ZULULAND

DISTRICT MUNICIPALITY

INFORMATION TECHNOLOGY

SECURITY POLICY

Table of Contents

Authorisation and Revision History

Approval Process	Position or Meeting number	Date
Originator:		
IT Manager:		
Reviewed by Legal Advisor: (Applicable to policies only)		
Approved:		
Recommended by Municipal Manager:		
Recommended by Audit Committee:		
Council Approval:		
Effective:		
Review frequency: Annually		

1. OBJECTIVE

The installation of the municipality's information technology (IT) network represents a significant capital outlay, and the objective of this policy is therefore to ensure that this investment in modern technology is properly managed.

The ancillary objective of this policy is to provide guidance to all current and future users of the computerised network.

The purpose of this policy is therefore not only to prevent abuse of the system and reduce the risk of errors, fraud and the loss of data confidentiality, integrity and availability, but to ensure that the system is optimally used and applied to the best advantage of the municipality.

2. SCOPE

This IT Security Policy is applicable to all Municipality employees and covers all Municipal IT Systems, infrastructure and data.

3. ADMINISTRATIVE ARRANGEMENTS

3.1. General Controls

The Municipal Manager or his nominee shall function as a Chief Information Technology Officer (CITO).

The Municipal Manager shall appoint an IT Committee that must meet at least bi-annually. The IT Committee's primary goal is to provide guidelines and policy on matters related to the use and implementation of technology at the Municipality.

The Municipal Manager shall appoint a System Administrator, and will advise all heads of departments and other users of the system in writing of such appointment. The System Administrator is responsible for both the operating and application system level security.

The CITO will on recommendation of the IT Committee issue guidelines on the use and application of the municipality's IT network, and shall monitor compliance with these guidelines. Such guidelines shall be strictly adhered to by all users of the IT system.

Included in the guidelines will be the required administrative controls applicable to the system, and these shall include the following:

- physical controls over computer hardware, back-ups and software (see Physical Controls Section below);
- access controls (see Access Control Section below);
- data security controls (see Data Ownership, Classification and Security Control Section below); and
- controls over internet usage (see Internet Usage Section below).

The CITO shall be responsible for the establishment and maintenance of municipality's official website (see Official Website Section below).

3.2. Programming and Documentation Standards

Only the CITO on recommendation of the committee may liaise with IT software suppliers to provide programmes for the municipality's use, and/or to have such programmes enhanced or amended.

The CITO shall keep a register of all such requests for the amendment and/or enhancement of the municipality's software and hardware, and shall inform the relevant users when such changes are affected.

3.3. Insurance

The CITO, shall ensure that appropriate and adequate insurance cover is obtained in respect of all components of the municipality's IT operations.

3.4. Reporting Requirements

The CITO 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 any 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 and may be obviated in future.

3.5. Periodic Random Audits

The Municipal Manager shall arrange random audits of the IT system, as and when appropriate.

These audits may be conducted by either the internal or external auditors or both, provided that sufficient budgetary provision exists for any external payments.

The findings of such random audits may be included in the report to the IT committee, or – if significant – in a special audit report.

4. PHYSICAL CONTROLS

Physical controls in regard to the IT network relate to measures which must be put in place to ensure the physical security and protection of all the relevant computer facilities and resources. These facilities and resources include computer hardware, software, manuals and the server room itself. The physical controls are required to provide protection both against natural hazards and the risk of wrongdoing and/or negligence on the part of the municipality's officials.

4.1. Hardware

Where personal computers have been allocated to officials, such officials shall accept that these computers must be used to fulfil operational functions within the organisation, and that their use is restricted to such official functions only.

No hardware may be installed or removed by any municipal official, other than with the authority and under the direct supervision of the System Administrator.

No hardware may be removed by any official from municipal premises without the prior written authority of the Municipal Manager or the System Administrator. The CITO shall keep such written authority on file, and the official who wishes to remove the relevant hardware must have a copy of such authority available for inspection when so required.

The System Administrator shall regularly test or have tested the UPS (uninterrupted power supply) in order to ensure that it is maintained in an operational condition. The System Administrator shall keep a register of all such tests, and this register shall be signed off monthly by the CITO.

Any malfunctioning of computer equipment must be immediately reported in writing to the Systems Administrator by the official to whom such equipment has been allocated, and the Systems Administrator shall immediately attend to the required repairs or replacement of the equipment, but subject to the necessary provision having been made in the budget.

