DRAKENSTEIN
MUNISIPALITEIT • MUNICIPALITY • U MASIPALA WASE

"A Place of Excellence"

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

DATE APPROVED/REVIEWED	COUNCIL MEETING DATE

DRAKENSTEIN MUNICIPALITY INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

Table of Contents

1. INTRODUCTION

The aim of this policy document is to provide guidelines in respect of the use of computer equipment, network equipment and related electronic appliances provided by the Drakenstein Municipality for use by employees and in particular to indicate possible abuse and the consequences of such abuse.

The goal is to outline the acceptable use of computer equipment at Drakenstein Municipality and to protect the employees and Drakenstein Municipality. Inappropriate use exposes the municipality to risks including virus attacks, compromise of network systems and services, and legal claims.

All computer systems and resources, network resources and electronic information technology placed at the disposal of the employee by the municipality, including any desk-top workstations, hard-drives, computer monitors, printers, fax machines, networking facilities, etc remain, at all times, the property of the Drakenstein Municipality. The herein referred to resources remain the property of the municipality and may under no circumstances be removed from the premises of the municipality without written consent. The latter restriction is not applicable to laptops.

Computers, electronic facilities and network facilities and information technology are provided to employees for the purpose of their work and all work-related activities. All electronic equipment must therefore be used in a manner that is consistent with the standard of conduct normally expected from employees.

This policy should be read with The Electronic Records Management Policy

1.1 Definitions

“Computer Systems” means the combination of computer hardware and software that allows for the user to input, store, and print or distribute municipal information for internal or external purposes. A typical computer system consists of a central processing unit, monitor screen, keyboard, mouse, printer, modem, operating system and application software.

“Computer Hardware” means any electronic device that is used to input store, print, process or distribute municipal information for internal or external purposes. This includes, however, is not limited to, personal computers, local area network file servers, laptops, desktop workstations, mainframe computers, printers, modems, scanners and back-up units.

“Computer Software” means any program or operating system that allows the user of computer hardware to input, store, and print or distribute municipal information for internal or external purposes. This includes, but is not limited to, personal computer operating systems, network operating systems, word processors, spreadsheets, databases, application software, electronic mail, management utilities and user interfaces.

Types of software include operating systems, system software, utility software, development tools, and application software.

“Computer Networks” means two or more computers that are connected together to share resources such as hardware, data, and software. Most common are the local area network

(LAN) and the wide area network (WAN) as defined here under:
"LAN" A Local Area Network (LAN) is a network of personal and other computers within a limited area, linked together by high performance cables to facilitate data exchange, sharing of peripherals and software stored on a central server.
"WAN" is a network that spans a large geographical area, the most common example being the Internet.
"Computer Services" means any advice, support, recommendation or contact with a computer system, regardless of form or physical characteristic that has been purchased or otherwise obtained by the Municipality. Computer services are performed by IT Section or by an approved outside consultant. Computer services include, but are not limited to, recommending, purchasing, configuring, installing and supporting computer systems. Support includes, but is not limited to, troubleshooting hardware and software problems, upgrading hardware or software, and assisting in using application software where possible. All computer services performed by the Municipality are to be considered the property of the Municipality.
"HR" means the Human Relations section of the municipality;
"ICT" means Information and Communication Technology.

1.2 Scope
This policy applies to employees, service providers, consultants, temporaries, and other workers at Drakenstein Municipality, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Drakenstein Municipality.

2. GENERAL POLICY
Drakenstein Municipality is responsible for securing its computer systems against unauthorised access and/or abuse, while making them accessible for authorised and legitimate users. This responsibility includes informing users of expected standards of conduct and the punitive measures for not adhering to them.

Any violation or attempt to violate the provisions of this policy may result in disciplinary action in accordance with the municipality's disciplinary code which may also include temporary or permanent revocation of user access, regardless of the success or failure of the attempt.

Aforesaid revocation shall be the responsibility of the Head of Department or his nominee in conjunction with the Chief Information Officer. Permanent revocations can result from disciplinary actions taken against transgressors of this policy but do not exclude other disciplinary sanctions that may be imposed in terms of the disciplinary code.

