UPHUHLISO KUMNTU WONKE

UMZIMVUBU
LOCAL MUNICIPALITY

ICT INTERNET USAGE POLICY

UPHUHLISO KUMNTU WONKE

UMZIMVUBU
LOCAL MUNICIPALITY

TABLE OF CONTENTS

1. DEFINITIONS

For the purpose of this policy, unless the context indicates otherwise, the terms in bold means:

ULM — Umzimvubu Local Municipality

Computer — Any device that accepts information (in the form of digitalized data) and manipulates it for some result based on a program or sequence of instructions on how the data is to be processed and for the purpose of this policy includes servers, desktop computers, laptop computers, monitors, cables, mouse, keyboards, all software, cards, components and all other software that enhance performance of a computer or any part or portion of the above mentioned;

Computer Virus — A computer program that interferes with, or damages the normal operation of the computer or software;

File Allocation Table — A table maintained by an operating system on a hard disk to provide a map of the clusters (the basic units of logical storage on a hard disk) that a file has been stored in and FAT has a corresponding meaning;

Firewall — A set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks;

Hard Disk — That part of a unit, that stores and provides relatively quick access to large amounts of data on an electromagnetically charged surface or set of surfaces and disk drive has a corresponding meaning;

HOD
Head of Department;

Hyper Text Transfer Protocol
The set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web (www) and Http has a corresponding meaning;

Internet
A global system of interconnected computer networks that use the standard Internet Protocol Suite to serve billions of users worldwide

Program
A specific set of ordered operations for a computer to perform;

Proxy server
A server that acts as an intermediary between a workstation user and the internet so that the enterprise can ensure security, administrative control, and caching service and a proxy has a corresponding meaning;

Server
A computer program that provides services to other computer programs (and their users) either in the same computer or other computers;

Software
The various kinds of programs used to operate computers and related devices;

Trap door
Means of access to a computer program that bypasses security mechanisms;

Trojan
A program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control of the computer and do its chosen form of damage, such as ruining the file allocation table on your hard disk;

User
An approved user of municipal computers and/ or IT Systems;

Virus programs — Programs designed to infect other computers by hiding computer viruses within e-mails or programs;

Worm — A self-replicating virus that does not alter files but resides in active memory and duplicates itself;

2. BACKGROUND

Internet connectivity presents the ULM with new risks that must be addressed to safeguard the facility’s vital information assets. These risks include: Access to the Internet by personnel that is inconsistent with municipal needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet. Additionally, the ULM may face loss of reputation and possible legal action through other types of misuse. All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate. Access to the Internet will be provided to users to support municipal activities and only on an as needed basis to perform their jobs and professional roles.

3. PURPOSE OF THIS POLICY

The ULM allows access to resources and services through internet connectivity thus the purpose of this policy is to:

- ensure that the internet is used as an effective, secure and productive tool;
- prevent the occurrence of inappropriate, unethical or unlawful usage of the internet;
- educate individuals who may use the internet, intranet, or both with respect to their responsibilities associated with such use;

- establish prudent and acceptable practices regarding the use of the internet.

4. SCOPE OF THIS POLICY

This policy is applicable to all ULM computer users including officials, the Mayor, the Speaker and Portfolio Councilors, who for the purpose of this policy shall be referred to collectively as “users". This policy must apply to service providers having access to ULM’s internet and intranet services when they are granted such permissions, an internet request form must be filled.

5. POLICY STATEMENTS

5.1. Resource Usage

- Internet access will be provided to users of ULM at the discretion of the executive municipal management or HOD based on the job requirements of the post.
- Internet access will be granted to users who require access for work purposes.
- All users are required to fill in Internet Request Form and submit it to the ICT department.
- Users may not download and distribute entertainment software, games or pirated software via the internet access provided by ULM.
- Users must not download image, audio or video files unless they are work related, this will be done with the authorization of management.
- Users may not access or attempt to access internet sites featuring pornography, terrorism, or racial, unethical and derogatory content.
- All files downloaded from the internet must be scanned for viruses using the approved IT virus detection software, currently this antivirus in individually installed on the user’s computer but should technology advance an automation of this process will happen at server level.
- All software used to access the internet shall be configured to use the HTTP firewall proxy on the user’s browser; the IT department will ensure that all users have their

browser settings aligned to the proxy server.

- Internet usage will be monitored and recorded via the municipal server and may be used as part of municipal controls or disciplinary hearings should the need arise.
- No employee may use the internet facilities to deliberately propagate any virus, worm, Trojan or trap door programs.
- Users may not upload any software licensed to the ULM or data owned by the ULM without authorization via the internet and users must not disclose confidential information of ULM on the internet.

5.2. Prohibited usage

ULM prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials. Activities that are strictly prohibited include, but are not limited to:

- Accessing ULM information that is not within the scope of one’s work. This includes unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.
- Misusing, disclosing without proper authorization personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.
- Deliberate pointing or hyper-linking of ULM Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the ULM.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.

- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Any form of gambling.

5.3. Personal usage

Using ULM computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination. All users of the Internet should be aware that the ULM network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed. Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet banking do so at their own risk. The ULM is not responsible for any loss of information or any consequential loss of personal property.

6. HOW THIS POLICY WILL BE APPLIED

a. Where technology allows, this policy will be enforced automatically.
b. IT Management reports and logs will be used to indicate possible usage violations.
c. The manager of the employee alleged to have violated this policy shall be responsible for ensuring that disciplinary proceedings are commenced with in terms of ULM's disciplinary procedure and policy. A failure on the part of such manager to take the necessary steps regarding disciplinary action shall in itself be grounds for disciplinary action being instituted against the manager concerned.
d. Managers must ensure that all their computer-using personnel, are made aware of the contents of this policy.

e. Managers are required to apply this policy to subordinates reporting to them.

7. COMMENCEMENT OF THE POLICY

a. The policy will come into effect on the date signed by ICT Governance Champion

7.1. INTERPRETATION OF THE POLICY

a. All words contained in this policy shall have the ordinary meaning attached thereto, unless the definition or context indicates otherwise
b. Any dispute on interpretation of this policy shall be declared in writing by any party concerned.
c. The Municipal Manager shall give a final interpretation of this policy in case of written dispute.
d. If the party concerned is not satisfied with the interpretation, a dispute may then be pursued with the South African Local Government Bargaining Council.

7.2. PERMANENT/TEMPORAL WAIVER OR SUSPENSION OF THE POLICY

a. This policy may be partly or wholly waived or suspended by the ICT Governance Champion on temporary or permanent basis however the Municipal Manager/Council may under circumstances of emergency temporarily waive this policy subject to reporting of such waiver or suspension to Council

7.3. COMPLIANCE AND ENFORCEMENT

a. Senior management is required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.
b. Failure to comply with this policy may result in disciplinary action, which may include termination of employment.
c. Any conduct that interferes with the normal and proper operation of the municipality’s IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.
d. The municipality management reserves the right to revoke the privileges of any user at any time.

8. AMENDMENT AND/OR ABOLITION OF THIS POLICY

a. This policy may be amended or repealed by ICT Governance Champion /Council as it may deem necessary.

9. Document Owner and Approval

The Municipality is the owner of this document. The Executive Management of the Municipality is responsible for ensuring that this policy document is reviewed regularly to ensure that it remains relevant to the organisation.

This document was approved by the Executive Management and is issued on a version controlled basis under the signature of the ICT Governance Champion.

Every page of this document must also be initialled by the Governance Champion.