"The City of Heritage"

INFORMATION TECHNOLOGY

IT Security Policy

Table of Contents

1. Introduction

Computers enable employees of Ulundi Municipality to conduct the organisation's day-to-day business activities more effectively and efficiently. In addition, computers also allow employees greater access to organisational resources and information. In order to promote a working environment that is conducive to teamwork and productivity, it is essential that all users understand their roles and responsibilities with regards to Information Technology (IT) security and adhere to the security requirements of Ulundi Municipality. IT security is therefore characterised as the preservation of:

a) **Confidentiality** – Ensuring that information is only accessible to those individuals who are duly authorised to have access to it.
b) **Integrity** – Safeguarding the accuracy and completeness of information and processing methods.
c) **Availability** – Ensuring that authorised users have access to information and associated assets as and when required.

As such, municipalities have different uses for their respective IT systems. The installation of Ulundi Municipality's IT network represents a significant IT investment and so IT equipment must be utilized in the best interest of, and be of benefit to, Ulundi Municipality.

2. Objectives

The objectives of the IT Security Policy are to:

a) Clarify to all users their responsibilities regarding the security of Ulundi Municipality's information and computing resources.
b) Define the potential risks and dangers for Ulundi Municipality in the event of misappropriation and abuse of computing equipment by users.
c) Maintain an appropriate level of physical and logical security to safeguard IT systems and resources against unauthorised use, modification, disclosure or loss to preserve the integrity of the Ulundi Municipality IT environment.
d) Regulate the professional and effective use of computing equipment within Ulundi Municipality, as well as between Ulundi Municipality and its external entities.
e) Establish a standard for creation of User ID's and strong passwords, the protection of those passwords, and the frequency of change thereof.
f) Identify the persons responsible for maintaining the security requirements.

g) Establish management direction, basis of procedures and requirements to ensure the appropriate protection of Ulundi Municipality's information and equipment resources by any means.
h) Ensure that this investment in information and equipment resources is properly managed.
i) Ensure that the system is optimally utilized in its full capacity to the best advantage of Ulundi Municipality.

3. Appointment of IT Committee

Ulundi Municipality shall appoint an IT Committee that must meet at least quarterly to discuss IT-related improvements or changes in the IT environment and infrastructure.

4. Responsibility for IT Security

The nominated and appointed Information Security Officer (ISO) will be responsible for implementing and maintaining Ulundi Municipality's IT security throughout the organization. Furthermore, the IT Security Policy must be reviewed at least once a year, or as deemed appropriate based on changes in technology or regulatory requirements.

5. Scope

This policy applies to all employees, consultants and temporary staff who access Ulundi Municipality's computer networks with an organization-owned or personal workstation and are responsible for an account (or any form of access that supports or requires a User ID and a password) on any system that resides at any Ulundi Municipality facility, has access to the network, or stores any non-public organisational information. All employees need to be aware of security risks and vulnerabilities in order to create organisation-wide security consciousness. Therefore, security awareness and training programmes shall be initiated and each employee shall be required to receive the necessary Information Security awareness and training provided by Ulundi Municipality.

6. Administrative Controls

6.1. General Controls

The IT Manager (or his nominee) will, on recommendation of the IT Committee, issue guidelines on the use and application of Ulundi Municipality's network and shall monitor compliance with these guidelines, which must be strictly adhered to by all users of any IT

systems. The required administrative controls applicable to the system will be included in these guidelines and will comprise the following:

a) Physical controls over computer hardware, backups and software;
b) Access controls;
c) Data security controls; and
d) Internet and email usage controls.

6.2. **Programming and Documentation Standards**

Only the IT Manager, on recommendation of the IT Committee, may liaise with IT software suppliers to provide software for Ulundi Municipality's use and to have such software developed further or amended. The IT Manager shall keep a register of all such requests for amendment and/or enhancement of Ulundi Municipality's software and hardware and shall inform the relevant users of any changes.

6.3. **Insurance**

The Finance Department shall ensure that appropriate and adequate insurance cover is obtained in respect of all components of Ulundi Municipality's IT operations.

