"The City of Heritage"

INFORMATION TECHNOLOGY

ICT System Access Policy

Table of Contents

1. Purpose

The purpose of this policy is to maintain an adequate level of security to protect Ulundi Municipality data and information systems from unauthorised access. This policy defines the rules necessary to achieve this protection and to ensure a secure and reliable operation of Ulundi Municipality information systems.

2. Scope

This policy applies to all computer and communication systems owned or operated by Ulundi Municipality and its subsidiaries. Similarly, this policy applies to all platforms (operating systems) and all application systems.

3. Authority & Responsibility

This policy affects all employees of Ulundi Municipality and its subsidiaries, and all contractors, consultants, temporary employees and business partners. Employees who deliberately violate this policy will be subject disciplinary action up to and including termination.

4. Definitions and Acronyms

IEEE – The Institute of Electrical and Electronics Engineers is a non-profit professional association headquartered in New York City that is dedicated to advancing technological innovation and excellence. It is one of the leading standards-making organisations in the world. IEEE performs its standards making and maintaining functions through the IEEE Standards Association (IEEE-SA). IEEE standards affect a wide range of industries. One of the more notable IEEE standards is the IEEE 802 LAN/MAN group of standards which includes the IEEE 802.3 Ethernet standard and the IEEE 802.11 Wireless Networking standard.

Firewall – A firewall is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorised access while permitting legitimate communications to pass.

Remote Access is access to the Local Area Network (LAN) from any location outside the firewall by any method, including but not limited to Virtual Private Network (VPN), dial-in modem, frame-relay, SSH, cable-modem and any other method of accessing the LAN from outside the firewall. Remote access can refer to remote desktop, remote terminal (like Telnet) or any type of remote application / device (including remote browser).

Operating System – An operating system (OS) is a set of programs that manage computer hardware resources and provide common services for application software. The operating system is a vital component of the system software in a computer system.

LAN – A local area network (LAN) is a computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building.

VPN – A virtual private network (VPN) is a secure network that uses primarily public telecommunication infrastructures, such as the Internet, to provide remote offices or traveling user's access to a central organisational network. VPNs typically require remote users of the network to be authenticated, and often secure data with firewall and encryption technologies to prevent disclosure of private information to unauthorised parties.

PDA – A personal digital assistant, also known as a personal data assistant, is a mobile device that functions as a personal information manager. Current PDAs often have the ability to connect to the Internet. A PDA has an electronic visual display, enabling it to include a web browser, but some newer models also have audio capabilities, enabling them to be used as mobile phones or portable media players. Many PDAs can access the Internet, Intranets or Extranets via Wi-Fi or Wireless Wide Area Networks. Many PDAs employ touch-screen.

Wi-Fi is a popular technology that allows an electronic device to exchange data wirelessly (using radio waves) over a computer network, including high-speed Internet connections. The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards". However, since most modern WLANs are based on these standards, the term "Wi-Fi" is used in general English as "WLAN".

SSH – Secure Shell is a network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that it connects via a secure channel over an insecure network: a server and a client (running SSH server and SSH client programs). The protocol specification distinguishes two major versions referred to as SSH-1 and SSH-2.

SCP – Secure Copy is a means of securely transferring files between computers. It is based on the Secure Shell (SSH) protocol. The term SCP can refer to the SCP protocol or the SCP program.

SFTP – The SFTP command is a command-line interface client program implementing the client-side of the SSH File Transfer Protocol as implemented by the SFTP-server command by the OpenSSH project, which runs inside the encrypted SSH connection. It provides an interactive interface similar to traditional FTP clients.

Telnet – a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection.

5. Policy

5.1. Authorised Users

Only authorised users are granted access to information systems, and users are limited to specific defined, documented and approved applications and levels of access rights. Computer and communication system access control is to be achieved via user IDs that are unique to each individual user to provide individual accountability.

5.2. Authentication

Any User (remote or internal), accessing Ulundi Municipality networks and systems, must be authenticated. The level of authentication must be appropriate to the data classification and transport medium. Entity authentication includes but is not limited to:

- Automatic logoff
- A unique user identifier
- And at least one of the following:
- Biometric identification
- Password
- Personal identification number
- A telephone call-back procedure
- Token

5.3. Workstation Access Control

- All workstations used for Ulundi Municipality business activity, no matter where they are located, must use an access control system approved by Ulundi Municipality. In most cases this will involve password-enabled screen-savers with a time-out-after-no-activity feature, and a logon password for the CPU and BIOs.
- Active workstations are not to be left unattended for prolonged periods of time, where appropriate. When a user leaves a workstation, that user is expected to properly log out of all applications and networks.
- Users will be held responsible for all actions taken under their sign-on. Where appropriate, inactive workstations will be reset after a period of inactivity (typically 20 minutes). Users will then be required to re-log on to continue usage. This minimizes the opportunity for

unauthorized users to assume the privileges of the intended user during the authorized user's absence

5.4. System Access Controls

Access controls will be applied to all computer-resident information based on its' Data Classification to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

5.5. Access Approval

- System access or modification to access will not be granted to any user without appropriate approval first.
- Management is to immediately notify the ICT Security Officer and report all significant changes in end-user duties or employment status.
- User access is to be immediately revoked or disabled if the individual has been terminated. In addition, user privileges are to be appropriately changed if the user is transferred to a different job.

