Patch Management Policy

CGICT_ICT_001

Version 1.1 July 2021

Version Control and Approval			
Document Name		Patch Management Policy	
Document Number/Version		1.1	
Status/Revision History			
Rev #	**Revision Update**	Revised By	Date
1.1	**Revised**	Mpumelelo Khumalo	July 2021
Approval			
Date Approved			
Date Last Amended		July 2021	
Date of Next Review		2023/24	
Related Policies		Patch Management Policy	
Authored By			
Name		Mr. Mpumelelo Khumalo	
Position		Acting ICT Manager	
Signature			Date: 30/03/2022
Reviewed and Recommended by			
Name		Ms. Sibongile Ngwenya	
Position		Executive Manager : Corporate Services	
Signature			Date: 30/03/2022
Name		Mr. Thamsanqa Mdontswa	
Position		Chief Executive Officer	
Signature			Date: 30/03/2022
Approved By			
Name		Ms. Portia Mushwana	
Position		Chairperson: ICT Steering Committee	
Signature			Date: 30/03/2022
Approved By			
Name		Mr. Chris Mudau	
Position		Chairperson : Board and Accounting Authority	
Signature			Date: 30/03/2022

Table of Contents

1 Introduction

SASSETA has a responsibility to uphold the confidentiality, integrity and availability of the data held on its ICT systems on and off site which includes systems and services supplied by third parties.

The organisation has an obligation to provide appropriate and adequate protection of all ICT assets whether it is ICT systems on premise, in the Cloud or outsourced systems and services supplied by third parties.

Effective implementation of this policy reduces the likelihood of compromise which may come from a malicious threat actor or threat source.

2 Purpose

This document describes the requirements for maintaining up-to-date operating system security patches, firmware and software version levels on all the organisation's electronic systems.

3 Definitions and Terms

Term/Acronym	Definition
Availability	Availability is the guarantee of reliable and constant access to data and information systems when required.
Confidentiality	The process followed to prevent unauthorised disclosure of information.
ICT System	Includes Workstations, Servers (physical and virtual), Firmware, Networks (including hardwired, Wi-Fi, switches, routers etc.), Hardware, Software (databases, platforms etc.), Applications, (including mobile apps), Cloud Services.
Integrity	Integrity assures that the data or information system can be trusted. Ensures that it is edited by only authorised persons and remains in its original state when at rest.
Patch	A patch is a set of changes to a computer program or software designed to update, fix, or improve it.
Risk	The potential for unauthorised use, disruption, modification or destruction of information because of a threat exploiting a vulnerability.
Third Party	External supplier of ICT Services to SASSETA.
Vulnerability	An unintended flaw or weakness in software code or a system that leaves it open to the potential for misuse and exploitation in the form

	of unauthorised access or malicious behaviour such as viruses, worms, Trojan horses, ransomware and other forms of malware.

4 Scope

This policy applies to:

- Workstations, servers, networks, hardware devices, mobile devices, software and applications owned and managed by SASSETA. This includes third parties supporting SASSETA ICT systems.
- Systems that contain company or customer/stakeholder data owned or managed by SASSETA ICT regardless of location. This includes third party suppliers.
- CCTV systems where recordings are backed up to the organisation's networks.
- Any access points for effecting payments utilising the organisation's networks.
- Third party suppliers of ICT systems as defined in Section 3.

5 Policy

- All ICT systems (as defined in section 3), either owned by SASSETA or those in the process of being developed and supported by third parties, must be manufacturer supported and have up-to-date and security patched operating systems and application software.
- Security patches must be installed to protect the assets from known vulnerabilities.
- Any patches categorised as 'Critical' or 'High risk' by the vendor must be installed within 14 days of release from the operating system or application vendor unless prevented by the organisation's ICT Change Control (CAB – Change Advisory Board) procedures.
- Where CAB procedures prevent the installation of 'Critical' or 'High risk' security patches within 14 days a temporary means of mitigation will be applied to reduce the risk.

    - **Workstations**
        - All desktops and laptops that are managed by SASSETA must meet the laptop and workstation minimum requirements specified by ICT. Any exceptions shall be documented and reported to the ICT Manager.

    - **Servers**
        - Servers must comply with the recommended minimum configuration which are specified by ICT which includes the default operating system level,

service packs, hotfixes and patching levels. Any exceptions shall be documented and reported to the ICT Manager.

Third Party Suppliers:

- Security patches must be up to date for ICT systems which are being designed and delivered by third party suppliers prior to deployment and going operational. Third party suppliers must be prepared to provide evidence of up-to-date patching before ICT systems are accepted into service and thus become operational.
- Once the ICT systems are operational the following patching timescales apply:
    - Critical or High-Risk vulnerabilities – 1-7 calendar days
    - Medium – 14 calendar days
    - Low – 30 calendar days

6 Roles and Responsibilities

- SASSETA ICT.
    - Will manage the patching needs for the Windows, Android, Apple Mac OS and Linux environments that is connected to the organisation's network.
    - Responsible for routinely assessing compliance with the patching policy and will provide guidance to all the stakeholder groups in relation to issues of security and patch management.
- Change Advisory Board.
    - Responsible for approving the monthly and emergency patch management deployment requests.
- End User.
    - The end user has a responsibility to ensure that patches are timeously installed and the machine is rebooted when required. Any problems must be reported to ICT.
- Third Parties.
    - Will ensure security patches must be up to date for ICT systems which are being designed and delivered by third parties prior to going operational.
    - Once the ICT systems are operational, third parties must ensure vulnerability patching is carried out as stipulated in Section 5 of this Policy. Where this is not possible, this must be escalated to the ICT Manager.

7 Monitoring and Reporting

Those with patching roles as detailed in section 6 above are required to compile and maintain reporting metrics that summarise 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 Internal Audit upon request.

8 Policy Review and Maintenance

The Policy will be reviewed and updated every second year, or as needed, to ensure that the policy remains aligned with changes to relevant laws, contractual obligations and best practice.

9 Policy Implementation

The ICT Business Unit and Corporate Services is accountable and shall also be responsible for its future amendments or reviews.

The CEO is accountable for the overall policy implementation and reserves the right to intervene and take necessary steps when the policy is not adhered to. The accountability may be delegated to the Corporate Services Executive or any other manager deemed fit for the function. Business Unit Heads, in consultation with ICT, are responsible for policy implementation in their respective divisions.

10 Non-Compliance to the Policy

The policy should be used in conjunction with the SASSETA Disciplinary Policy, where disciplinary action could be a consequence due to non-compliance.

11 Policy Validity

This policy will be effective from the date of approval. In an event of any doubt about the authenticity of a policy document, the document signed by the CEO shall be considered as the only document with validity, authority and a force of law.