6.4. **Reporting**

The IT Manager shall report to the IT Committee on the general use and application of the IT network, indicating in such report whether existing administrative controls need to be reviewed or amended, specifying operational problems of material importance which have arisen during the quarter to which the report relates, and indicating how such problems have been or are being addressed.

6.5. **Random Audits**

a) The IT Manager, in consultation with the Municipal Manager, shall arrange random audits of the IT systems on a periodic basis. These audits may be conducted by either the internal or external auditors (or both), provided that sufficient budgetary provisions have been provided for.
b) The findings of such random audits may be included in the audit report to the IT Committee, or if findings are significant then they must be reported to a special audit committee. Also, the findings should be forwarded to the audit committee of Ulundi Municipality for consideration.

7. Physical Controls

Physical controls with regards to the Ulundi Municipality IT network relate to measures which must be put into place to ensure the physical security and protection of all relevant computer hardware, software, manuals and the server room. The physical controls are required to provide protection against natural hazards, theft, etc.

7.1. Hardware

a) Where personal computers have been allocated to officials, such officials shall accept that these computers are for official use only.
b) No hardware may be installed or removed by any municipal official without prior consent and authorization or direction from the IT Manager.
c) No hardware may be removed by any official from municipal premises without the prior written authority of the Municipal Manager or IT Manager. The IT Manager shall keep such written authority on file, and the official who wish to remove the relevant hardware must have a copy of such authority for inspection when required.
d) Any malfunctioning computers must be immediately reported in writing to the IT Manager by the official to whom such equipment has been allocated, and the IT Manager shall immediately attend to the required repairs or replacement of the equipment, but subject to the necessary provision having been made in the budget.
e) Given the significant cost of printing, officials to whom the use of printers has been allocated must ensure that all printing is kept at a minimum. Where multiple copies of a particular document are required, the original shall be printed and photocopied. Wherever possible, screen previews should be used rather that physical printing. Original toners and inkjet cartridges must be used when printing is necessary, as not only may the compatible or refilled products void Ulundi Municipality's warranty in respect of the equipment, but they can also (in given circumstances) damage the printers.

7.2. Software

a) The IT Manager shall maintain a list of approved software to be used on the IT network, as well as the number of licenses owned and the number of copies of such software loaded onto the system. Only authorized and licensed software listed on the approved software listing from Council (HOD or CFO) may be loaded onto Ulundi

Municipality computers, and this may only be implemented with the consent and supervision of the IT Manager. The IT Manager shall further ensure that this authorized list, referred to as the “Council Approved Software List”, is reviewed and updated periodically in order to address any new software which is released into the market that may be relevant to Ulundi Municipality and as the demand for new or additional software arises.

b) **Caution:** No software may be downloaded through the Internet or via email without the approval of the IT Manager or the relevant Head of Department. Also, pirated software by any official will not be permitted whatsoever. As such, here are examples of Council’s list of approved software:

Standard Applications - A new user is entitled to the following standard applications upon receiving a new computer or the user is new to the institution:

- Microsoft Office Suite
- Antivirus Software
- Acrobat Reader
- WinZip

Specialised Applications - A user is entitled to the following specialized applications once duly authorized:

- PAYDAY
- Pastel Evolution

7.3. Server Room

a) Only IT personnel shall have regular access to the server room.

b) The server room shall always remain locked unless in eye view of I.T. personnel.

- The IT Manager shall ensure that adequate fire prevention, detection and extinguisher systems are installed in the server room, and that this equipment is regularly checked and maintained. No official may tamper with such equipment, and no official may remove any such equipment from the server room other than for the purpose of having it tested or serviced.
- The IT Manager shall ensure that a properly designed, maintained, and operated air conditioning system is installed in the server room.
- The IT Manager shall ensure that the servers are placed above the ground or on raised flooring in the event of flooding.
- The IT Manager shall regularly test the Uninterrupted Power Supply (UPS) to ensure that it is maintained in an operational condition.

8. Access Control

8.1. General

Access control is necessary to restrict unauthorized user access to any portion of the IT network or to any particular component of the system. It is therefore necessary that the bona fide user, to gain access, must first be authorized, i.e. the access of such user to the system must be properly authenticated. Access to the IT network comprises three steps:

- Physical access to a terminal;
- Access to the system; and
- Access to specific commands, transactions, programmes and data within the system.

