MANGAUNG
AT THE HEART OF IT ALL

CENTLEC
Reg No. 2003/011612/30

PATCH MANAGEMENT POLICY

DIRECTORATE: OFFICE OF THE CEO	
SUBJECT: PATCH MANAGEMENT POLICY	POLICY NO:
REV NO: 1	REV DATE: 10 May 2023
SUB-DIRECTORATE: Information Management	BOARD ITEM NO:
SIGNATURE:	
DATE APPROVED:	EFFECTIVE DATE: 01 July 2023

Definitions:

Patch: a piece of software designed to fix problems with or update a computer program or its supporting data

Trojan: a class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions

Virus: a computer program that can copy itself and infect a computer without the permission or knowledge of the owner.

Worm: a self-replicating computer program that uses a network to send copies of itself to other nodes.

CENTLEC (SOC) LTD – PATCH MANAGEMENT POLICY

1. OBJECTIVES

- To outline the requirements for maintaining up-to-date operating system security patches on all Centlec owned and managed workstations and servers.

2. POLICY PRINCIPLES

a) This policy applies to workstations or servers owned or managed by Centlec (SOC) Ltd. This includes systems that contain company or customer data owned or managed by Centlec regardless of location.

b) Workstations and servers owned by Centlec must have up-to-date operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by the entity.

3. WORKSTATIONS

Desktops and laptops (workstations) must have automatic updates enabled for operating system patches. This is the default configuration for all. Any exception in relation to this policy provision must be documented and approved by the ICT manager.

4. SERVERS

Servers must comply with the minimum baseline requirements that have been approved by ICT services. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the entity asset and the data that resides on the system. Any exception in relation to this policy provision must be documented and approved by the ICT manager.

5. ROLES AND RESPONSIBILITIES

The ICT section shall be responsible for manage the patching needs for all the servers owned or controlled by Centlec (SOC) Ltd as well as all workstations.
ICT administrator should control and install the patches progressively using any form of patch security software or servers
All users must ensure that they allow patch updates to be installed on to their computers as prompted on their screens.

The ICT manager shall be responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.

The Executive Manager: Engineering Retails shall be responsible for approving the monthly and emergency patch management deployment.

6. MONITORING AND REPORTING

The ICT shall establish security administrator who will be responsible for patch management activities. The security administrator will be responsible to compile and maintain reporting metrics that summarize the outcome of each patching cycle.

These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to both Internal and External Auditors upon request.

7. ENFORCEMENT

Implementation and enforcement of this policy is ultimately the responsibility of all employees at Centlec (SOC) Ltd during updated prompt by the updated server onto their screen. ICT services and Internal Audit may conduct random assessments to ensure compliance of the updates. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the appropriate internal register and support teams shall be dispatched to remedy the situation.

8. REVIEW AND APPROVAL

This policy and underlying strategies will be reviewed at least annually, or as necessary, to ensure its continued application and relevance.

Revised by:

Signed: 

Manager: Information Management

Date: 22/05/2023

Supported by:

Signed: 

Act Executive Manager: Engineering Retail

Date: 22/05/2023

Approved by:

Signed: 

Chief Executive Officer

Date: 22/05/2023