UMZIMVUBU
LOCAL MUNICIPALITY

ICT EMAIL ACCEPTABLE USE POLICY

UMZIMVUBU
LOCAL MUNICIPALITY

TABLE OF CONTENTS

1. INTRODUCTION

E-mail is the most important means of communication throughout the business world this is particularly the case at Umzimvubu Local Municipality as this platform is used to accelerate service delivery and thus a key factor in productivity. Messages can be transferred quickly and conveniently across our internal network and globally via the public Internet. However, there are risks associated with conducting business via e- mail.

However, it must be noted that E-mail is not inherently secure, particularly outside the municipality's own internal network. Messages can be intercepted, stored, read, modified and forwarded to anyone, and do sometimes go missing. Casual comments may be misinterpreted and lead to contractual or other legal issues against the municipality or its staff.

2. PURPOSE

This policy defines and distinguishes acceptable/appropriate from unacceptable/inappropriate use of electronic mail (e-mail).

The purpose of this policy is to ensure the proper use of ULM's email system and make officials aware of what ULM deems as acceptable and unacceptable use of its email system. ULM reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

3. SCOPE

This is a standard corporate policy that applies throughout the organisation as part of the corporate governance framework. It applies to all users of the corporate e-mail systems.

4. ROLES AND RESPONSIBILITIES

4.1. The IT Manager

a. The IT Manager shall implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.
b. Responsible for building, configuring, operating and maintaining the corporate e-mail facilities (including anti-spam, antimalware and other e-mail security controls) in accordance with this policy.
c. Responsible for assisting users with secure use of e-mail facilities, and acts as a focal point for reporting e-mail security incidents.
d. Responsible for maintaining this policy and generally advising on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

4.2. All employees

All employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with our information security policies.

4.3. Internal Audit

The Internal Audit department is authorised by management to assess compliance with all corporate policies at any time.

5. POLICY STATEMENTS

a. Do not use e-mail:
   - to create, send, forward or store e-mails with messages or attachments that might be illegal or considered offensive by an ordinary member of the public i.e. sexually explicit, racist, defamatory, abusive, obscene, derogatory, discriminatory, threatening, harassing or otherwise offensive;
   - to commit the Municipality without authorization to a third party for example through purchase or sales contracts, job offers or price quotations, unless you are explicitly authorised by management to do so. Do not interfere with or remove the standard corporate e-mail disclaimer automatically appended to outbound e-mails.
   - for private or charity work unconnected with the municipality's legitimate business;
   - in ways that could be interpreted as representing or being official public statements on behalf of the municipality, unless you are a spokesperson explicitly authorised by Municipal manager to make such statements;
   - to send a message from anyone else's account or in their name (including the use of false 'From:' addresses); if authorised by the manager, a secretary may send e- mail on the manager's behalf but should sign the e-mail in his/her own name per pro ('for and on behalf of') the manager;
   - to send any disruptive, offensive, unethical, illegal or otherwise inappropriate matter, including offensive comments about race, gender, colour, disability, age, sexual orientation, pornography, terrorism, religious beliefs and practice, political beliefs or national origin, hyperlinks or other references to indecent or patently offensive websites and similar materials, jokes, chain letters, virus warnings and hoaxes, charity requests, viruses or other malicious software; and
   - for any other illegal, unethical or unauthorised purpose.

b. Employees are allowed to use email to:
   - Users shall use only the official email system in their official correspondences;
   - All users must have ULM approved e-mail signature on their every e-mail composed;

- Officials must have signatures in their emails which will include their names, job title, Contact telephone number and the department name using approved stationary for ULM with ULM Logo;
- Users shall compress attachments larger than 5MB before sending them;
    - Maximum size allowed of sending out emails external is 7 MB
    - Maximum size allowed within ULM is 5 MB
    - Maximum size allowed for receiving external is 7 MB
- If you send emails, state clearly what action you expect the recipient to take;
- Only mark emails as important if they really are important;
- Emails should be answered within at least 5 working hours, but users shall answer priority emails immediately; and
- Change your password at least once per month.
- Out of office reply must be activated when users are taking leave and will not be available on e-mail
- All mailbox sizes limit shall be 1GB before users are asked to archive their e-mails because of space

c. ULM e-mail services are provided to serve operational and administrative purposes in connection with the business. All e-mails processed by the ULM's IT systems and networks are considered to be the organisation's property.

d. ULM electronic communications systems generally shall be used only for business activities. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

e. Misrepresenting, obscuring, suppressing or replacing the identity of a user on an electronic communications system is forbidden. The user name, electronic mail address, organisational affiliation and related information that are included with electronic messages or postings shall reflect the actual originator of the messages or postings.

f. Apply your professional discretion when using e-mail, for example abiding by the generally accepted rules of e-mail etiquette. Review e-mails carefully before sending, especially formal communications with external parties.

g. Do not unnecessarily disclose potentially sensitive information in "out of office" messages.

h. E-mails on the ULM's IT systems are automatically scanned for malicious software, spam and unencrypted proprietary or personal information. E-mail scanning process is not 100% effective (e.g. compressed and encrypted attachments may not be fully scanned), therefore undesirable/ unsavory e-mails are sometimes delivered to users. Delete such e-mails or report them as security incidents to IT Help/Service Desk in the normal way.

i. Except when specifically authorised by management or where necessary for IT system administration purposes, employees shall not intercept, divert, modify, delete, save or disclose e-mails.

j. Limited personal use of the ULM's e-mail systems is permitted at the discretion of local management provided always that it is incidental and occasional, and does not interfere with business. Employees should have no expectations of privacy, all e-mails traversing the municipality systems and networks are subject to automated scanning and may be quarantined and/or reviewed by authorised employees.

k. Limited use of Gmail, Hotmail, Yahoo or similar external/third-party e-mail services (commonly known as "Webmail") for business purposes are allowed in cases of emergencies. Do not forward or auto-forward corporate e-mail to external/third party e- mail systems. You may access your own Webmail via corporate IT facilities at management discretion provided that such personal use is strictly limited and is not considered private

l. Be reasonable about the number and size of e-mails you send and save. Periodically clear out your mailbox, deleting old emails that are no longer required and filing messages that need to be kept under appropriate e-mail folders.

6. COMMENCEMENT OF THE POLICY

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

6.1. 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.

6.2. 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. COMPLIANCE

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. KEY REFERENCES

The document has been drafted with particular reference to:

9.1. The Promotion of Access to Information Act, 2000 (Act no. 2 of 2000)

9.2. The Protection of Information Act, 1982 (Act no. 84 of 1982)

9.3. SABS/ISO 17799

9.4. Minimum Information Security Standards (MISS)

9.5. Guidelines for the Handling of Classified Information (SP/2/8/1)

9.6. Electronic Communications and Transaction Act, 2002 (Act no. 25 of 2002)

10. 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.