



ICT USER AND NETWORK ACCESS POLICY

1 July 2024

Table of Contents

1. ABBREVIATIONS	2
2. PREAMBLE	3
3. USER AWARENESS	3
4. PURPOSE	4
5. DOCUMENTS THAT SHOULD BE READ WITH THE POLICY	4
6. ROLES AND RESPONSIBILITIES	4
7. ENFORCEMENT/LEGAL FRAMEWORK	5
8. USER AND NETWORK ACCESS POLICY	6
9. USER ACCOUNT MANAGEMENT	7
10. PASSWORD MANAGEMENT	12
11. OPERATING SYSTEM ACCESS RIGHTS	13
12. REMOTE ACCESS CONNECTIONS	13
13. SERVER ACCESS	14
14. MONITORING	14
15. CLIENT DATA ACCESS	14
16. BREACH OF THIS POLICY	14
17. POLICY REVIEW	15

1. ABBREVIATIONS

“ICT” refers to Information Communication Technology.

“IT” refers to Information Technology.

“SWDM” refers to Swellendam Municipality.

“Municipality” refers to the Swellendam Municipality.

“email” refers to electronic mail

“MM” refers to the Municipal Manager.

“Site Manager” refers to the service provider appointed to provide technical support.

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

“CFO” refers to the Chief Financial Officer.

“SAPS” refers to the South African Police Services

“SCM” refers to Supply Chain Management

“HR” refers to Human Resource Management

“Users” refers to Councillors, Employees, End Users, Interns, Temporary Staff Members and Contract Workers

“Manager” refers to the Head of each Division

“Network Devices” refers to computers and devices interconnected by communications channels that facilitate communications among users.

“IR” refers to the Information Resources.

“SLA” refers to Service Level Agreement.

“Workstations” refers to computers, laptops, printers and photocopiers

“VPN” refers to Virtual Private Network

“ISO” refers to International Organization for Standardization

“POPIA” refers to the Protection of Personal Information Act

2. PREAMBLE

- 2.1 SWDM ICT Division has developed the SWDM ICT User and Network Access Policy to establish specific requirements for accessing SWDM IR and monitoring.
- 2.2 SWDM ICT User and Network Access Policy protect SWDM IR from accidental and/or negligent deletion, destruction and modification.
- 2.3 Formal procedures must be put in place:
 - 2.3.1 that will control who will have access to what type of information,
 - 2.3.2 determine the privilege levels that each information user will have.
 - 2.3.3 control how access is granted and how such access is changed and the period of such access.
- 2.4 The policy also mandates a standard for the creation of strong passwords, password protection and frequency of changing passwords. Modification and/or destruction of information should be traced.

3. USER AWARENESS

- 3.1 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 using the Municipality's computers, networks, data and other information resources. Each user is responsible for reporting any suspected breaches of this policy's terms to the Manager: ICT Services.
- 3.2 The contents of this policy will be made available through presentations to all staff members and all those who attend must sign an attendance register and/or email and/or place it on the SWDM Network.

4. PURPOSE

- 4.1 The purpose of this policy is to protect and monitor the Municipality's ICT resources and to safeguard the confidentiality and integrity of information, resources, data, ICT equipment and council documentation.
- 4.2 This policy will guide the controls to be put in place:
- 4.2.1 By controlling who has the right to use what type of information,
 - 4.2.2 Monitoring the network,
 - 4.2.3 Generating stability and vulnerability reports,
 - 4.2.4 and guard against unauthorized use and access to information.

5. DOCUMENTS THAT SHOULD BE READ WITH THE POLICY

- 5.1 COBIT 5
- 5.2 ISO/IEC 20000
- 5.3 ISO/IEC 27000
- 5.4 ITIL v3
- 5.5 SWDM ICT Security and Firewall Policy
- 5.6 Information Technology Standard Operating procedures (To be developed)

6. ROLES AND RESPONSIBILITIES

- 6.1 This policy applies to every network user of SWDM including and not limited to councillors, staff members, third-party service providers, partners, interns, contract workers, services and agents:
- 6.1.1 SWDM ICT Division is responsible for ensuring that IR is maintained in compliance with the Municipality's ICT User and Network Access policy and procedures.