8.2. Physical Access to Terminals and Systems

After the bona fide user has switched on his or her computer, the user must enter a computer password to gain further access to terminals and systems accordingly.

8.3. Access to specific Commands, Transactions, Programs and Data within the System

The IT Manager or relevant Head of Department (HOD) shall set access level priorities in accordance with the job descriptions of the officials concerned and to comply with the specific further requirements of the officials of the Finance Department. Access level and amendment priorities shall be set out in writing by the IT Manager or relevant HOD.

8.4. User Codes and Passwords

a) Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Ulundi Municipality's entire corporate network.

b) As such, all Ulundi Municipality employees, consultants and temporary staff with access to the organization's systems are responsible for taking the appropriate steps (as outlined below) to select, maintain and secure their passwords at all times and never use an account assigned to another user, as they will be held responsible for total use or misuse of their account. All officials, to whom user codes and passwords have been allocated, must ensure that these codes and passwords are properly safeguarded. Under no circumstances may the employee share any use code or password with colleagues.

c) Passwords are used for various purposes at Ulundi Municipality. Some of the more common uses include: user level accounts, web accounts, email accounts, screensaver protection, application logins and local router logins. All users should be aware of how to select strong passwords. Hence, the following password guidelines must be adhered to by all users on all servers and computers within Ulundi Municipality:

- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords should not be a word in any language, slang, dialect or jargon.
- Do not use the same password for Ulundi Municipality accounts as for other non-organisational access (e.g. personal account, option trading, benefits, etc.).
- Users must not use the "Remember Password" feature for applications (e.g. PAYDAY, Internet Explorer, etc.), and must not write passwords down and store them anywhere that is easily accessible within their offices.
- Users must not store passwords in a file on any computer system (including laptops or similar devices) without encryption.
- Users must avoid using the same password for multiple applications.

- If an account or password is suspected to have been compromised, the user must report the incident to the IT Manager and change all their passwords accordingly.
- If a user is requested to provide their password details to any IT staff member, they must ensure that they monitor the actions performed by the staff member. Thereafter, the user should change their password immediately once the IT staff member has left.
- If an account or password is suspected to have been compromised, immediately report the incident to the IT Manager and change all passwords accordingly.

d) Where possible, systems have been configured to follow Ulundi Municipality standards. The organisation's requirements for password settings should be as follows:

- A minimum of eight (8) characters in length;
- Must be changed every 90 days;
- A password history of 24 previous passwords should be maintained.
- User accounts are set to lockout after 3 unsuccessful login attempts;
- Comprised of both letters and numbers (i.e. alphanumeric);
- Must contain at least one (1) capital letter and one (1) special character (e.g. #, @, %, $, etc.);
- Users should not use their usernames as passwords;

e) Additional Configuration settings for Active Directory Server

- A minimum password age of 1 days;
- Accounts should be set to lockout indefinitely (until IT Manager unlocks);
- Accounts are set to lockout after 3 invalid log-on attempts.

f) Users must take note that for all activity performed using their user name and password, they will be held accountable and may face disciplinary action in the event of misuse. It is therefore of utmost importance that users follow the guidelines below on password construction and safeguarding their password in order to minimise the threat of others obtaining their passwords.

- A password should be created from a pass-phrase. For example, the phrase "security is vital to this company and me" might result in the password of "siv2Tcam!" by using the first letter of each word in the phrase, substituting the word "to" for the number "2", and adding the exclamation mark at the end to increase complexity.

- Personal details, such as spouse's name, licence plate, ID number or birthday, must not be used.
- Words in a dictionary, derivatives of user ID's and common character sequences such as "123456" must not be used as well.
- Passwords should not be based upon month / year combinations such as "jan09" or "april2009". Hackers use these types of words in attempts to guess passwords.
- Users must not use cyclical passwords. For example, users should not add a numeric at the end of the password in sequence.
- Passwords must not consist of all identical numeric or alphabetic characters, such as: "1111111" or "aaaaaaa".
- Employees must never share their passwords with anyone, including IT staff, administrative assistants or secretaries.
- All passwords are to be treated as sensitive organisational information.

g) Users must take note of and adhere to the following "Don'ts":

- Do not reveal a password over the phone to anyone.
- Do not reveal a password in an email message.
- Do not talk about a password in front of others.
- Do not hint at the format of a password (e.g. "my family name").
- Do not reveal a password on questionnaires or security forms.
- Do not share a password with family members or colleagues.
- Do not reveal a password to co-workers while on vacation.

