


King AbdulAziz University  
Cyber-Security Center

## **Patch Management 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	Ashwaq bint Samir Abd al-Jawad	In accordance with the requirements of the Authority and the addition of Control 2-10-3-4

## Table of Contents

<b><i>Objectives</i></b> .....	<b>4</b>
<b><i>Scope and Applicability of the Work</i></b> .....	<b>5</b>
<b><i>Policy Clauses</i></b> .....	<b>5</b>
<b><i>Roles and Responsibilities</i></b> .....	<b>6</b>
<b><i>Compliance with the Policy</i></b> .....	<b>6</b>

## Objectives

This policy aims to define cyber-security requirements, based on best practices and standards, relating to patch management for King AbdulAziz University systems, applications, databases, network devices, and information processing devices, so as to reduce cyber-risks and to protect the University from internal and external threats, through focus on the essential objectives of protections, which are: Confidentiality, integrity, and availability of information.

This policy follows national legislative and regulatory requirements and best international practices, which is itself a legislative requirement expressed in Control 3-3-3-3 and Control 2-10-3-4 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 systems, applications, databases, network devices, information processing devices, and industrial control devices and systems pertaining to King AbdulAziz University, and applies to all King AbdulAziz University employees.

## Policy Clauses

1– Patch management must be employed in such a way as to ensure the protection of systems, applications, databases, network devices, and information processing devices.

2– Patches must be downloaded from licensed and reliable sources, in accordance with the procedures followed within King AbdulAziz University.

3– Reliable and secure technical systems must be used to conduct periodic scans for vulnerabilities and patches, the implementation of which must be tracked.

4– The Deanship of Information Technology must test patches in the test environment prior to installing them upon systems, applications, and information processing devices in the production environment, to ensure the compatibility of patches with systems and applications.

5– A rollback plan must be put in place, and implemented in the event that patches have a negative impact upon the performance of systems, applications, or services.

6– The Supervisory Committee for Cyber-Security must ensure the implementation of patches on a periodic basis.

7– Priority must be given to patches that address security vulnerabilities according to the level of risk linked to them.

8– Patches must be scheduled corresponding to the phases of software releases offered by suppliers.

9– Patches must be installed at least once monthly for critical systems connected to the Internet, and once every three months for internal critical systems. (CSCC-2-3-1-3)

10– Patches must be installed onto technical assets along the following lines:

Asset Type	Frequency of Update Installation	
	Technical and Informational Assets	Technical and Informational Assets Pertaining to Critical Systems
Operations Systems	Monthly	Monthly
Databases	Every three months	Monthly
Network Devices	Every three months	Monthly
Applications	Every three months	Monthly

11– The patch management process must follow the change management process requirements.

12– In the event that high-risk security vulnerabilities are present, emergency patches must be installed in accordance with the emergency change management process.

13– Patches must be installed onto a centralized patch management server before their installation onto systems, applications, databases, network devices, and information processing devices, with the exception of patches for which supported automated tools are not available.

14– After patches are installed, independent and reliable tools must be used to ensure that vulnerabilities are effectively addressed.

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

16– The Patch Management Policy and procedures must be reviewed yearly, and changes must be documented and approved.

17– Cyber-security requirements and their implementation must be reviewed yearly.

## Roles and Responsibilities

–Responsible Party and Owner of the Document: 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.

## Compliance with the Policy

1– The Cyber-Security Center must ensure the compliance of King AbdulAziz University with this policy on a continual basis.

2– The Cyber-Security Center and the Deanship of Information Technology 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.