Given the significant cost of laser and ink jet printing, officials to whom the use of printers has been allocated must ensure that all printing is kept to a realistic minimum. Where multiple copies of a particular document are required, the original is to be printed and photocopied. Wherever possible, screen previews should be used rather than physical printing. Original toners and ink jet cartridges must be used when printing is necessary, as not only may the compatible or refilled products void the municipality's warranty in respect of the equipment, but they can also in given instances damage the printers.

4.2. Software

The CITO shall maintain a list of approved software to be used in the IT network, as well as the number of licences owned and the number of copies of such software loaded onto the system. Only software from the approved list may be loaded onto any computer, and this may only be done with the consent of and under the direct supervision of the System Administrator. The CITO shall further ensure that this list, to be known as the "Council approved software list" is reviewed and updated from time to time, as new software is realised into the IT market, and as the demand for new or additional software arises.

No software of any kind whatsoever may be downloaded either through the internet or via e-mail by any official without the approval of the CITO or the relevant head of department. Every staff member will be held personally responsible for any software loaded onto any computer assigned to such staff member. It shall be the responsibility of each such official to bring to the immediate attention of the System Administrator any foreign or unauthorised software loaded onto the computer.

Software piracy by any official shall not be permitted.
Contravention of the Municipality's software policy shall lead to disciplinary proceedings being initiated against the offending staff member.

4.3. Computer Manuals

The originals of software, hardware and systems manuals and guides shall be kept by the CITO with the relevant software licences and discs in a locked cabinet in a fireproof strongroom.

The CITO shall further ensure that the manuals and release notes are updated with each new release installed on the system.

4.4. Server Room

Only the CITO, a delegated official and the System Administrator shall ordinarily have access to the server room.

The server cabinet and server room shall be kept locked by the System Administrator, and the keys shall be kept as follows:

- one set in the strongroom with the other securities;
- one set with the CITO; and
- one set with the System Administrator.

The CITO shall ensure that adequate fire prevention, detection and extinguishing systems are installed in the server room, and that this equipment is regularly checked and properly maintained. No official may tamper with such equipment, and no official may remove any such equipment from the server room other than for purposes of having it serviced or tested.

The CITO shall ensure that a properly designed, maintained and operated air conditioning system is installed in the server room.

5. ACCESS CONTROL

5.1. General

Access control is necessary to restrict unauthorised user access to any portion of the IT network or to any particular component of the system. It is therefore necessary that a bona fide user, in order to gain access, must first be authorised, that is, 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.

5.2. Physical Access to Terminals

Only authorised Municipal employees shall have access to municipal IT equipment. All visitors must sign a Visitors log book and should at all times be accompanied by a Municipality staff member

5.3. Access to the System

After a bona fide user has switched on his or her computer, such user must immediately enter the required code before the computer will boot up. Thereafter the user must enter that particular computer's unique password to gain further access (see User Codes and Passwords section below).

5.4. Access to Specific Commands, Transactions, Programmes and Data within the System

The CITO or relevant departmental head shall set such access level priorities in accordance with the job descriptions of the officials concerned and to comply with the specific further requirements of the officials in the Finance Department.

Access level and amendment priorities shall be set out in writing by the CITO or relevant departmental head.

5.5. User Codes and Passwords

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 employees share any user code or password with colleagues.

The CITO shall have a list available of all user codes and passwords, and shall ensure that this list is kept in a secure place with other IT related securities (see Server Room section above).

The CITO shall ensure that, where system functionality allows, all user codes and passwords meet the following requirements:

Restriction	**Setting**
Password ageing	60 to 90 days, before user is required to change their password
Minimum password length	At least 6 characters
Password history length	At least 12 passwords
Password Expires	Yes
Account Lockout	Enabled
Lockout accounts after	At most 3 bad attempts
Counter resets after	At least one day
Lockout duration	Forever (until admin unlocks)
Password complexity	Enabled

The CITO shall ensure that access privileges of any dismissed, resigned, retired or transferred officials are immediately revoked.

For further details around user access and administration please refer to the Municipality's User Access and Administration Procedure

6. DATA OWNERSHIP, CLASSIFICATION AND SECURITY CONTROL

6.1. Privilege and Exposure

As stated in sections Access to the System and Access to Specific Commands, Transactions, Programmes and Data within the System above, access by users to the municipality's IT system shall be restricted in accordance with the job descriptions of the 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. For further details around the granting of user access and the periodic reviews that are performed please refer to the Municipality's User Access and Administration Procedure

6.2. Backups

As only a percentage of the municipality's critical business information resides on its servers, backup procedures are required also in respect of information saved on personal computers. Backup procedures will be determined from time to time by the CITO, and communicated in writing to the relevant users. These procedures shall be adhered to by all users on the system. For further details around the backup procedures that are performed please refer to the Municipality's Back-up Policy and Procedure.