9. Data Security Control

9.1. Privileges and Exposure

As stated above, access by users to Ulundi Municipality's IT systems shall be restricted in accordance with the job descriptions of officials concerned. Users are responsible for the protection of sensitive information by ensuring that only officials whose duties require such information are allowed to obtain knowledge of such information while it is being processed, stored or in transit.

9.2. Backups

As only a small percentage of Ulundi Municipality's critical business information resides on its servers, backup procedures are required in respect of information saved on personal computers. Backup procedures will be determined by the IT Manager, and communicated

in writing to all relevant users accordingly. These procedures shall be adhered to by all users on the system.

10. Internet and Email

10.1. Use of Internet

a) Internet access and related IT resources are provided to Ulundi Municipality at significant cost and are made available primarily for business use. Users who have access to the Internet shall use this access solely in connection with official responsibilities, including communicating with clients, working related partners, local and provincial government agencies, providers of goods and services to Ulundi Municipality, and to also research relevant topics and obtain business related information which is of use to Ulundi Municipality. Limited personal use on approved sites may be authorized when such access will be to the best advantage of Ulundi Municipality only.

b) All users who have access to the Internet shall conduct themselves honestly and appropriately, and respect copyrights, software licensing rules, property rights, privacy and the prerogatives of others. Specifically, officials who use the Internet shall ensure that intellectual property of others is protected and that Ulundi Municipality's resources are not misused, that information and data security (including confidentiality where applicable) are at times respected, and that the Internet is not used for any form of abuse.

c) Every official using the Internet facilities of Ulundi Municipality shall identify himself or herself honestly, accurately and completely. Officials using the Internet shall do so only when this is required to fulfill their official responsibilities and/or when they are authorized to do so.

d) Whenever an official downloads any file from the Internet, such a file must be scanned for viruses before it is run or accessed. If the official is uncertain as to the procedure to be followed, such official shall immediately seek assistance of the IT Manager.

10.2. Authority to Speak on the Behalf of Ulundi Municipality

Only those officials who are duly authorized by the Municipal Manager to speak to the media, to analysts, in public gatherings or send external emails on behalf of Ulundi Municipality may do so.

10.3. Integrity of Ulundi Municipality's Image

a) Officials who are authorized to speak on behalf of Ulundi Municipality, as set out in 10.2 above, shall ensure that they honour the image and integrity of Ulundi Municipality at all times, do not engage in any unauthorized political advocacy, and refrain from the unauthorized endorsement by Ulundi Municipality of any commercial product or service not sold or provided by Ulundi Municipality itself.

b) Moreover, such officials must ensure that, where inputs are provided on behalf of Ulundi Municipality to any news group or chat room, such inputs have been grammar and spell-checked, and that the inputs reflect the corporate view of Ulundi Municipality (where applicable) rather than the personal opinions of the writer.

10.4. Security

a) Prompt disciplinary action shall be instituted against any official who attempts to disable, defeat or circumvent any firewall, proxy, Internet address screening programmed or any other security systems installed by the IT Manager or any IT suppliers to assure the safety and security of Ulundi Municipality's IT network.

b) Any officials who obtain a password or user code (ID), which allows access to the Internet and/or the organization's IT network, shall keep such a password and user code confidential, except if any occasion arises where any authorized technical support official requires knowledge of such password or user code in order to solve a computer related problem. As set out in 8.4. (b) above, the present policy strictly prohibits the sharing of user codes and passwords between employees. Furthermore, logging onto the IT network or Internet with one's personal user code and password, and then allowing another user to use or work on the Internet or the IT network, shall be viewed as an attempt to bypass official security procedure, and is strictly prohibited and will be dealt with accordingly.