5.6. Privileged / Super User Access

- For security reasons Ulundi Municipality should try to minimise the number of super users in the organisation.
- A super user is an administrator across all the configured environments; it's not just individual environments. Hence, care should be taken when assigning someone as a super user, and this process must follow a thorough approval process in order to obtain the correct authorisation based on the user's job roles and responsibilities. Thereafter, super user access can only be granted accordingly.
- When any system gets installed, it installs a default profile, which will be used for any unknown user who accesses the system. The default profile is very restricted, and allows access to only certain parts of the system. A super user can modify the default profile at any time, but it should be executed with caution for obvious security reasons.

5.7. Do's and Don'ts of Privileged / Super User Access

- Don't change the root password on your machine.
    - Don't change the password of any users, especially root. The only password you are responsible for, and the only password you are allowed to change is your own. Changing the root or any other password will result in loss of privileged access and possible termination of your account.
- Don't add user accounts to the system.

- Access to computer systems at Ulundi Municipality must be controlled and monitored exclusively by the IT Department.

- Don't grant super user access to any user.
  - Being granted privileged access to a machine does not entitle you to grant the same access to others. Anyone who needs such access must request it from the IT Manager. Granting privileged access to others will result in loss of privileged access and possible termination of your account.
- Choose an extraordinary password for your personal account.
  - This is especially important because your password can be used to exercise certain root privileges. For similar reasons, we expect anyone who accepts these privileges to take extraordinary care in protecting their password. Never send your password in the clear over the network (and change your password immediately should you do this), never email your password, and never share your password with anybody.
- Don't run network daemons, i.e. no ircd, no ftpd, torrents, etc.
  - If you think you need to run a network service, please talk with a system administrator first.
- Don't use another user's account.
  - It is a violation of Ulundi Municipality policy to use the account of another user. Doing so will result in the loss of your privileged access and possible termination of your account.
- If you make changes to your system, write down what you did.
  - It is the policy of Ulundi Municipality that all machines should be able to be rebuilt at any point in time, and so the IT Department should be made aware of any specific customisations made on your machine in order to ensure your change needs survive Operating System reinstalls.
  - If you want to make a change to your system configuration, please talk to the systems administrators first, who may have already provided a solution to the problem you are trying to solve. Also, what you want may be something we should be doing organisation-wide.
  - Extraordinary user customisation is not a valid excuse to defer or forgo an Operating System upgrade when it becomes available.
- If a system is compromised by your action, you will be held accountable for the results.
- When in doubt, ask the IT Manager.
- If you're not absolutely sure of what you're doing, consult the administrators first, as doing so is encouraged and saves time.

5.8. Need-to-Know

Users will be granted access to information on a “need-to-know” basis. That is, users will only receive access to the minimum applications and privileges required performing their jobs.

5.9. Compliance

- Users who access Ulundi Municipality’s information systems must sign a compliance statement prior to issuance of a user ID. Refer to the Ulundi Municipality ICT Security Policy and Procedures for further details.
- A signature on this compliance statement indicates the user understands and agrees to abide by Ulundi Municipality policies and procedures related to computers and information systems.
- Annual confirmations will be required of all system users.

5.10. Audit Trails and Logging

Logging and auditing trails are based on the Data Classification of the systems.

5.11. Confidential Systems

Access to confidential systems will be logged and audited in a manner that allows the following information to be deduced:

- Access time
- User account
- Method of access
- All privileged commands must be traceable to specific user accounts
- In addition, logs of all inbound access into Ulundi Municipality‘s internal network by systems outside of its defined network perimeter must be maintained.
- Audit trails for confidential systems should be backed up and stored in accordance with Ulundi Municipality back-up and disaster recovery plans.
- All system and application logs must be maintained in a form that cannot readily be viewed by unauthorised persons.
- All logs must be audited on a periodic basis, and audit results must be included in periodic management reports.

5.12. Access for Non-employees

- Individuals who are not employees, contractors, consultants, or business partners must not be granted a User ID or otherwise be given privileges to use Ulundi Municipality computers or information systems unless the written approval of the Department Head has first been obtained and then sent to the ICT Security Officer accordingly.
- Before any third party or business partner is given access to Ulundi Municipality computers or information systems, a chain of trust agreement defining the terms and conditions of such access must have been signed by a responsible manager at the third party organisation.

5.13. Unauthorized Access

- Employees are prohibited from gaining unauthorised access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems.
- System privileges allowing the modification of ‘production data’ must be restricted to ‘production’ applications only.