2.1 Legislation
This policy complies with the applicable legislation set out below. All users of the municipality's computer systems are required to at all times comply with these legislation: Non-compliance with any of the applicable legislation may lead to litigation in which case the municipality will be required to assist the litigating authority with information required in the litigation process:-

- Electronic Communications and Transactions Act 25 of 2002,
- Copyright Act 98 of 1978,
- Promotion of Access to Information Act 2 of 2000,
- Regulation of Interception of Communications Act 70 of 2002,
- Counterfeit Goods Act 37 of 1997,
- Municipal Systems Act 32 of 2000 and other related legislation.

2.2 Privacy

All electronic equipment used by employees as well as all data, messages, or other files created while using the equipment will be considered the property of the municipality. The municipality reserves the express right to monitor and review all activities performed on electronic equipment by the employee, including information created or obtained by the employee.

Such monitoring includes, but is not limited to, reviewing files or correspondence created by any software medium, periodic scans of an employee's computer hard drive, and review of log files. All users of electronic equipment must be properly informed of the municipality's right to monitor the activities on equipment used and will be provided with copies of this policy document.

2.2.1 Acceptance of terms and conditions

All employees will be required to accept the terms and conditions of this policy document before access to the computer systems will be made available. Such acceptance must be confirmed by users as part of the login process. Refusal will result in the employee not receiving computer system access and possible disciplinary action.

2.3 Personal Use of Computers

Employees may not place personal copies of software or data on any municipal equipment. This includes, but is not limited to, games, screen savers, and questionable material. If found, the software or data will be removed and reported to the user's head of department outlining what was found and the action taken to remove it.

If an employee requires any specific work related software, a copy may be purchased by the municipality.

Municipal owned software may not be installed on an employee's home computer for whatever use, regardless of the software's licensing agreement.

2.4 General Prohibitions

The following practices in respect of the use of computer or network equipment are specifically prohibited:

2.4.1 The viewing, storing, downloading or forwarding of sexually explicit or sexually suggestive text, images, movie images, sound files or sound recordings;

2.4.2 The sending of messages, by electronic mail or any other system, that is racist, sexually explicit, sexually suggestive, harassing, intimidatory or defamatory,

2.4.3 Any form of system “hacking”, including but not limited to attempting to gain access to restricted resources either within the organisation or outside the network provided by the municipality, impersonating another user, damaging or deleting files of another user or obtaining, without authorisation, the access-codes and/or passwords of another user.

2.4.4 The downloading, installing or using of unlicensed or unauthorised software;

2.4.5 Any form of violation of privacy or network security, including but not limited to the unauthorised access to or the use of data, systems or networks, unauthorised interference with network servers or equipment.

2.4.6 A user who contravenes any of the provisions in 2.4.1 to 2.4.6 will be subject to action in terms of the Municipality’s disciplinary code.

2.5 Confidentiality

Unless otherwise dictated by legislation, all information regarding the computer systems, or data created by employees, is confidential and employees who use these systems must take the necessary care not to disclose confidential information.

Removal of data from the municipal offices without the express consent of the Head of the Department will amount to a breach of this confidentiality and is punishable in terms of the disciplinary code of the municipality.

3. PURCHASING OF EQUIPMENT

The purpose of this section is to set guidelines for the researching, pricing, and acquisition of computer system hardware and software, and outside computer support. All computer system hardware and software purchases must be pre-approved by the ICT Steering Committee.

3.1 Purchase Requests

All computer system purchases will be undertaken as per agreement between the ICT Department and the Supply Chain Management Section.

3.2 Receiving Orders

All computer system orders are dealt with by the ICT Department. The purchase order must be checked against the packing slip to determine if all of the items have been received and are correct. The requesting department and ICT Department thereafter must make arrangements with the supplier and department for a date and time to install the equipment. In case all ordered items have not all been received, the requesting department must indicate whether the installation should proceeded or not.

If incorrect or damaged equipment is received, the IT Department must identify the problem and ensure that it is attended to and rectified.

4. INSTALLATION OF EQUIPMENT

The purpose of this section is to set guidelines for the installation and configuration of computer system hardware and software. The ICT Department will be responsible to oversee the installation and configuration of computer hardware and software. Consultants in collaboration with the ICT Department will be responsible for specialised software and hardware where specific skills are needed. (E.g. Financial system, HR/Payroll System etc.). Consultants must install the hardware and/or software with the minimum disruption to the user whenever possible.