c) Every authorized user shall sign all security and confidentiality agreements provided to them by the IT Manager before attempting to gain access to the Internet and/or the network.

d) Software and systems have been installed to monitor and record all Internet usage. The IT Manager shall be authorized to record (for each user) every website visited, every chat room or newsgroup visited, every email message sent or received, and every file transfer in to and out of Ulundi Municipality's internal networks. No official shall have the right to privacy in respect of his or her Internet or network usage.

e) The IT Manager will review all Internet activities and analyze the relevant usage patterns. Thereafter, appropriate action will be taken on the user wherever any abuse of the system is evident.

f) Any software or files downloaded by any user from the Internet onto Ulundi Municipality's IT network shall become the property of Ulundi Municipality, and may be used only in a manner consistent with the applicable licenses and/or copy rights.

10.5. Electronic Mail (Email)

a) Only authorized officials shall use the available email facility.

b) The IT Manager shall scan all emails for any inappropriate content or offending words or phrases.

c) All copies of emails shall be kept as records.

d) Only authorized officials shall be permitted to receive attachments through the email system, and such attachments shall be scanned by the IT Manager to ensure that they are related to responsibilities of the official concerned.

e) The IT Manager shall maintain a list of prohibited and blocked email, and shall update and amend such list as circumstances require.

10.6. Internet Browser

As indicated in 10.4 and 10.5 above, Ulundi Municipality reserves the right to track all visited sites.

10.7. Unacceptable Practices

a) No official may display any kind of sexually explicit material on any organizational system. Furthermore, no sexually explicit material may be archived, stored, distributed, edited or recorded using any of Ulundi Municipality's resources.

b) The IT Manager shall have the right to block access from within Ulundi Municipality's networks to all Internet sites identified as inappropriate. If any user is connected to a site which contains sexually explicit or otherwise offensive material, such user must immediately disconnect from the site concerned, regardless of whether such site has previously been deemed acceptable by any screening or rating programmers.

c) Ulundi Municipality's IT related facilities, and especially its Internet facilities, may not be used knowingly by any official to violate the laws and regulation of the Republic of South Africa or any other nation, or the laws and regulations of any province or municipality. The use of any municipal resources or illegal activities shall be ground for the immediate dismissal of the official concerned, and the Council and it's official

undertake further to cooperate with any legitimate law enforcement agency in this regard.

d) No employee may knowingly use Ulundi Municipality's IT facilities and resources to download or distribute pirated software or data.
e) No official may knowingly use the Internet facilities to propagate any viruses, worms, Trojan horses or trap doors (i.e. malicious code).
f) No official may knowingly use Ulundi Municipality's Internet facilities to disable or overload any computer or network or to circumvent any system intended to protect the privacy or security of another user.
g) No employee with authorized Internet access may upload any software licensed to Ulundi Municipality or date owned or licensed to Ulundi Municipality without prior authorization of the IT Manager.
h) No official may create a communication link requiring dial-out access from any computer which is also connected to the IT network.
i) No official may use any software which is not provided or approved by the IT Manager or relevant HOD.
j) Only the IT Manager or relevant HOD shall authorize the provision of email addresses to authorized users.

10.8. Ownership and Classification of Data

Any Ulundi Municipality data that is created, sent, printed, received or stored on systems owned, leased, administered or authorized by Ulundi Municipality is the property of Ulundi Municipality and its protection is the responsibility of Ulundi Municipality's owners, designated custodians and users. As such, data shall be classified as either: Confidential, Sensitive or Public.

Confidential: Sensitive data that must be protected from unauthorized disclosure or public release based on local or governmental law (e.g. the Promotion of Access to Information Act, No. 2 of 2000) and other constitutional, statutory, judicial and legal agreements. Examples of "Confidential" data may include but are not limited to:

- Personally Identifiable Information, such as a name in combination with Identification Number (ID) and/or financial account numbers
- Employee records
- Intellectual Property, such as copyrights, patents and trade secrets

Sensitive: Sensitive data that may be subject to disclosure or release under the Promotion of Access to Information Act, No. 2 of 2000, but requires additional levels of protection. Examples of “Sensitive” data may include but are not limited to:

- Operational information
- Personnel records
- Information security procedures
- Research
- Internal communications

Public. Information intended or required for public release as described in the Promotion of Access to Information Act, No. 2 of 2000. However, any data owned or under the control of the South African Government must comply with the national classification authority and national protection requirements.