- 6.1.2 The Manager of the ICT Services Division is responsible for monitoring compliance with the Municipality's ICT User and Network Access Policy.
- 6.1.3 All SWDM ICT Service Division Team members are responsible to make sure that they adhere to the SWDM ICT User and Network Access Policy and that they enforce this policy.
- 6.1.4 HR must alert SWDM the Manager of the ICT Services Division of new network access needs whenever new appointments are made and inform when employees terminate their services.
- 6.1.5 The Manager of the ICT Services Division shall inform the Help Desk of any terminations of services so that the user names are disabled.
- 6.1.6 It is the user's responsibility to ensure that they safeguard their passwords to prevent being used to gain unauthorized access to the network. It is the user's responsibility to ensure that they do not leave their computers active while not attending and ensure that it is either lock it or log off.

7. ENFORCEMENT/LEGAL FRAMEWORK

- 7.1. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
- 7.2. Employees who violate this policy will be disciplined in terms of measures contained in or published in one or more of the following acts, regulations and policy prescripts (this list is by no means exhaustive):
 - 7.2.1. Amended State Information Technology Agency Act, 2002
 - 7.2.2. Promotion of Access to Information Act, 2000
 - 7.2.3. Municipal Finance Management Act, 2003
 - 7.2.4. Municipal Systems Act, 2000
 - 7.2.5. Copyright Act, 1978

- 7.2.6. National Archives Act, 2003
- 7.2.7. Protection of Personal Information Act, 2013
- 7.2.8. King Code of Government Principles (King IV)
- 7.2.9. Electronic Communication and Transaction Act, 2002
- 7.2.10. Any other applicable legislation, regulation or policy.

8. USER AND NETWORK ACCESS POLICY

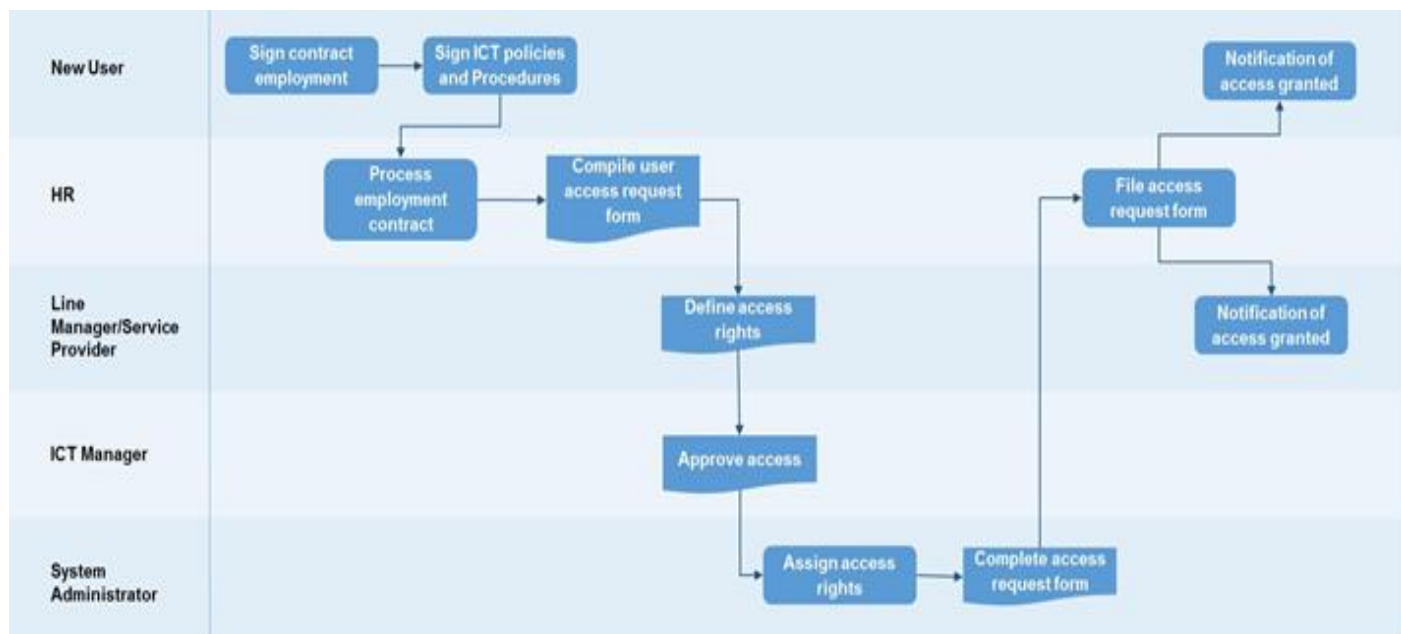
- 8.1 Formal user access control must be documented, implemented and kept up to date for application and information systems to ensure authorized user access and prevent unauthorized user access.
- 8.2 The process and physical access must be documented from the moment the user is registered on the network until the time the user is deregistered on the network.
- 8.3 Each user must be granted access and rights according to their needs and job.
- 8.4 Each user's access rights must be reviewed yearly by the Manager of ICT Services.
- 8.5 Only SWDM ICT Service Division officials must have administrative rights and they must be recorded as such. Any other person that needs to have administrative rights will be recorded and the rights will be removed at the end of the session.
- 8.6 All third-party vendor physical access to the server and switch room must be logged in a register in the format (Name, Surname, Company, Purpose, Date and Time) and must be accompanied by an SWDM ICT Service Division official at all times.
- 8.7 Third-party service providers will only be granted controlled access to remotely access the network by Director: ICT Services under strict supervision by SWDM ICT Services Division official or its appointed party. Audit trails must be in place at all times. The Service Provider must provide access to audit trail reports.