4.1 Computer Hardware Installations

Once the computer equipment has been received, IT Section will contact the requesting department and supplier(s) for a date and time to install the equipment.

Under no circumstances may any user, employee, consultant or anybody else be allowed to move, open or do physical repairs on any of the computer equipment or peripherals of the Drakenstein Municipality without the permission of the ICT Department. The ICT Department must ensure that the necessary maintenance contracts as well as warranties on hardware are provided by suppliers.

4.2 Computer Software Installations

Once the computer software has been received, the ICT Department will contact the requesting department and suppliers for a date and time to install the software. It is the responsibility of the relevant department and users to ensure that all licensing agreements are being met.

The recording and tracking of software licenses as well as securing the software and licensing is the responsibility of the ICT Department. The availability of media and instructional manuals is the responsibility of the department which purchased, or acquired, the software.

4.3 Disposal of redundant or excess computer equipment

It is the responsibility of the ICT Department, in collaboration with the relevant Department and Directorate: Financial Services to ensure that the relevant forms are completed and signed for transfer or disposal of redundant or excess computer equipment. The ICT Department will collect the completed form and deliver it to the Stores together with redundant or excess equipment. If the said equipment is to be transferred to another department, the **Computer Hardware Installations** procedure under 4.1 above will be followed. If it is declared redundant or surplus, Stores must take steps for final disposal thereof.

5. SECURITY

5.1 Physical Security

The municipality requires that sound business and management practices be implemented in

the workplace to ensure that information and technology resources are properly protected. The municipality believes that effective security of assets in the workplace is a responsibility held jointly by both management and employees.

Physical security involves providing environmental safeguards as well as controlling physical access to equipment and data.

5.1.1 All departments must ensure that adequate fire extinguishing devices are provided in the office area. Such equipment must be maintained and reviewed on an annual basis by the responsible department.

5.1.2 Departments which house computing equipment in a raised floor environment must have appropriate fire and water detection devices resident under the raised floor. These devices must be maintained and tested on an annual basis.

5.1.3 Desktop computers, laptops, docking stations and file servers must be connected to UPS (Uninterrupted Power Supply – "red plugs") equipment to prevent power spikes, power failures, and subsequent damage to data and hardware.

5.1.4 No equipment other than computer equipment should be connected to UPS power ("red plugs"). This excludes laser printers which may never be connected to UPS power outlets.

5.1.5 All non-essential computer equipment should be turned off during non-working hours (i.e. week nights, weekends, vacations, and holidays). This includes CPUs, monitors, printers and modems.

5.1.6 Essential computer equipment includes: network file servers, workstations attached to networks that perform after hours system back-ups, and computers receiving data after hours.

5.1.7 Adequate air conditioning should be operational in office environments that house desktop computing and high technology resources to prevent long-term heat damage and equipment failure.

5.1.8 Proper attention must be given by all employees with regard to overloading electrical outlets with too many devices. Proper and practical usage of extension cords should be reviewed annually in the office environment.

5.1.9 All spaces housing personal computers and desktop equipment should be kept locked when not occupied by the employee in order to reduce the occurrence of unauthorised entry and access.

5.1.10 Desktop computing equipment which is located in ~~a~~ public access areas must be secured to a piece of furniture, counter top, etc., with a security/theft inhibiting device. Laptop/portable computers must also be secured with security/theft inhibiting devices.

5.1.11 It is the Head of the Department's or his nominee's responsibility to ensure that all equipment is protected against theft or misuse.

5.1.12 All computing equipment should have serial numbers and property tags recorded in Drakenstein Municipality's asset system for identification purposes, should this equipment become damaged or stolen.

5.1.13 Telephone equipment in public areas should be programmed to prevent off-building or

long distance calls.

5.1.14 The Financial Services department, as part of its asset management policy, must conduct a physical inventory of desktop computing equipment on a yearly basis, accounting for the location of the assets.

5.1.15 The municipality shall utilise access control systems for all spaces containing critical information technology assets/equipment.

5.1.16 Employees are expected to be cognisant of equipment located within their immediate offices and to immediately report missing equipment to supervisors.

