Document Identification: IT Governance Policies		
Section It Acceptable Use Policy	Applicable to the following sections:	All
Custodian: DEPUTY DIRECTOR PLANNING AND DEVELOPMENT SERVICES	Date:	25-05-2023

Effective date: 25-05-2023
Revised Date: 30-06-2023
Location: IT Policies, Forms and Information

Controlled Document
This is a controlled document and may be subject to change at any time.
Owner: Chief Technology Officer
Status: Final Document

Revision History Release No.	Date	Author	Revision Description
V1.1	2023/05/25	CTO	Final Document

Table of Contents:

Document Identification: IT Governance Policies		
Section It Acceptable Use Policy	Applicable to the following sections:	All
Custodian: DEPUTY DIRECTOR PLANNING AND DEVELOPMENT SERVICES	Date:	25-05-2023

1 Overview

Amajuba District Municipality's (ADM) intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the Municipality's established culture of openness, trust, and integrity. The ADM is committed to protecting the ADMs employees from illegal or damaging actions by individuals, either knowingly or unknowingly.

Resources, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of the ADM. These systems are to be used for business purposes in serving the interests of the ADM, and of our clients and stakeholders in the course of normal operations.

Effective security is a team effort involving the participation and support of every employee who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2 Purpose

The purpose of this policy is to outline the acceptable use of IT Resources at the ADM. These rules are in place to protect the employee and the ADM. Inappropriate use exposes the ADM to risks including virus attacks, compromise of network systems and services, and legal issues.

3 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct the ADM business or interact with internal networks and business systems, whether owned or leased by the Municipality. All employees, interns, secondees, consultants and temporary staff at the Municipality are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the ADM policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2.

This policy applies to employees, interns, secondees, consultants, and temporary staff at the Municipality. This policy applies to all equipment that is owned or leased by the Municipality.

4 Policy

4.1 General Use and Ownership

4.1.1 The ADM proprietary information stored on electronic and computing devices whether owned or leased by the ADM, the employee or a third party, remains the sole property of the ADM. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

SERVICES

4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of ADM proprietary information.

4.1.3 You may access, use, or share the ADM proprietary information only to the extent it is authorized and necessary to fulfil your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

4.1.5 For security and network maintenance purposes, authorized individuals within the ADM may monitor equipment, systems, and network traffic at any time, per Policy.

4.1.6 The ADM reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the minimum access policy.

4.2.2 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees from an ADM email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the ADM, unless posting is in the course of business duties.

4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Acceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the ADM authorized to engage in any activity that is illegal under local and state, law while utilizing the ADM-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following are strictly prohibited with no exceptions.

4.3.1.1 Violations of the rights of any person or the ADM protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the ADM.

4.3.1.2 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the ADM or the end user does not have an active license is strictly prohibited.

4.3.1.3 Accessing data, a server, or an account for any purpose other than conducting the ADM business, even if you have authorized access, is prohibited.

4.3.1.4 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4.3.1.5 Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4.3.1.6 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

4.3.1.7 Using an ADM computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

4.3.1.8 Making fraudulent offers of products, items, or services originating from any ADM account.

4.3.1.9 Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

4.3.1.10 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing and denial of service for malicious purposes.

4.3.1.11 Port scanning or security scanning is expressly prohibited unless prior notification to information security (ICT information security) is made.

4.3.1.12 Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.

4.3.1.13 Circumventing user authentication or security of any host, network, or account.

4.3.1.14 Introducing honeypots, honeynets, or similar technology on the ADM network.

4.3.1.15 Interfering with or denying service to any user other than the employee’s host (for example, denial of service attack).

4.3.1.16 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet.

4.3.1.17 Providing information about, or lists of, the ADM employees to parties outside the ADM.

4.3.2 Email and Communication Activities

When using the ADM resources to access and use the Internet, users must realize they represent the ADM. Whenever employees state an affiliation to the ADM, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the ADM". Questions may be addressed to the IT Department.

4.3.2.1 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

4.3.2.2 Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.

4.3.2.3 Unauthorized use, or spoofing, of email header information.

4.3.2.4 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

4.3.2.5 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

4.3.2.6 Use of unsolicited email originating from within the ADM's networks of other Internet service providers on behalf of, or to advertise, any service hosted by the ADM or connected via the ADM's network.

4.3.2.7 Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging and social media

4.3.3.1 Blogging by employees, whether using the ADM's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of the ADM's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the ADM's policy, is not detrimental to the ADM's best interests, and does not interfere with an employee's regular work duties. Blogging from ADM's systems is also subject to monitoring.

4.3.3.2 The ADM's confidential information policy statement also applies to blogging. As such, Employees engaged in blogging are prohibited from revealing any of ADM's confidential or proprietary information, trade secrets or any other material covered by ADM's confidential information policy statement.

4.3.3.3 Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the ADM and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the ADM's non-discrimination and antiharassment policy statement.

4.3.3.4 Employees may also not attribute personal statements, opinions or beliefs to the ADM when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of the ADM. Employees assume any and all risk associated with blogging.

4.3.3.5 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, the ADM's trademarks, logos and any other the ADM intellectual property may also not be used in connection with any blogging activity.

5 POLICY COMPLIANCE

5.1 Compliance Measurement

The Council will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Council.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 REFERENCE DOCUMENTATION

Refer to ADM IT Policies, Forms and Information stored on ADM report repository.

SOURCE.....	Nhlonipho Mdakane
REPLACING.....	New
REVISION No.	Version 1.1
Signature of Head of Department.....	

7 THE ADM'S USER AGREEMENT

Employee Agreement:

I have received a copy of the ADM's Acceptance Use Policy on acceptable use of all ICT related resources dated_____; I recognize and understand that the ADMS's ICTs systems

are to be used for conducting the ADMS's business only. I understand that use of these facilities for private purposes and contrary to the applicable guidelines is strictly prohibited.

As part of the ADM's organization and use of the ADM's gateway to the resources, I understand that this Acceptable Use Policy applies to me.

I have read the aforementioned document and agree to follow all policies and procedures that are set forth therein. I further agree to abide by the standards set in the document for the duration of my employment with the ADM.

I am aware that violations of this Acceptable Use Policy may subject me to several disciplinary steps leading up to and including possible termination of employment with the Municipality.

I further understand that my communications on and through the use of the resources reflect on the ADM, to our stakeholders, customers and suppliers.

I furthermore understand that the ADM may at its own discretion and at any time amend this document.

_____ _____

Employee Signature Date

_____

Employee Printed Name