b>4</b>
<b><i>Roles and Responsibilities</i></b> .....	<b>7</b>
<b><i>Compliance with the Policy</i></b> .....	<b>8</b>

## Objectives

The purpose of this policy is to provide and fulfill cyber-security requirements, based on best practices and standards, for cyber-security incident and threat management pertaining to King AbdulAziz University, in order to reduce cyber-threats 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 2-13-1 of the Essential Cyber-Security Controls promulgated by the National Cyber-Security Authority.

## Scope and Applicability of the Work

This policy covers all King AbdulAziz University technical and informational assets, and applies to all King AbdulAziz University employees.

## Policy Clauses

### 1– General Clauses

1-1 King AbdulAziz University must provide the technologies necessary to identify and detect cyber-security incidents in a timely manner, or to receive reports submitted by King AbdulAziz University employees, or beneficiaries or administrators of King AbdulAziz University services, in an effective manner.

1-2 King AbdulAziz University must address cyber-security threats proactively, with reliance upon preventive means of defense, in order to forestall or reduce related impacts upon the confidentiality, integrity, and availability of information.

1-3 Cyber-security incidents include, but are not limited to, the following examples:

1-3-1 Unauthorized changes to user desktop and/or mobile device settings, and changes to server settings.

1-3-2 Infection with malware.

1-3-3 Changes to applications in terms of appearance (unusual appearance) and modifications to user privileges, such as raising levels of access.

1-3-4 Unauthorized access to data, and/or modifications made without user permissions or privileges.

1-3-5 Attempts to obtain information that could be used to carry out attacks, such as network port scans, social engineering attacks, targeted scans across IP range, etc.

1-3-6 Unauthorized activation of suspended or deleted user accounts.

1-4 An incident-response plan that explains procedures for addressing cyber-security incidents, the roles and responsibilities of the response team, privileges for taking important decisions, and means for communication with internal and external parties, as well as escalation mechanisms, must be documented and approved.

1-5 In the event that a cyber-security incident is detected at King AbdulAziz University, the incident-response team must take the steps necessary to immediately address the detected incident, including analysis of the incident data and identification of its effects.

1-6 In the event that a cyber-security incident is detected, the relevant available information must be analyzed, such as system and network logs and logs from relevant security products (such as logs from anti-malware solutions, firewalls, and advanced intrusion detection and prevention defense systems).

1-7 The necessary evidence must be processed (for example, evidence-gathering in accordance with legal restrictions and protected from tampering), documented, and maintained in a protected manner, such that it does not lose its usefulness for analysis, and then analysis must be carried out in such a way that the evidence is not destroyed or does not lose its original form.

1-8 In the event that a cyber-security incident occurs, the reasons for the incident must be investigated, and input should be requested from specialists, such as digital forensics analysts and cyber-incident response teams.

1-9 The Incident Response Plan must be reviewed at least once yearly.

1-10 Cyber-security incidents must be classified based on their level of severity and the extent of their effects upon King AbdulAziz University operations. (ECC-2-13-3-2)

1-11 Cyber-security incidents must be classified in accordance with the table below:

Table 1: Classification of cyber-incidents

Risk Level	Description	Targeted Response Time	Targeted Resolution Time
<b>Seriously Elevated</b>	Serious damage that directly affects the reputation and credibility of King AbdulAziz University, or that affects numerous functional operations units or the operations site in a significant way, such that the activation of operational continuity procedures is required.	Immediately	Two hours
<b>Elevated</b>	Major interruptions of service that affect functional operations units or primary services or sites	3 hours	6 hours
<b>Moderate</b>	Moderate impact upon the workflow of functional operations units, sites, or information technology assets, in addition to medium-to-high impact upon non-significant King AbdulAziz University operations units	5 hours	10 hours

Risk Level	Description	Targeted Response Time	Targeted Resolution Time
Low	Limited impacts upon small numbers of resources whose effects can be sustained for a certain period of time	7 hours	24 hours

## 2– Cyber-Security Incidents Reporting

2-1 The levels of security awareness of King AbdulAziz University employees must be raised, and their responsibilities with regard to cyber-security incidents must be explained and clarified, so that they will be able to give immediate reports of any cyber-security incidents or threats.

2-2 King AbdulAziz University must identify an internal contact point for incident reports, whether by means of telephone or email.

2-3 King AbdulAziz University must specify the incidents and threats that must be reported, the time within which they must be reported, and the parties to whom they must be reported, such as the University Director, the Director of the Cyber-Security Center, the King AbdulAziz University Incidents Response Team, and the responsible administrators of technical and informational assets.

2-4 Prior to the disclosure to external parties of any information relating to cyber-incidents, the necessary permissions must be obtained, in accordance with the relevant legislative and regulatory requirements.

2-5 Reports concerning cyber-security incidents must be made to the National Cyber-Security Authority. (ECC-2-13-3-3)

2-6 King AbdulAziz University must inform the National Cyber-Security Authority concerning incident reports and indicators and reports of violations. (ECC-2-13-3-4)

## 3– Cyber-Security Event Response and Recovery

3-1 The Incident Response Unit of the Cyber-Security Center must compose detailed reports concerning cyber-security incidents, which must include the type and category of the incident, the parties who reported the incident or the instruments used to detect it, the services or assets that were affected by it, how the incident was discovered, and any other documents or resources related to the incident.

3-2 Suppliers must be involved in resolving incidents or restoring services when necessary.

3-3 Procedures for cyber-security incident recovery must include the identification of the vulnerabilities that were exploited in the course of the incident, and the technical and administrative measures used in addressing it, such as the following examples:

3-3-1 Application of compensating security controls.

3-3-2 Installation of up-to-date update and repair patches.

3-3-3 Restoration of system backup versions.

3-3-4 Resetting of system security settings, such as the firewall system and penetration detection systems.

3-4 The Cyber-Security Center must maintain incident reports (which must include information concerning security penetrations and incidents, such as information relating to the individuals, offices, and systems involved and/or attack methods) in a secure and access-restricted place.

3-5 Incident escalation is required in the event that an incident is not resolved within the specified period, according to the incident classification, the procedures for addressing it, and the approved escalation mechanism.

3-6 The change management procedures approved by King AbdulAziz University must be complied with in the event that dealing with a cyber-incident requires changes to be made to technical components.

3-7 After dealing with an incident, the Incidents Response Team at the Cyber-Security Center must hold meetings to discuss the “lessons learned” with the relevant offices, so as to improve approaches to addressing cyber-security incidents in the future, and also to address cyber-security threats in a proactive manner, in order to forestall or reduce the effects consequent upon them for King AbdulAziz University operations.

#### **4– Threat Intelligence**

4-1 Collaboration must be had with providers of threat intelligence in order to maintain continuous awareness of cyber-security incidents and threats, and to deal with this information in a direct manner. (ECC-2-13-3-5)

4-2 Threat intelligence must be maintained and organized in flexible databases suitable for the formulation of operational notes and descriptive data regarding indicators, such as knowledge base software.

4-3 Advanced intrusion prevention and detection systems must be updated with threat intelligence, and these systems must be ensured to have the ability to detect and address threats in an effective manner.

#### **5– Other Requirements**

5-1 Cyber-security requirements pertaining to cyber-security incident and threat management must be reviewed periodically.

5-2 Key Performance Indicators (KPI) must be used to ensure the continual development of cyber-security incident and threat management.

5-3 This policy must be reviewed at least once a year.

## **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 on a continual basis.
- 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.