5.1.17 Employees are expected to report any unauthorised access, entry or suspicious activity to supervisors and/or management immediately.

5.2 User Responsibilities

The guidelines below are intended to assist users to make the best use of the computer resources at their disposal. The following will apply:

5.2.1 Users are individually responsible for protecting the data and information they work with;

5.2.2 Where users are uncertain about the sensitivity of information, the head of department must be approached for assistance;

5.2.3 Information is an asset and must be treated as such;

5.2.4 Users must immediately report anything unusual about data or information on their computers to their head of department;

5.2.5 People who appear to be strangers in a work area may be confronted by users to determine the purpose for their presence;

5.2.6 Equipment must be protected from theft and kept away from food and drinks;

5.2.7 All data must be stored on a network drive (**not local c: drive**) to ensure that data is backed up regularly.

5.3 Password security

Passwords are an important aspect of computer security and the front line of protection for user accounts. A poorly chosen password may compromise the municipality's entire corporate network. As such, all employees (including service providers and vendors with access to the municipality's systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

5.3.1 Password that would be hard to guess must be chosen;

5.3.2 Computers must be logged off before leaving a workstation, when working on sensitive information or leaving a workstation for any length of time.

5.3.3 Each password must be at least six (6) characters in length.

5.3.4 Passwords must be alphanumeric i.e. must include both letters and numbers.

5.3.5 Passwords must use a combination of upper- and lower-case letters, with numbers and punctuation marks interspersed throughout. It is insufficient to simply use a number at the beginning or the end of the password.

5.3.6 Names or words must not be used: strong passwords are a random combination of numbers, letters and punctuation marks.

5.3.7 Passwords must be changed every (60) days. (Administrator passwords must be changed every thirty (30) days.)

5.3.7 Newly created passwords must be different from the previous ten passwords used.

5.4 Prohibitions

The following are prohibited-

- Revelation of a password over the phone to any person;
- Revelation of a password in an e-mail message;
- Talking about a password in front of others;
- Any hint at the format of a password (e.g., "my family name");
- Revelation of a password on questionnaires or security forms;
- Sharing a password with family members;
- Revelation of a password to co-workers while on vacation.

6. E-MAIL USAGE

6.1 Definitions

Term	**Definition**
E-mail	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical e-mail clients include “GroupWise” and Microsoft Outlook.
Forwarded e-mail	E-mail resent from an internal network to an outside point.
Chain e-mail or letter	E-mail sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information	Information is considered sensitive if it can be damaging to Drakenstein Municipality or its customers' reputation or market standing.
Virus warning	E-mail containing warnings about virus or malware. The overwhelming majority of these e-mails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
Unauthorised Disclosure	The intentional or unintentional revealing of restricted information to people, both inside and outside Drakenstein Municipality who do not have a need to know that information.

6.2 Purpose

The purpose of this policy is to ensure proper use of the municipality’s e-mail system and to make users aware of what the municipality regards as acceptable and unacceptable use of its e-mail system. The municipality reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

6.3 Scope

This policy covers use of any e-mail sent from a municipal e-mail address and applies to all employees, vendors, and agents operating on behalf of the municipality, including private e-mail.

6.4 Prohibited Use

The municipal e-mail system may not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or nationality. Employees who receive any e-mail with this content from any employee should report the matter to their supervisor immediately.

E-mail is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature e-mail seems to be less formal than other written communication, the same laws apply. Users are again referred to the general prohibitions under paragraph 2.4 above.

The following acts are prohibited-

- Sending of unsolicited e-mail messages;
- The forging or attempted forging of e-mail messages;
- Sending of e-mail messages using another person's e-mail account;
- Copying of a message or attachment belonging to another user without permission of the originator;
- Disguising or attempted disguising of identity when sending mail.

6.5 Best practice

Users must devote time to manage their e-mail accounts on a regular basis. The municipality considers e-mail as an important means of communication and recognises the importance of proper e-mail content and speedy replies in conveying a professional image and delivering good customer service. Therefore users must adhere to the following guidelines-

6.5.1 **Writing e-mail**:

- E-mail should be well-structured with short, descriptive subjects.
- The municipality's e-mail style is informal. This means that sentences can be short and to the point. It can be started with 'Hi', or 'Dear', and the name of the person. Messages can be ended with 'Best Regards'. The use of characters such as "smileys" however, is not encouraged.
- Signatures must include the name, job title and company name. A disclaimer will be added underneath such signature.
- A spell check should be used before sending out an e-mail.
- E-mail should not be written in capitals.

