



ICT PATCH MANAGEMENT POLICY

1 July 2024

TABLE OF CONTENTS

1. ABBREVIATIONS 2

2. PURPOSE OF THIS POLICY 3

3. LEGISLATIVE FRAMEWORK 4

4. USER AWARENESS..... 4

5. DOCUMENTS THAT SHOULD BE READ WITH THIS POLICY 5

6. SCOPE OF APPLICATION 5

7. ROLES AND RESPONSIBILITIES..... 6

8. WORKSTATIONS 7

9. ICT SERVERS 7

10. MONITORING AND REPORTING..... 8

11. EXCEPTIONS 8

12. ENFORCEMENT 8

13. BREACH OF POLICY 9

14. REVIEW OF POLICY 9

1. ABBREVIATIONS

“**SWDM**” refers to Swellendam Municipality.

“**ICT Services Division**” refers to Swellendam ICT Department and its staff members.

“**Site Manager**” refers to anyone appointed as the head of technical operations.

“**Manager ICT Services**” refers to the Head of the ICT Services Division

“**COBIT**” refers to Control Objectives for Information and Related Technology

“**ICT**” refers to Information and Communication Technology

“**ITIL**” refers to ICT Infrastructure Library

“**SIP**” refers to a Service Improvement Plan

“**CRF**” refers to Change Request Forms.

“**Email**” refers to electronic mail.

“**CFO**” refers to Director Financial Services.

“**HOD**” refers to the Manager or Head of Division.

“**IP**” refers to Internet Protocol

“**ISO**” refers to International Organization for Standardisation

2. PURPOSE OF THIS POLICY

- 2.1 The ICT Services Division has developed the ICT Information Security Controls Policy that shall apply to all SWDM officials, its contractors, service providers, interns, students, councillors; other authorized 3rd party entities, and every individual and/or organization and/or entity that will need the Municipality's ICT Infrastructure and Financial Systems to perform their respective duties at SWDM.
- 2.2 SWDM is responsible for ensuring the confidentiality, integrity, and availability of its data and that of customer data stored on its systems. SWDM must provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data entrusted to the system. Effective implementation of this policy will limit the exposure and effect of common system vulnerability threats to the systems within this scope.
- 2.3 The purpose of the policy is to present regulations that need to be adhered to by all departments as well as all individuals who use SWDM ICT Systems.
- 2.4 This policy directs the implementation of appropriate security measures to ensure that information and information systems are protected in a manner commensurate with their sensitivity, value, and criticality against a variety of risks/threats or vulnerabilities such as errors, fraud, theft, embezzlement, privacy, sabotage, violence, service interruption, inception, fabrication, modification, hardware failure, industrial espionage, viruses, and natural disasters.
- 2.5 The Patch Management policy will minimize the security threats such as interruption, interception, modification, and fabrication of the computing systems and financial systems. The policy describes the Information Technology Services requirements for maintaining up-to-date operating system security patches on all SWDM-owned and managed workstations and servers.

3. LEGISLATIVE FRAMEWORK

- 3.1 The policy was drafted bearing in mind the legislative conditions, as well as to leverage internationally recognized ICT standards. The following legislation, among others, was considered in the drafting of this policy:
- 3.1.1 Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
 - 3.1.2 Copyright Act, Act No. 98 of 1978;
 - 3.1.3 Electronic Communications and Transactions Act, Act No. 25 of 2002;
 - 3.1.4 Minimum Information Security Standards, as approved by Cabinet in 1996;
 - 3.1.5 Municipal Finance Management Act, Act No. 56 of 2003;
 - 3.1.6 Municipal Structures Act, Act No. 117 of 1998;
 - 3.1.7 Municipal Systems Act, Act No. 32, of 2000;
 - 3.1.8 Provincial Archives and Record Service of South Africa Act, Act No. 3 of 2005;
 - 3.1.9 Provincial Archives Regulations and Guidelines;
 - 3.1.10 Promotion of Access to Information Act, Act No. 2 of 2000;
 - 3.1.11 Protection of Personal Information Act, Act No. 4 of 2013;
 - 3.1.12 Regulation of Interception of Communications Act, Act No. 70 of 2002;
 - 3.1.13 Treasury Regulations for Departments, trading entities, constitutional institutions, and public entities, Regulation 17 of 2005;
 - 3.1.14 Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014;
 - 3.1.15 Control Objectives for Information Technology (COBIT) 5, 2012;
 - 3.1.16 ISO 27002:2013 Information technology — Security techniques Code of practice for information security controls;
 - 3.1.17 King IV - Code of Governance Principles.

4. USER AWARENESS

- 4.1 Every councillor, employee, contractor, and authorized 3rd party entity should become familiar with this Policy's provisions and the importance of adhering to it when effecting changes to SWDM ICT Infrastructure.

- 4.2 This policy will be sent using email to all users of ICT services and it is expected of all users to familiarize themselves with the contents and provisions of this policy.
- 4.3 The ICT Services Division must ensure that by requesting for changes to be effected and signing the change control form, this policy was read and understood.
- 4.4 Permanent Employees are to be provided with Information Security awareness tools to enhance awareness and educate them regarding the range of threats and the appropriate safeguards;
- 4.5 An appropriate summary of the Information Security Policies must be formally delivered to, and accepted by, all temporary Employees before they started any work for the SWDM;
- 4.6 The Municipality is committed to providing regular and relevant Information Security awareness communications to all Employees by various means, such as electronic updates, briefings, newsletters, etc.;
- 4.7 All Employees are to receive Information Security awareness training. The Information Policy must form part of all employees' induction conducted by the SWDM.