- 8.8 All user access forms shall be signed off by the ICT Manager and Director Financial Services and filed for safekeeping.

9. USER ACCOUNT MANAGEMENT

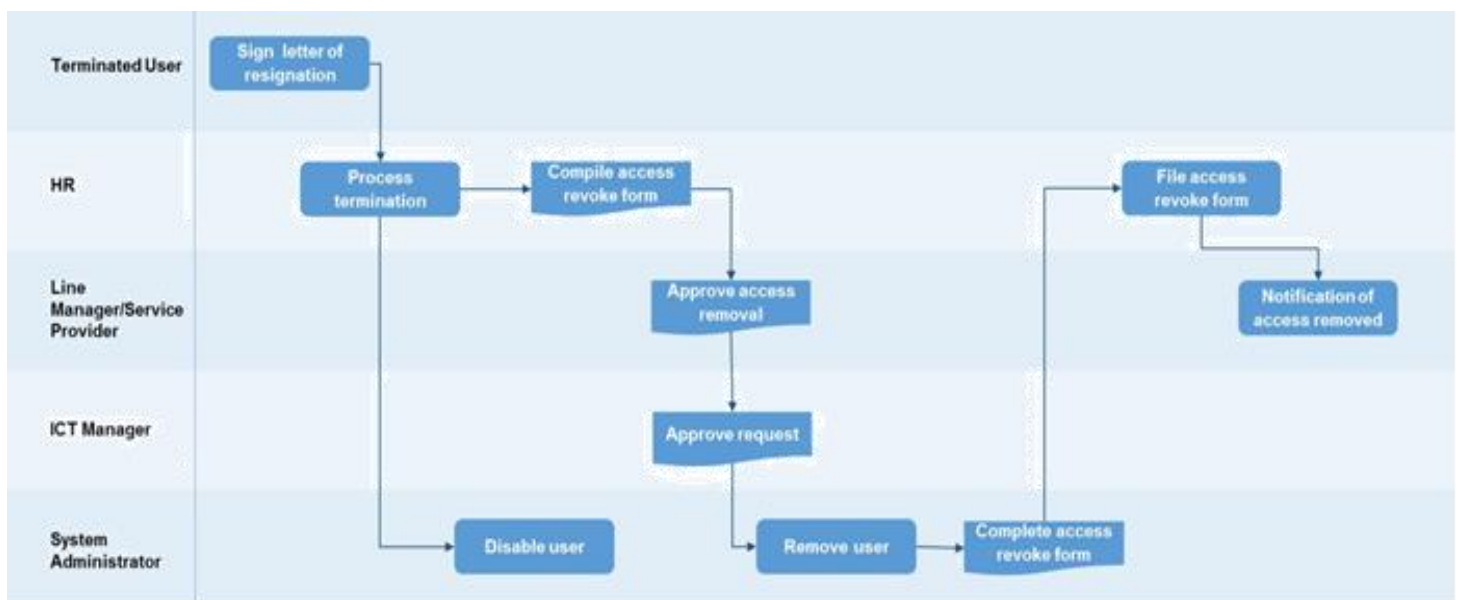
9.1 New User Registration

- 9.1.1 Each employee that requires access to the SWDM network shall complete the network access form which is provided by the ICT Manager and must be recommended by the Director of the employee for registration of the user account.
- 9.1.2 Network access forms must be approved by the Manager of ICT Services and Director Financial Services.
- 9.1.3 No network access shall be granted to unauthenticated individuals.
- 9.1.4 The following diagram below indicates the formal new user registration process:



9.2 Termination of Users

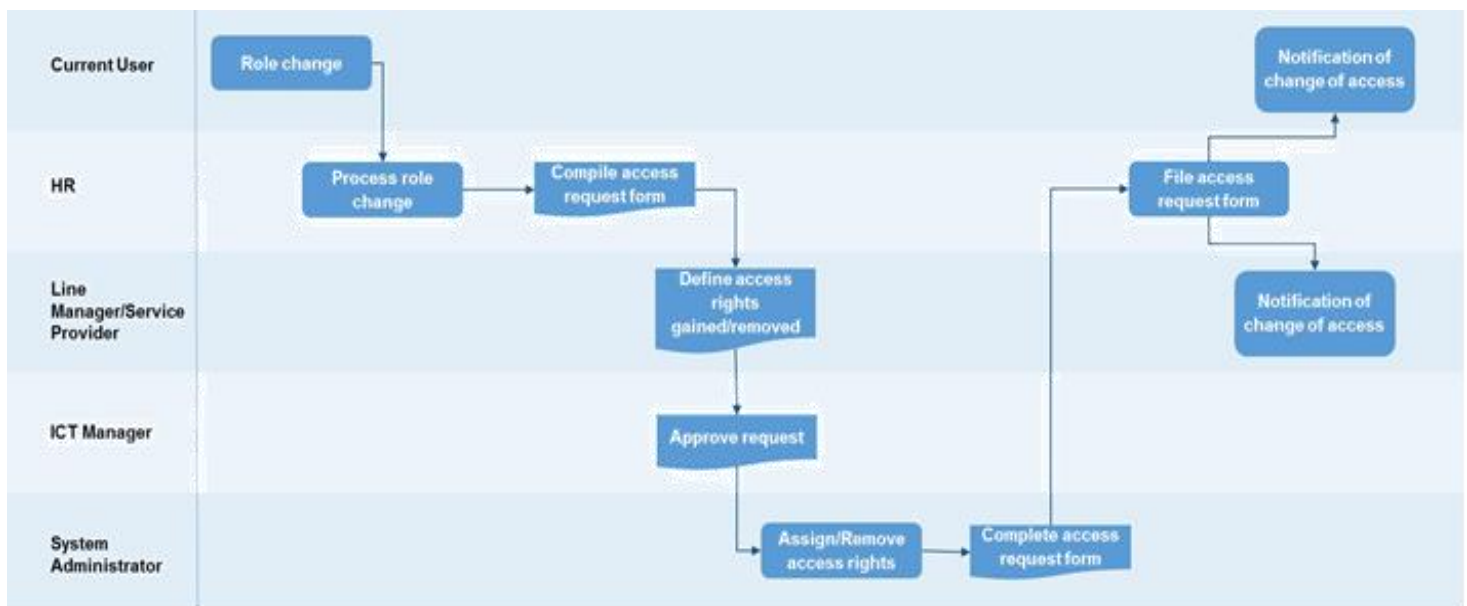
- 9.2.1 When the employee ceases to work for SWDM it is the responsibility of HR to inform the ICT Service Division of such termination of employment.
- 9.2.2 The ICT Service Division will disable the account of such users within three (3) days of receipt of the termination form. ICT Services Division shall effect such termination on Active Directory, Exchange Server and any other network services.
- 9.2.3 The ICT Service Division shall not terminate any user account without being informed by HR or the relevant Director of such need to terminate.
- 9.2.4 All user accounts and mailboxes may be deleted immediately by the ICT Services Division, upon an employee's departure from the Municipality either by dismissal, transfer, resignation, retirement, death or any other form of departure as informed by HR.
- 9.2.5 The following diagram below indicates the formal new user termination process:



9.3 User Access Change Request

9.3.1 An employee's access to a user account will be changed/modified by ICT Services Division, once the employee has transferred to a different Division per the employee's new job functions and requirements as recommended by the relevant Director

9.3.2 No user account will be created or modified without a signed network access form by the relevant Director and approved by the Director of Financial Services.



9.4 General User Access Rights Management

9.4.1 There shall be a register maintained by the ICT Manager to record terminations and new appointments and such information will form part of the ICT Service Division monthly reports and be reported to the ICT Steercom meetings quarterly.

9.4.2 All user accounts at the Municipality are created as Standard User Accounts. This means that users have standard privileges to log onto the network, use network printers that have been assigned to them,

access their email, and use the internet and any other privilege that is a core requirement of their job function.

- 9.4.3 Access rights may include, but are not limited to:
- a) General office applications (E-mail, Microsoft Office, SharePoint, etc.);
 - b) Department-specific applications and/or databases;
 - c) Network Shares;
 - d) Administrative tasks;
 - e) RAS/VPN Access;
 - f) Wi-Fi; and
 - g) BYOD – Bring Your Own Device
- 9.4.4 Access to Wi-Fi must only be provided to users who require access to the network throughout the Municipality, to fulfil their business function.
- 9.4.5 RAS/VPN access must only be granted to users who require the service to fulfil their business functions.
- 9.4.6 RAS access must only be granted to employees who require remote access to a system to administer the environment.
- 9.4.7 VPN access must only be granted to employees who:
- (a) Work remotely (Not at the office);
 - (b) Work overtime, or not within regular office hours.
- 9.4.8 It is the responsibility of the ICT Manager to ensure all users must be made aware of the security risks and obligations associated with RAS/VPN access.
- 9.4.9 RAS/VPN access must be monitored and audit logs reviewed every quarter (3 months) by system administrators.
- 9.4.10 All reviews must be formally documented and signed off by the ICT Manager and Director of Financial Services.

- 9.4.11 Documentation must be kept for record-keeping purposes.
- 9.4.12 The ICT Manager must approve all hardware and software, owned by Municipal employees and service providers/vendors if it is to be used for official purposes (BYOD).
- 9.4.13 The ICT team must ensure that all mobile devices must be protected with a PIN.

9.5 User Accounts

- 9.5.1 User names are standardized and the employee's name and the first letter of the surname are used to enable the user to log onto the network and the user's computer.
- 9.5.2 All dormant user accounts will be deleted or disabled thirty (30) days after the user has been informed that their account has not been used for longer than thirty (30) days. If the user cannot be contacted the supervisor shall be informed accordingly.
- 9.5.3 Should it be discovered that the user has not been able to access the computer account due to leave, the account shall be disabled.
- 9.5.4 Should it be discovered that an account has not been accessed or be used for a period of hundred and twenty (120) consecutive days such an account shall be deleted without notice.
- 9.5.5 Email addresses are also standardized with the employee's name and the first letter of the user's surname. In the instance where there are users with the same name and first letter of the user's surname, the user's full name and another initial and surname may be used as an email address.