- Broadcasting of messages is allowed by authorised persons only;
- The action to be taken by the recipient of mail must be stated clearly;
- E-mail should not be sent unless the content could be displayed on a public notice board. If it cannot be displayed publicly in its current state, it must be rephrased, using other means of communication, or protecting information by using a password;
- E-mail should not unnecessarily be marked as important;
- E-mail in excess of 10 Megabyte will be blocked by the system but may be allowed by special arrangement with the ICT Department.

6.5.2 Replying to e-mail:

- E-mail should be answered as soon as possible, and priority must be given to urgent e-mails;
- Priority e-mail is e-mail from existing customers and business partners and municipal employees.

6.5.3 Newsgroups:

- Users are only allowed to subscribe to work related newsletters or news groups.

6.5.4 Maintenance:

- E-mail messages which have been dealt with must be deleted.
- E-mail client will be set to automatically empty 'deleted items'.

6.6 Personal Use.

Although the municipality's e-mail system is meant for business use, the reasonable use of e-mail for personal use will be allowed provided the following guidelines are adhered to-

- Personal use of e-mail should not interfere with work;
- Personal e-mail must adhere to the guidelines in this policy;
- The forwarding of chain letters, junk mail, jokes and executables is prohibited;
- On average, users are not allowed to send more than 2 personal e-mail a day;
- Mass mailings are prohibited;
- The municipality shall have access to all messages distributed via the e-mail system, including personal e-mail.

6.7 Monitoring

Users should have no expectation of privacy in any data or records they create, store, send or receive on the municipality's computer system. E-mail may be monitored without prior notification. In case of non-compliance with the guidelines set out in this policy, the municipality will be entitled to take disciplinary action.

6.8 Users' Responsibility for Security

Users are responsible for the security of their electronic mail account password and any electronic mail that is sent via their account. The following precautionary measures must be taken-

- To log off from electronic mail account before leaving a computer unattended.
- Not to give out a password. Users are responsible for messages sent via their account. and tampering with an account is prohibited;
- E-mail passwords should be changed once a month.

6.9 E-mail accounts

All e-mail accounts maintained on e-mail systems are the property of Drakenstein Municipality. E-mail accounts not used for 60 days will be deactivated and may be deleted.

7. INTERNET USE

7.1 User Responsibilities

These guidelines are intended to assist users to make the best use of the Internet resources at their disposal. The following guidelines apply:

- Drakenstein Municipality provides Internet access to staff to assist them in carrying out their duties. It is envisaged that it will be used to research details about suppliers, products, to access government information and other statutory information. It should not be used for personal reasons;
- Internet may only be accessed by using the Drakenstein Municipality's content scanning software, firewall and router;
- Access to internet will be subject to written authorization by the head of department;
- Usage of the Internet must be restricted to a minimum;
- Information accessed on the Internet must be accurate, complete and current;
- Validity of information found must be checked;
- Protection to data and software provided by copyright and licenses must be respected;
- The ICT Department must be informed immediately of any unusual occurrence.

The following acts are prohibited-

- Downloading of text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity;
- Downloading of content from Internet sites which is not work related;
- Downloading of software from the Internet and installation thereof on the municipality's computer equipment without authorisation by ICT Department;
- Using the municipality's computers to make unauthorised entry into any other computer or network;
- Impersonating another person;
- Using Internet access to transmit confidential, political, obscene, threatening, or harassing materials;

- A user who contravenes any of the above provisions will be subject to disciplinary action as contemplated in 2.4 above.

7.2 Internet Control and Logging System

All activity on the internet will be monitored and logged including all sites visited, the duration of the visits, amount of data downloaded, and types of data downloaded. The time of recorded activity may also be logged.

A logging system with the following capabilities will be maintained:

- The ability to prevent users from visiting inappropriate or pornographic web sites. It will have its database of categorised websites updated regularly.
- The ability to log user internet activity including:
  - Time of the internet activity.
  - Duration of the activity.
  - The website visited.
  - Data and type of data downloaded
- The system will cache web pages to increase the internet connection speed
- Internet access is granted using Active Directory. Only users with permitted to use the Internet and logged in to the network will be able to browse the Internet.