6.3. Data Ownership and Classification

All data contained or stored on Municipal systems is owned by the Zululand District Municipality. No data should be altered or disclosed without the specific authorisation from the data owner.

All Municipal data must be classified in accordance with the Minimum Information Security Standard (MISS) which replaced the former Guidelines for the Protection of Classified Information (SP 2/8/1) of March 1988. The standard requires that all official matters requiring the application of security measures (exempted from disclosure) must be classified "Restricted", "Confidential", "Secret" or "Top Secret". By default, Municipal data has been classified as Restricted and a separate log is kept recording all data classified as Confidential, Secret or Top Secret.

7. INTERNET USAGE

7.1. Use of the Internet

As internet access and related IT resources are provided to the municipality at significant cost, and are made available primarily for business-related purposes, users who have access to the internet shall use such access solely in connection with their official responsibilities, including to communicate with clients, work-related partners, local and provincial government agencies, and providers of goods and services to the municipality, and to research relevant topics and obtain business-related information which is of use to the municipality. Limited personal use to approved sites may be authorised when such access will be to the best advantage of the municipality.

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

Every official using the internet facilities of the municipality shall identify himself or herself honestly, accurately and completely. Officials using the internet shall do so only when this is required to fulfil their official responsibilities and/or when authorised to do so.

Whenever an official downloads any file from the internet, such file must be scanned for viruses before it is run or accessed. If the official is uncertain as to the procedure to be followed or the results obtained, such official shall immediately request the System Administrator for assistance.

7.2. Authority to Speak for the Municipality

Only those officials who are duly authorised by the Municipal Manager to speak to the media, send external e-mails, speak to analysts or in public gatherings on behalf of the municipality may speak or write in the name of the municipality to any internet newsgroup , chatroom or send any external e-mails.

7.3. Integrity of Municipality's Image

Officials who are authorised to speak for the municipality, as set out above, shall ensure that they at all times honour the image and integrity of the municipality, do not engage in any unauthorised political advocacy, and refrain from the unauthorised endorsement or appearance of endorsement by the municipality of any commercial product or service not sold or provided by the municipality itself.

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

7.4. Security

Prompt disciplinary action shall be instituted against any official who attempts to disable, defeat or circumvent any firewall, proxy, internet address screening programme and any other security systems installed by the CITO and System Administrator or by the municipality's IT suppliers to assure the safety and security of the municipality's IT network.

Any official who obtains a password or user code (ID) which allows access to the internet and/or the municipality's IT network shall keep such password and code confidential, except if any occasion arises where any authorised technical support official requires knowledge of such password or code in order to solve a computer-related problem. As set out in the User Codes and Passwords section above, the present policy strictly prohibits the sharing of user codes or passwords between employees. Furthermore, logging onto the IT network or internet with one's personal code and password, and then allowing another user to use or work on the internet or network, shall be viewed as an attempt to bypass official security procedures, and is strictly prohibited.

Every authorised user shall sign all security and confidentiality agreements required by the CITO before attempting to gain access to the internet and/or the IT network (see Acceptance of Policy section below).

Software and systems have been installed to monitor and record all internet usage. The CITO and System Administrator shall be severally authorised to record, for each user, every worldwide website visited, every chatroom or news group visited, every e-mail message sent or received, and every file transfer into and out of the

municipality's internal networks. No official shall have any right to privacy in respect of his or her internet or network usage.

The CITO and System Administrator shall review all internet activities and analyse the relevant usage patterns, and shall take appropriate action wherever any abuse of the system is evident.

Any software or files downloaded by any user from the internet onto the municipality's IT network, shall become the property of the municipality, and may be used only in a manner consistent with the applicable licences and/or copyrights.

7.5. Electronic Mail (E-mail)

Only authorised officials shall use the available e-mail facility..

The System Administrator shall scan all e-mails for whatever content or offending words or phrases. All copies of e-mails shall be kept at records. Only authorised officials shall be permitted to receive attachments through the e-mail system, and such attachments shall be scanned by the System Administrator to ensure that they are related to the responsibilities of the official concerned.

The System Administrator shall maintain a list of prohibited and blocked mail, and shall update and amend such list as circumstances require.

