


King AbdulAziz University
Cyber-Security Center

Cyber-Security Events Logs and Monitoring Policy

Restricted-Internal

Document Authorization:

Role	Name	Date	Signature
Owner	Cyber-Security Center	14/11/2022	

Document Versions:

Version	Date	Editor	Reasons for Revision
1.0	15/11/2021 CE	Shuruq bint Khalid Banafi	
1.1	14/11/2022 CE	Nawf bint A'id al-Qarni	In accordance with the requirements of the Authority

Table of Contents

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

Objectives

The purpose of this policy is to provide and fulfill cyber-security requirements, based on best practices and standards, so as to reduce cyber-risks and to protect King AbdulAziz University assets from internal and external threats through the use of the Cyber-Security Events Log Management and Monitoring System.

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 1-12-2 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 AbdulAziz University systems for cyber-security events log management and monitoring, and applies to all King AbdulAziz University employees.

Policy Clauses

1– General Clauses

1-1 The necessary Security Information Event and Management (SIEM) technologies must be provided in order to gather cyber-event logs for informational assets, applications, systems, databases, networks, and protection systems at King AbdulAziz University. These logs must contain the following information as a minimal requirement:

- 1-1-1 Event type
- 1-1-2 Event location or system
- 1-1-3 Event time and date
- 1-1-4 User or user device used to carry out the event
- 1-1-5 Success vs. failure

2– Events to be Recorded

2-1 Systems to be monitored must activate event logs when an event occurs, at a minimum, as follows:

2-1-1 Event logs pertaining to cyber-security for all technical components of critical systems (operating systems, databases, data storage, applications, and networks).

2-1-2 Event logs pertaining to cyber-security for the production network and communications linked to it.

2-1-3 Event logs pertaining to accounts that have important and sensitive privileges over informational assets.

2-1-4 Event logs pertaining to browsing, connection to the Internet, and wireless networks.

2-1-5 Information transfer via external storage media.

2-1-6 Illegitimate changes made to logs and critical systems via File Integrity Management (FIM).

2-1-7 Changes to system, network, or servers' settings, including downloads of patches, or other changes to installed software.

2-1-8 Suspicious activities, such as activities discovered by the Intrusion Prevention System (IPS).

2-2 Security procedures and standards that apply best standards must be developed, so as to maintain event logs in a way that ensures their safety from modification, deletion, or unauthorized access.

2-3 Event logs must be monitored, and periodically analyzed in accordance with their classification, to include monitoring and analysis of the behavior of users of critical systems.

2-4 Centralized clock synchronization is required, with reference to an accurate and reliable source, for all systems being monitored.

2-5 Key Performance Indicators (KPI) must be used to ensure the continual development of the Cyber-Security Events Logs Management and Monitoring System.

2-6 Event logs must be archived and backed-up periodically.

2-7 The period for which cyber-event records are maintained must be at least 12 months, and at least 18 months for critical systems, in accordance with internal policies and relevant legislative and regulatory requirements.

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.