The system used to prevent users from visiting inappropriate, pornographic, or dangerous web sites shall be Microsoft Threat Management Gateway 2010. This same system will not require an additional login ID and will use Active Directory to identify internet users. The system shall be able to log the time of internet activity, duration of the activity, the website visited, any data downloaded and the type of data downloaded. The system will cache web pages.

8. REMOTE ACCESS TO MUNICIPAL NETWORK

8.1 Definitions

"Dial-in Modem"	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send via the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
"3G/HSDPA"	3G and HSDPA are acronyms that refer to broadband access for mobile networking and are based on cellular technology (Vodacom/MTN).
"Remote Access"	Any access to Drakenstein Municipality's corporate network through a non-Drakenstein Municipality controlled network, device, or medium.
"VPN"	Virtual Private Network (VPN) utilises public telecommunications networks to conduct private data communications.
"ADSL"	Asymmetric Digital Subscriber Line (ADSL), a new modem technology, converts existing twisted-pair telephone lines into access paths for multimedia and high speed data communications. ADSL will allow access to the Internet without using a dial-up service, will allow a phone line to be

used for conversation and the Internet simultaneously, and will probably be charged at a monthly rate.

8.2 Purpose

The purpose of this section is to define standards for connecting to the municipality's network from any host. These standards are designed to minimise the potential exposure to the municipality from damages which may result from unauthorised use of municipal resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical municipal internal systems, etc.

8.3 Scope

This section applies to all Drakenstein Municipality employees, service providers, vendors and agents with a municipality-owned or personally-owned computer or workstation used to connect to the municipal network as well as to remote access connections used to do work on behalf of the municipality, including reading or sending e-mail and viewing intranet web resources.

Remote access implementations that are covered by this section include, but are not limited to, dial-in modems, 3G Access, ADSL, etc.

8.4 General

8.4.1 It is the responsibility of the municipality's employees, councilors, service providers, vendors and agents with remote access privileges to the municipality's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the municipality.

8.4.1 General access to the Internet for recreational use by immediate household members through the municipal network on personal computers is not permitted.

8.5 Requirements

8.5.1 Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication. For information on creating a strong pass-phrase see the Password Policy.

8.5.2 Employees and service providers with remote access privileges must ensure that their municipal owned or personal computer or workstation, which is remotely connected to the municipality's corporate network, is not connected to any other network at the same time.

8.5.3 Employees and service providers with remote access privileges to the municipality's corporate network must not use non-Drakenstein Municipality e-mail accounts (i.e., Hotmail, Yahoo, Gmail), or other external resources to conduct municipal business, thereby ensuring that official business is never confused with personal business.

8.5.4 Non-standard hardware configurations must be approved by Remote Access Services, and the ICT Department must approve security configurations for access to hardware.

8.5.5 All hosts that are connected to Drakenstein Municipality's internal networks via remote access technologies, which include personal computers, must use the most up-to-date anti-virus software as approved by the ICT Department;

8.5.6 Personal equipment used to connect to the municipal networks must meet the requirements of the municipal owned equipment for remote access.

8.5.7 Employees or councilors, who wish to implement Remote Access solutions to the municipal production network, must obtain prior approval from ICT Committee.

9. VIRUS PROTECTION

9.1 Overview

This section applies to the ICT Department only. It defines anti-virus policy on every computer including how often a virus scan is done, how often updates are done and what programs will be used to detect, prevent, and remove malware programs. It defines what types of files attachments are blocked at the mail server and what anti-virus program will be run on the mail server. It may specify whether an anti-spam firewall will be used to provide additional protection to the mail server. It may also specify how files may enter the trusted network and how these files will be checked for hostile or unwanted content, e.g. it may specify that files sent to the enterprise from outside the trusted network be scanned for viruses by a specific program.

9.2 Purpose

This section is designed to protect the organisational resources against intrusion by viruses and other malware.

9.3 Application

The municipality will use "Microsoft Forefront endpoint protection" as a single anti-virus product for anti-virus protection. The following minimum requirements will apply:

9.3.1 The anti-virus product shall be operated in real time on all servers and client computers and shall be configured for real time protection.