5. DOCUMENTS THAT SHOULD BE READ WITH THIS POLICY

- 5.1 ICT Standard Operating Procedure.
- 5.2 ICT User and Network Access Policy.
- 5.3 SWDM Asset Management Policy.
- 5.4 ICT Remote Access Policy.
- 5.5 ICT Data Backup and Recovery Policies.
- 5.6 ICT Security Control Policy

6. SCOPE OF APPLICATION

- 6.1 The scope of this policy covers any ICT-related equipment or asset and includes and is not limited to software (Financials, GIS, OS, Utility, drivers, patches, updates, upgrades, service packs), hardware (servers, printers, desktops, laptops, scanners, 3Gs, etc), applications (office, adobe, etc), documents, plans and procedures relevant to the running, support, and maintenance of ICT Systems and Services.

- 6.2 This policy shall apply to all employees of SWDM, and any other person or system granted permission to use the ICT Infrastructure and Financial Systems of SWDM.
- 6.3 The following systems have been categorized according to management:
 - 6.3.1 Microsoft Windows servers
 - 6.3.2 Workstations (desktops and laptops)

7. ROLES AND RESPONSIBILITIES

- 7.1 All SWDM ICT Services Division are responsible to make sure that they are providing access and effect changes in compliance with the Municipality's ICT Information Security Policy. It is the responsibility of every user of ICT Infrastructure to ensure adherence to this Information Security Policy.
- 7.2 SWDM ICT Services is responsible for informing users of prospective changes that affect them through email and their Directors and/or Managers whichever is applicable or both.
- 7.3 No Employee may tamper with any security settings on any computer that may endanger the SWDM, including but not limited to the removal of screen-savers, removal of anti-virus software, etc;
- 7.4 Confidential Information should be shared only with other authorized persons in terms of POPIA;
- 7.5 Following is a list of responsibilities for software patch management:
 - 7.5.1 The ICT Manager will manage the patching needs for all the financial servers on the network.
 - 7.5.2 The ICT Service Provider will manage the patching needs for the Microsoft Windows servers on the network.
 - 7.5.3 The ICT Server Administrators will manage the patching needs of all workstations on the network.
 - 7.5.4 The ICT Manager will manage the updating and patching needs of all workstations and servers installed with the antivirus system on the network.

- 7.5.5 The ICT Manager will be responsible for approving the major and emergency patch management deployment requests, requested through Change Management Process.

8. WORKSTATIONS

- 8.1 Workstations and servers owned by SWDM must have up-to-date (as defined by ICT's minimum baseline standards) operating system security patches installed to protect the information assets from known vulnerabilities. This includes all laptops, desktops, and servers owned and/or managed by SWDM.
- 8.2 Desktops and laptops may have automatic updates enabled for operating system patches. This can be the default configuration for all workstations built by SWDM. Any exception to the policy must be documented and forwarded to the ICT for review. These changes must follow a change management procedure of SWDM.
- 8.3 Should it be noted that any desktop and laptop update does not run automatically the ICT Services Department may manually run the updates and enable and test that updates run automatically.

9. ICT SERVERS

- 9.1 Servers must comply with the minimum baseline requirements that have been approved by ICT. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the ICT information assets and the data that resides on the systems.
- 9.2 The ICT Manager must check and install firewall upgrades and patches on a weekly basis. An obsolete firewall (one that is not supported by the vendor any longer and/or has known security vulnerabilities) must be replaced.
- 9.3 Any exception to the policy must be documented and forwarded to ICT for review.

10. MONITORING AND REPORTING

- 10.1 Active patching teams noted in the Roles and Responsibility section (7) are required 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 Internal Audit and Management upon request.
- 10.2 Internal Audit and Management may conduct random assessments to ensure compliance with the policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the SWDM issue tracking system and support teams shall be dispatched to remediate the issue. Repeated failures to follow the policy may lead to disciplinary action.

11. EXCEPTIONS

- 11.1 Exceptions to the patch management policy require formal documented approval from ICT Management. Any servers or workstations that do not comply with policy must have an approved exception on file with the Manager ICT Services.

12. ENFORCEMENT

- 12.1 Implementation and enforcement of this policy is ultimately the responsibility of the Management of ICT Services together with the Users. Deployment of such services may be enforced through the system policies, manual configurations, and Push Technology systems.
- 12.2 For the quality of service and assurance manual patches will be used to deploy the latest Microsoft product updates to computers running Microsoft Windows Server 2008, Microsoft Windows Server 2010, Microsoft Windows® XP, Microsoft Windows 7, 8, and Microsoft Windows 10 operating systems.
- 12.3 Manual patches are deployed as a precautionary measure to ensure continuity of service. This is currently the most cost-effective method and the most efficient system based on the size and simplicity of SWDM.

- 12.4 Other patches and updates shall follow the OEM requirements.
- 12.5 WSUS will be used to run updates on all the workstations and servers at SWDM.
- 12.6 The test environment shall be used to test patches, hotfixes, updates, service packs, etc before they are deployed on a live environment.

13. BREACH OF POLICY

- 13.1 Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the CFO and evaluated on its level of severity.
- 13.2 The appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy.
- 13.3 Actions include, but are not limited to:
 - 13.3.1 Revocation of access to Municipal systems and ICT services;
 - 13.3.2 Disciplinary action in accordance with the Municipal policy; or
 - 13.3.3 Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978).
 - 13.3.4 Punitive recourse against a service provider in terms of the contract.

14. REVIEW OF POLICY

- 14.1 The policy shall be reviewed annually.