Furthermore, authorized officials who don’t participate in Internet chats and news groups shall refrain from revealing confidential municipal information, client data and any other material covered by existing council policies and municipal procedures with regards to confidential information. Officials, who release protected information through the Internet whether or not it is advertent, shall be subject to all the applicable penalties in terms of Ulundi Municipality’s existing data security policies and procedures.

11. Supplier Relationship

The Ulundi municipality is committed to working with our suppliers to realise the full value of our relationships and to positively contribute to our communities, people and the environment.

- Proactively engage with our suppliers with a focus on building trusting, co-operative and long-term relationships;
- Apply good governance to provide oversight and means through which the objectives of the process are monitored, audited and integrity is maintained;
- Define and apply appropriate sourcing methods in our procurement of goods and services, ensuring all capable suppliers have an equal access to opportunities to work with us;
- Deal with suppliers in good faith, ethically and responsibly, and make payments in accordance with agreed terms;
- When all other vetting requirements remain equal, give preference to suppliers that demonstrate a commitment to sustainably manage their business performance, with values complementary to our own;
- Set clear expectations for our suppliers regarding their sustainability performance and embed its minimum requirements within supplier contracts;
- Employ appropriate methods for assessing the performance of our key strategic suppliers and those engaged in higher risk activities and monitoring their progress over time;
- Encourage our key suppliers to make available high value, environmentally and socially responsible products and services as well as to improve the sustainability performance of their businesses; and
- Actively engage with key suppliers and provide data and other relevant information to enable innovation and the development of products that meet our aspirations.

12. Official Website

The IT Manager shall be responsible for the design and maintenance of Ulundi Municipality's website. Each Head of Department shall ensure that all information required by the Municipal Finance Management Act, as well as any other relevant legislations and Council Policies, is promptly and appropriately submitted to the IT Manager for display on the official website. The IT Manager shall (in consultation with the relevant Heads of Department) further decide on any other information to be made available on the website. Only the IT Manager and Heads of Department shall be authorized to amend, add and delete information on the official Ulundi Municipality website.

13. Protocols

13.1. Reporting Security Incidents

a) If an IT security incident or breach is suspected or noticed by any employee, then it is the obligation of that employee to immediately notify the Information Security Officer.
b) Users are required to note and report any suspected security threats and/or weaknesses in and around IT systems and services. Critically, users must not attempt to prove a suspected weakness within a system, as testing weaknesses might be interpreted as a potential misuse of the system, which could lead to disciplinary action thereafter.
c) The Information Security Officer tasked with the security responsibility of Ulundi Municipality must report all instances of a breach of security, or failure to comply with security measures, or conduct constituting a security risk, as soon as possible to the Chief Directorate Security of the National Intelligence Agency (NIA), and where appropriate to the South African Police Services (SAPS - Crime Prevention Unit) or the South African National Defence Force (SANDF - MI). Where official encryption is concerned, a security breach must also be reported to the South African Communication Security Agency (SACSA).
d) When a breach of security occurs, the existing channels must be used to report it. It is the responsibility of the Information Security Officer to ensure that all breaches of security are reported.
e) Breaches of security must at all times be dealt with using the highest degree of confidentiality in order to protect the ISO concerned and prevent him or her from being unnecessarily done an injustice to.

13.2. Adding New Users

a) When a new employee starts working at Ulundi Municipality, the Human Resources department will issue him or her with an **"New User Access Form".**
b) The employee will then fill in the form and sign it accordingly to state that he or she agrees with the conditions of use as stated in the form.
c) The HOD/Supervisor will also have to sign the form before it goes to the IT division.
d) The HOD/ Supervisor should also ensure that the employee receives training from business division for the required applications and from the IT division.
e) The new employee will then forward the form to the IT Manager, who will then assign a unique user ID and email account to the applicant.

f) The IT Manager will then assign access to the relevant facilities that the applicant requires.