9.3.2 The anti-virus library definitions shall be updated daily.

9.3.3 Anti-virus scans shall be done daily on all user controlled workstations and servers.

9.3.4 Only domain administrators may stop anti-virus definition updates and anti-virus scans.

9.3.5 Users must ensure that floppy disks, memory sticks and other media that are used on municipal systems are checked for viruses.

9.3.6 I.T. Services must be informed immediately of any suspected virus at a workstation.

9.4 E-mail Server Policy

There will be no virus scanner on the e-mail server as files are encrypted and cannot be scanned. Virus scanning of e-mail will be done at the workstation level.

9.5 E-mail Malware Scanning

Malware scanning of e-mail will be done at the workstation level.

9.6 Proxy or anti-spam Server

Anti-spam will be done through a subscription service of an internet service provider.

10. APPROVED APPLICATIONS

10.1 Overview

All employees and personnel that have access to municipal computer systems must adhere to the approved application policy in order to protect the security of the network, protect data integrity, and protect computer systems.

10.2 Purpose

This section is designed to protect the municipality's resources on the network by requiring all network users to only run or install application programs approved by the ICT Department

10.3 Approved Applications

Users may only operate programs on the approved application list (available at the ICT Department). All new applications must be approved by the ICT Steering Committee prior to installation. A user who causes a security problem on the network by installing and running an unapproved program will be subject to disciplinary action.

10.4 Exemptions

Depending on the function and the skills of users, exemptions may be granted from the provisions of paragraph 10.3. Examples are the following:

10.4.1 Where the user is the person who needs to test new applications on a test network, and on the main network.

10.4.2 Where the user is a developer who runs applications developed by himself/herself in order to test his/her own work.

10.4.3 Network administrators may be allowed to operate and test new software.

11. SYSTEM OWNERS

11.1 Overview

This section applies to the software system owners (as approved by the ICT Steering Committee) only. The system owner is the business person ultimately accountable for the functionality of the system.

11.2 Purpose

This section is designed to ensure -

a) that the system:
   - Meets the business objectives for which it was created;
   - Has sufficient funds for yearly operations and maintenance;
   - Confirms to all IT standards, policies and security requirement;

a) And that the system owner:
   - Decide who has access to the system (and with what rights and privileges);
   - Ensure system's personnel are properly designated, monitored, and trained,
   - Grant individuals the fewest possible privileges necessary for job performance (any privileges not specifically granted are denied access) so that privileges are based on a legitimate need to have system access, and re-evaluated the access privileges annually, revoking access in a timely manner upon personnel transfer or termination;
   - There is an approved service level agreements in place where applicable.
   - Schedule regular meetings with service providers to monitor and review the performance of the SLA and the system.
   - Ensure that Standard Operating Procedures (SOP) for the system are developed and approved.

12. NETWORK DOCUMENTATION

12.1 Overview

This network documentation policy applies to the ICT Department only and defines the requirements for network documentation such as documentation of switch ports connections. It also defines access to read network documentation, authorisation to change it and notification of changes made.

12.2 Purpose

This policy is designed to provide for network stability by ensuring that network documentation is complete and current. It will complement disaster management and recovery by ensuring that documentation is available in the event of rebuilding of systems. It will reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to the network.

12.3 Documentation

The network structure and configuration must be documented to provide the following information:

12.3.1 IP addresses of all devices on the network with static IP addresses and full details regarding location, make and model.

12.3.2 Network drawings showing:

12.3.2.1 The locations and IP addresses of all hubs, switches, routers, and firewalls on the network.

12.3.2.2 The various security zones on the network and devices that control access between them.

12.3.2.3 The interrelationship between all network devices showing lines running between the network devices.

12.3.2.4 All subnets on the network and their relationships including the range of IP addresses on all subnets and net mask information.

12.3.2.5 All wide area network (WAN) information including network devices connecting them and IP addresses of connecting devices.

12.3.2.6 Configuration information on all network devices as done and updated on a daily basis by the network management software. These devices include but are not limited to:

- Switches;
- Radios;
- Routers;
- Firewalls;

12.3.3 Configuration shall include but not be limited to:

- IP Address;
- Netmask;
- Default gateway;
- DNS server IP addresses for primary and secondary DNS servers;
- Full running configuration.