10. PASSWORD MANAGEMENT

- 10.1 The password that an employee uses to log onto the network will be applied to access the employee's email account and internet application.
- 10.2 The Mayor, the Speaker, the Chief Whip, full-time and part-time Councillors, Interns and temporarily appointed contractors will be issued with usernames and passwords, which will be operative until their service is terminated.
- 10.3 Passwords must not contain the user's entire parts of the user's Surname or Name.
- 10.4 Passwords must contain characters from three of the following five categories:
- 10.4.1 Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
 - 10.4.2 Lowercase characters of European languages (a through z, sharps, with diacritic marks, Greek and Cyrillic characters)
 - 10.4.3 Base 10 digits (0 through 9)
 - 10.4.4 Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
 - 10.4.5 Non alphanumeric characters: ~!@#\$%^&* -+=`| \(){}[]:;'"<>.,?/
- 10.5 Passwords must never be written down on a piece of paper or shared with anyone. Passwords must be kept safe and secret.
- 10.6 Use different passwords for all user accounts.
- 10.7 Passwords should be changed every 30 days.
- 10.8 No official is allowed to show or share their passwords with ICT Service Division officials for any reason.

11. OPERATING SYSTEM ACCESS RIGHTS

- 11.1 Each system administrator must be given their own account within the administrator group. Should shared accounts be required to fulfil a business function, then this account must be approved and documented by the ICT Steering Committee.
- 11.2 The default administrator account must be renamed and a password must be randomly generated and sealed in an envelope and kept in a safe.
- 11.3 The default guest account must be removed or renamed and disabled.
- 11.4 Segregation of duties must be practised, in such a way that application administrators cannot perform general user tasks on an application. This is to prevent any fraudulent activity from taking place.
- 11.5 Applications administrators must remain independent of the department utilising the application, except for the ICT Services Division.
- 11.6 The ICT Manager must review monthly all users with administrative access to the environment and assess their rights for appropriateness. Should a user be found with excessive rights, a user access change request must be performed.
- 11.7 All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record-keeping purposes.

12. REMOTE ACCESS CONNECTIONS

- 12.1 A remote access connection is only allowed for server access and authorization must be granted by the Manager: ICT Services and Director Financial Services.
- 12.2 An application form must be completed by the third party required access to the SWDM network.

- 12.3 The ICT Manager will be responsible to maintain a register of all remote access granted.
- 12.4 All activities must be monitored monthly by the ICT Manager and changes should be recorded in the register accordingly.

13. SERVER ACCESS

- 13.1 Physical access to servers must be limited to ICT Service Division officials and all changes to servers must be made in accordance with the change management and control policies and procedure manuals.
- 13.2 All server users with administrative access rights must be documented.
- 13.3 ICT Service Division officials will use their login credentials to log on to servers at all times.

14. MONITORING

- 14.1 Mechanisms shall be put in place to monitor network access, failed login attempts, trends, monitor network stability, logged-out frequency etc.
- 14.2 Reports shall be generated monthly.

15. CLIENT DATA ACCESS

- 15.1 User Data folders must have permissions enabled and only the owner of the folder and files and administrators should be allowed access to these folders.

16. BREACH OF THIS POLICY

- 16.1 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 must be reported to the Director of Financial Services which will assess its level of severity. Appropriate disciplinary action or punitive recourse may be instituted against any user who contravenes this policy.

16.2 Actions may include, but are not limited to:

- 16.2.1 Revocation of access to Municipal systems and ICT services;
- 16.2.2 Disciplinary action in accordance with the Municipal policy;
- 16.2.3 Civil or criminal penalties e.g. violations of the Copyright Act, Act No. 98 of 1978; or
- 16.2.4 Punitive recourse against the service provider/vendor as stated in the service provider/vendor's SLA with the Municipality.

17. POLICY REVIEW

17.1 The policy shall be reviewed annually by the ICT Steering Committee.