5.14. Remote Access

- Any employee using any computing device remotely must ensure that such a device is updated with the most recent security patches for their Operating System. Please refer to the Ulundi Municipality ICT Security Policy for details regarding patch management.
- All machines on the Ulundi Municipality LAN as well as any remote computing device must run the most up-to-date versions of anti-virus software with regularly updated virus definitions, i.e. at a minimum, once a week. However, whenever deemed necessary by the ICT Department, these updates may be required to run more frequently due to business requirements. Please refer to the Ulundi Municipality ICT Security Policy for details regarding anti-viruses.
- All remote computing devices must be running an appropriately configured firewall program. Users at a public Wi-Fi “Hotspot” must be aware that, if such remote computing devices are not running an appropriately configured firewall, a malicious user could gain access to the device. Please refer to the Ulundi Municipality ICT Security Policy for details regarding firewall configurations and settings.
- Any authorised user using a remote computing device outside the firewall must use the VPN to send and receive Ulundi Municipality email or to access the Internet and Intranet accordingly. No Ulundi Municipality email may be sent using third-party email services

(including, but not limited to, Gmail, Hotmail, Webmail, etc.). Please refer to the Ulundi Municipality ICT Security Policy for details regarding remote access and VPN.

- Any authorised user accessing any computer or device on the LAN for remote management or administration must use SSH or VPN. For remote file transfer, employees must use SCP, SFTP or VPN. Under no circumstances shall Telnet, FTP or any other unencrypted access methods be used.
- All employees using any computing device to remotely access and connect to Ulundi Municipality's LAN shall not do so while still connected to any other network, except for a personal network over which such employee has complete control over.
- All employees requiring remote access to Ulundi Municipality's LAN needs to complete and submit a Change Request Form to the ICT Security Officer for relevant approval first. Please refer to the Ulundi Municipality ICT Security Procedure for details regarding the provision of remote access to the Ulundi Municipality network.

5.15. Network Access Points

- Administrative Access
  - ICT Security must decide over which interfaces and ports an administration connection is allowed and from which network or host the administration is to be performed, and then restrict access to those specific locations accordingly.
  - Do not leave an Internet-facing administration interface available without encryption and countermeasures to prevent hijacking. In addition:
  - Disable unused interfaces.
  - Apply strong password policies.
  - Use static routing.
  - Audit Web-facing administration interfaces.
- Disable Unused Interfaces
  - Only required interfaces and ports should be enabled on the router. An unused interface is not monitored or controlled, and it is probably not updated, hence this might expose Ulundi Municipality to unknown attacks on those interfaces.
  - Open ports are high-risk areas. A firewall allows administrators to disable unnecessary TCP and UDP ports. The known ports are the critical ones required for Operating System function. The registered ports are those able to be used by only that service or application.
  - By obtaining a list of ports and their associated services and applications, administrators/service provider must determine which ones are required for critical

functions to Ulundi Municipality. For instance, to prevent any traffic, the known ports associated with these applications can be blocked. Similarly, known software and malware have known associated ports, all that can and should be blocked by Ulundi Municipality to create a more secure server posture. Hence, best practice is to close all ports not in use.

- Apply Strong Password Policies
    - Brute force password software can launch more than just dictionary attacks. It can discover common passwords where a letter is replaced by a number. Always use uppercase and lowercase, number, and symbol combinations when creating passwords.
    - Refer to the ICT Security Policy for further information on the appropriate password policies that should be applied to all network and computing devices at Ulundi Municipality.
- Use Static Routing
    - Static routing prevents specially formed packets from changing routing tables on the router. An attacker might try to change routes to cause denial of service attacks, or to forward requests to a rogue server. By using static routes, an administrative interface must first be compromised to make routing changes.
- Services
    - On a deployed router, every open port is associated with a listening service. To reduce the attack surface area, default services that are not required should be shut down. ICT should also scan Ulundi Municipality routers to detect which ports are open accordingly.
- Auditing and Logging
    - By default, a router logs all deny actions; this default behaviour must not be changed.
    - Log files should be stored in a central location. Modern routers have an array of logging features that include the ability to set severities based on the data logged.
    - An auditing schedule should be established to routinely inspect logs for signs of intrusion and probing.
- Intrusion Detection

- With restrictions in place at the router to prevent TCP/IP attacks, the router should be able to identify when an attack is taking place and notify a system administrator of the attack.
- Attackers learn what your security priorities are and attempt to work around them. Intrusion Detection Systems (IDSs) can show where the perpetrator is attempting attacks, and should be implemented by Ulundi Municipality accordingly.

5.16. Enforcement

- Non-compliance, violation and disregard of this policy shall result in disciplinary action and sanctions against the employee concerned and such sanctions may lead to termination of the employee's employment contract, depending on the circumstance and the gravity of the transgression.
- In the event of Ulundi Municipality incurring financial loss as a result of non-compliance, violation and / or disregard of this policy, Ulundi Municipality shall be entitled to institute legal proceedings to recoup the loss it has incurred from the employee / user, and this shall be in addition to the disciplinary action that Ulundi Municipality would have taken against the employee.

6. Cross-Reference to other Policies/Procedures

- ICT System Access Procedure; and
- Activity Monitoring Policy

7. Approvals

The table below provides necessary approvals of this policy.

Approver	**Signature**	**Date**
His Worship The Mayor: Cllr W.M. Ntshangase		
Municipal Manager: Mr. S.M. Khomo		