12.3.4 DHCP server settings showing:

- Range of IP addresses assigned by all DHCP servers on all subnets.
- Subnet mask, default gateway, DNS server settings, WINS server settings assigned by all DHCP servers on all subnets.
- Lease duration time.

12.4 Access

The ICT networking staff shall have full access to all network documentation. The ICT networking staff shall have the ability to read and modify network documentation.

12.5 Change Notification

The help desk staff, server administration staff, application developer staff, and ICT management shall be notified when network changes are made including-

12.5.1 Reboot of a network device including switches, routers, and firewalls.

12.5.2 Changes of rules or configuration of a network device including switches, routers, and firewalls.

12.5.3 Upgrades to any software on any network device.

12.5.4 Additions of any software on any network device.

12.5.5 Changes to any servers which perform significant network functions whether configuration or upgrade changes are made. These servers include:

- DHCP
- DNS
- Domain controllers

- WINS

Notification shall be done by e-mail to designated groups of people which include the support staff both internal and external.

12.6 Documentation Review

The Operations & Support manager must ensure that network documentation is kept current by performing a monthly review of documentation. The remedy or help desk requests within the last month should be reviewed to help determine whether any network changes were made. Any current or completed projects affecting network settings should also be reviewed to determine whether any network changes were made to support the project.

12.7 Storage Locations

Network documentation shall be kept either in written form or electronic form in a minimum of two places. It must be kept in separate buildings.

13. BACK-UP POLICY

13.1 Definitions

"**Back-up"** The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

"Archive" The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

"Restore" The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

13.2 Overview

This policy defines applies to the ICT Department only and defines the back-up policy for computers within Drakenstein Municipality. These systems are servers that include the file servers, the mail server, and the database server.

13.3 Purpose

This policy is designed to protect data in the municipality in order to be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

13.4 Scope

This policy applies to all equipment and data owned and operated by the municipality.

13.5 File servers

Full back-ups must be performed daily on working days. If a back-up cannot take place on the day, it should be done as soon as possible thereafter.

13.6 Financial and HR/Payroll

Full back-ups are performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday of production databases. If for maintenance reasons, back-ups are not performed on Friday, it must be done on Saturday or Sunday.

Back-up sets must be rotated every other week and kept in the Fire Departments safe.

13.6 Database servers

SQL databases are backed up to disk before backing up tape.

13.7 Tape Storage

A separate tape or set of tapes must be used for each back-up day including Monday, Tuesday, Wednesday, Thursday and Friday. Back-up tapes must be kept offsite at the Fire Department in Paarl in a fireproof safe.

Bach-up tapes for the current week must be kept in the server room, at the ICT Department, in the Civic Building, in Paarl.

13.8 Monthly Back-ups

A monthly back-up tape must be made using the oldest back-up tape or tape set from the tape sets. Every last working day of the month the back-up tape must be removed from the set and marked as the current date, i.e. “End of July 2010”. It must be kept offsite at the Fire Department in Paarl.

13.9 Responsibility

The Operations & Support manger must ensure that regular back-ups be performed. He/she must develop a procedure for testing back-ups and test the ability to restore data from back-ups on a monthly basis.

13.10 Testing

The ability to restore data from back-ups shall be tested at least once per month.

13.11 Data Backed Up

Systems to be backed up include all file servers but are not limited to:

- File servers;
- Mail server;
- Production database servers;
- Domain controllers;

13.12 Restoration

Users that need files restored must submit a request to the ICT help desk. Information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed, must be provided.

13.13 Tape Storage Locations

Offline tapes used for nightly back-up and monthly tapes must be stored at the Fire Department

in a fireproof safe in a fireproof safe. Monthly tapes must be stored across town in another facility in a fireproof safe.

14 ICT Steering Committee

14.1 Establishment

Information systems functions and activities must be coordinated and monitored to ensure that their performance would support the municipality's overall business processes and objectives within reasonable costs. In order to give effect to this monitoring function, the Municipal Manager must establish an ICT Committee with a charter stipulating the roles, responsibilities, authority and membership.

Ooo000ooo