7.6. Internet Browser

As indicated in the Security section above, the municipality reserves the right to track all sites visited.

7.7. Unacceptable Practices

No official may display any kind of sexually explicit image or document on any municipal system, Furthermore no sexually explicit material may be archived, stored, distributed, edited or recorded using any of the municipality's IT resources.

The CITO and System Administrator shall have the right to block access from within the 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 programmes.

The municipality's IT-related facilities, and specifically its internet facilities, may not be used knowingly by any official to violate the laws and regulations of the Republic of South Africa or of any other nation, or the laws and regulations of any province or municipality. The use of any municipal resources for illegal activities shall be a ground for the immediate dismissal of the official concerned, and the Council and its officials undertake further to co-operate with any legitimate law enforcement agency in this regard.

No employee may knowingly use the municipality's IT facilities and resources to download or distribute pirated software or data.

No official may knowingly use the municipality's internet facilities to propagate any virus, worm, Trojan horse or trapdoor programme code.

No official may knowingly use the municipality's internet facilities to disable or overload any computer system or network or to circumvent any system intended to protect the privacy or security of another user.

No employee with authorised internet access may upload any software licensed to the municipality or data owned or licensed to the municipality without the prior written authorisation of the CITO.

No official may create a communication link requiring dial-out access from any computer which is also connected to the IT network.

No official may use any software which is not provided by or approved by the CITO or relevant departmental head.

Only the CITO or relevant departmental head shall be authorised to provide e-mail addresses to authorised users.

7.8. Confidential Information

Authorised officials who do 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 in regard to confidentiality of information. Officials who release protected information through the internet, whether or not such release is inadvertent, shall be subject to all the applicable penalties in terms of the municipality's existing data security policies and procedures.

8. OFFICIAL WEBSITE

The Municipal Manager shall be responsible for the design and maintenance of the municipality's website.

The CITO shall ensure that all information required by the Municipal Finance Management Act 2003, other applicable legislation, and any Council policy is promptly and appropriately displayed on such website. The CITO shall further, in consultation with the Mayor, Municipal Manager and heads of departments, from time to time decide on any other information to be made available on the website.

Only the CITO or HOD:PCD shall be authorised to amend, add and delete information on the website.

9. DISASTER RECOVERY PLAN

The CITO, in consultation with the Municipal Manager, and with the approval of the Council, shall enter into such agreements with the municipality's IT suppliers and/or with one or more other municipalities as are necessary to ensure that an adequate IT disaster recovery plan is in place and is reviewed at least once per annum.

The CITO shall prepare, review and update (as circumstances require) a list of persons who must be contacted by users in the event of the occurrence of any of the situations set out in the disaster recovery plan. Such list shall be made available to all authorised users on the municipality's IT network. For further details and specifics regarding the Municipality's IT Disaster Recovery Plan please refer to the Municipalities Disaster Recovery Plan.

10. TRAINING

The CITO shall liaise with the various heads of departments and the Human Resources Officer in regard to the selection, training and monitoring of officials who have IT-based and/or IT-related responsibilities. The CITO and the System Administrator shall co-ordinate, and where possible, provide the required training.

11. SECURITY BREACHES

In terms of the Minimum Information Security Standards (MISS), chapter 9, the CITO will 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 SAPS (Crime Prevention Unit) or the SANDF (MI). Where official encryption is concerned, a security breach will also be reported to the South African Communication Security Agency (SACSA).

When a breach of security occurs, the CITO must be notified and it is then their responsibility to notify the relevant authorities.

The CITO will also inform the Municipal Manager and Auditor-General of South Africa (AGSA) and the NIA of all instances of non-compliance with the MISS in which the threat posed by the incident is indicated.

Breaches of security will at all times be dealt with using the highest degree of confidentiality in order to protect the individuals concerned and prevent him or her from being unnecessarily done an injustice to.

12. ACCEPTANCE OF POLICY

Every official who is allocated the use of IT equipment and/or authorised to access the internet and/or the municipality's IT network shall be provided by the CITO with a copy of the present policy. Such employees shall furthermore be required to sign a statement attached to such policy to indicate their understanding and acceptance of this policy.

13. CONTRAVENTION OF POLICY

Any user or individual found to be in contravention of the Municipality's policies and procedures will be subject to disciplinary measures in terms of the Municipality's Disciplinary Process. For more details about the disciplinary process please refer to the Municipality's Disciplinary Procedure document.