13.3. Application for Additional Facilities

a) Applicants must fill in the **"New User Access Form"** and indicate on the form that additional facilities are needed.
b) The application is then treated as per the aforementioned process in 12.2.

13.4. Employee Transferred, Resignation or Termination

a) The Human Resources department forwards a list of employees who have been transferred or terminated to the IT division.
b) The IT division, after receiving this list, will then confirm that access will be removed for the resigned employee's user ID at the stated last day of service.
c) The user ID will then be disabled on the system for a month and kept for future reference if required.
d) The IT Manager will then remove the user ID at the stated date accordingly.
e) The IT Manager will then verify and ensure that access privileges of any dismissed, resigned, retired or transferred official are appropriately revoked.

13.5. User Names

a) All users must have proper usernames and passwords that will grant them access to the network and network services available for Ulundi Municipality. The username and password must be in accordance with standards used in all other government levels and departments to ensure a standardized network that can be easily managed and supported. As such, this standard incorporates the user's full name and first letter of user surname for the Network (e.g. Thokozani Ndwandwe's ID would be: TNdwandwe), for PASTEL incorporates the user's First initial and full surname (e.g. John Smith's ID would be: SmithJ) and PAYDAY incorporates number as user names.
b) In the case of duplicate user names, a digit shall be added as a suffix of the username to make a user ID unique. No user is allowed to use the Administrator profile to gain access to the network unless that user is authorized to do so by the IT Manager.

14. PC Support

All support must be performed against a logged call with the details of the call that was logged. All network and PC support calls should be given priority and should be attended to as soon as is possible.

15. Disaster Recovery Plan

The IT Manager, in consultation with the Municipal Manager and with the approval of Council, shall enter into such agreements with Ulundi Municipality's IT suppliers and/or with one or more other municipalities as necessary to ensure that the Ulundi Municipality Disaster Recovery Plan is in place, is operational, and is reviewed and tested at least once a year. The IT Manager shall prepare, review and update (as circumstances require) a list of persons who must be contacted by users in the event of any disastrous occurrence as set out in the Ulundi Municipality Disaster Recovery Plan. Such list shall be made available to all authorized users on Ulundi Municipality's IT network.

16. Training

The IT Manager shall liaise with various Heads of Departments and the Human Resources department with regards to the selection, training and monitoring of officials who have IT based and/or IT related responsibilities. The IT Manager shall coordinate, and where possible, shall provide the appropriate training to such officials as deemed necessary.

17. Acceptance and Compliance with the IT Security Policy

Every employee who is allocated the use of any Ulundi Municipality IT equipment and/or authorized to access the Internet and/or Ulundi Municipality's computer network shall be provided with an email copy of the IT Security Policy by the IT Manager. All employees are required to read through the entire IT Security Policy and then sign the IT Security Compliance Agreement form (see Appendix A) attached to the policy in order to indicate that they have read, understood and accept to comply with this policy accordingly.

18. Enforcement

Non-compliance, violation and disregard of this policy by any Ulundi Municipality employees, consultants and temporary staff shall result in disciplinary action and sanctions against the individual concerned and such sanctions may lead to termination of the individual'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 individual and this shall be in addition to the disciplinary action that Ulundi Municipality would have taken against the individual.

19. Approvals

The table below provides necessary approvals of this strategy.

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

Appendix A

IT Security Policy Compliance Agreement

Employee Name (PRINTED):

_____

Department:

_____

I agree to take all reasonable precautions to assure that municipal internal information, or information that has been entrusted to the Ulundi Municipality by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with Ulundi Municipality, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Municipal Manager, who is the designated Information Owner.

I have access to an emailed copy of the Ulundi Municipality IT Security Policy, I have read and understood this policy, and I understand how it impacts on my job. As a condition of continued employment, I agree to abide by the policy and other municipal requirements, including non-disclosure of company information. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties. I also agree to promptly report all violations or suspected violations of IT policies and procedures to the designated Information Security Officer (ISO) in charge.

Employee Signature: **Date:**

_____ _____

Information Security Officer Signature: **Date:**

_____ _____