A 90/2009.

Reviewed A22/2004.

MATJHABENG MUNICIPALITY

COMPUTER USER POLICY

INTRODUCTION

This procedure document describes policies for use of Matjhabeng Municipality's computer systems.

REVIEW

This policy should be reviewed annually so as to be in line with current trends and/or technology.

DEFINITIONS

Municipality	The Municipality of Matjhabeng.
User	Any person who uses a computer of Matjhabeng Municipality inclusive but not limited to employees, contractors and political office bearers .
Password	A secret code you type into a computer system to prove you are who you say you are, much like the number you use to access your account at a bank machine. The best password is one that combines letters, symbols and numbers, like ***black1***.
E-mail	Electronic mail sent by a user from one computer to another user at another computer – sending and receiving messages through a computer network including intranet. To use electronic mail, you need a computer, modem or network connection and an e-mail address. E-mail is convenient because all messages are sent and received almost immediately, even over long distances.
E-mail address	An electronic address that enables you to send and receive e-mail.
Internet	The biggest computer network in the world, reaching millions of people, on thousands of interconnected networks. The Internet has a staggering amount of information you can access. No one person or group controls the Internet, so finding a particular piece of information can be challenging.
Internet account	A user name and password which allows you to access the Internet.
Data	Any information stored electronically and without limiting the generality of the aforementioned shall include information stored on a computer hard drive and/or a computer network.
Crash	This occurs when a critical electronic part of the computer fails or burns out.
Back-up	A secondary means of storing data so that if the computer crashes, the data is still available.
Remote administration	Repairing or configuring a computer from another computer via the network.

OWNERSHIP OF RESOURCES

Computer facilities and data owned by the Municipality are to be used solely for municipal business activities. All access to centralized computer systems must be authorized by the ICT Department.

All data is considered to be an asset of the the Municipality and shall be protected from loss, corruption, misuse and inappropriate disclosure. Certain data, by law, is confidential and may not be released without permission. Users of the Municipality's computers and/or computer systems are responsible for the privacy, back-up and protection of data over which they have control.

ELECTRONIC COMMUNICATIONS & E-MAIL POLICY

- **E-mail policy**

  This policy describes the Municipality's guidelines with regard to access to and disclosure of e-mail messages sent or received by the Municipality with use of the the Municipality's e-mail system. The Municipality respects the individual privacy of its employees. However, employee's privacy does not extend to the employee's work-related conduct or to the use of the Municipality-provided equipment or supplies, which specifically includes e-mail. You should be aware that the following guidelines may affect your privacy in the workplace.

- **Management's right to access information**

  The e-mail system has been installed by the Municipality to facilitate the Municipality communications. Although each employee has an individual password to access this system, it belongs to the Municipality and the contents of e-mail communications are accessible at all times by the Municipal Manager or his delegate for any business purpose. These systems are subject to permanent monitoring and unannounced inspections, and should be treated like other shared filing systems. All system passwords and encryption keys must be available to the Municipal Manager or his delegate and you may not use passwords that are unknown to your supervisor or install encryption programs without turning over encryption keys to the Manager Municipal Manager. All e-mail messages are Municipality records. The contents of e-mail, properly obtained for legitimate business purposes, may be disclosed within the municipality without your permission. Therefore, you must take note that e-mail messages are not confidential. Back-up copies of e-mail may be maintained and referenced for business and legal reasons.

- **Personal use of e-mail**

  Because the Municipality provides the e-mail system to assist you in the performance of your job, you should use it for Municipality business. Incidental and occasional personal use of e-mail is permitted by the Municipality, on condition that it does not disrupt network services for business purposes and must not detract from the performance of work in the office. The Municipality reserves the right to access and disclose as necessary all messages sent over its e-mail system, without regard to content. Since your personal messages can be accessed by the Municipal Manager or his delegate without prior notice, you should not use e-mail to transmit any messages you would not want read by a third party. For example, you should not use the Municipality's e-mail for gossip, including personal information about yourself or others, for forwarding messages under circumstances likely to embarrass the sender, or for emotional responses to business correspondence or work situations. In any event, you should not use these systems for such purposes as soliciting for commercial ventures, religious or personal causes or outside

organizations or other similar, non-job-related solicitations. If the Municipality discovers that you are misusing the e-mail system, you will be subject to disciplinary action up to and including termination of service.

- **Forbidden content of e-mail communications**

You may not use the Municipality's e-mail system in any way that may be seen as insulting, disruptive or offensive by other persons, or harmful to morale. Examples of forbidden transmissions include sexually-explicit messages, cartoons or jokes; unwelcome propositions or love letters; ethnic or racial slurs; or any other message that can be construed to be harassment or mocking of others based on, inter alia, their sex, race, sexual orientation, age, national origin or religious or political beliefs. Use of the Municipality-provided e-mail system in violation of this guideline will result in disciplinary action, up to and including termination of service.

- **Password and encryption key security and integrity**

Employees are prohibited from the unauthorized use of the passwords and encryption keys of other employees to gain access to the other employee's e-mail messages.

- **Communications**

Each employee is responsible for the content of all text, audio or images that they place or send over the Municipality's e-mail/Internet system. No e-mail or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else or someone from another organization or entity.

All messages communicated on the Municipality's e-mail/Internet system should contain the employee's name.

Any messages or information sent by an employee to another individual outside of the Municipality via an electronic network (e g bulletin board, online service or Internet) are statements that reflect on the Municipality. While some users include personal "disclaimers" in electronic messages, there is still a connection to the Municipality and the statements may be tied to the Municipality.

All communications sent by employees via the Municipality's e-mail/Internet system must comply with this and other municipality policies and may not disclose any confidential or proprietary municipality information.

- **Copyright issues**

Copyright materials belonging to entities other than this municipality, may not be transmitted by employees on the Municipality's e-mail/Internet system. All employees obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission, or as a single copy to reference only. Failure to observe copyright or license agreements may result in disciplinary action up to and including termination of service.

Intellectual property and their terms of use, residing on Municipality computers must be declared to the Municipal Manager, by the end user.

End users will be allowed to take a copy of their declared intellectual property on termination of service.

INTERNET USAGE GUIDELINES

- **Acceptable uses of the Internet**

The Municipality provided Internet access is intended to be for business reasons only. The Municipality encourages the use of the Internet because it makes communication more efficient and effective. However, Internet service is Municipality property and its purpose is to facilitate Municipality business. Every staff member has a responsibility to maintain and enhance the Municipality's public image and to use access to the Internet in a productive manner. To ensure that all employees are responsible, the following guidelines have been established for using the Internet. Any improper use of the Internet is not acceptable and will not be permitted.

- **Unacceptable uses of the Internet**

The Municipality's Internet access may not be used for transmitting, retrieving or storage of any communications of a discriminatory or harassing nature or materials that are obscene or X-rated. Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference shall be transmitted. No abusive, profane or offensive language is to be transmitted through the Municipality's Internet system. Internet may also not be used for any other purpose that is illegal or against Municipality policy or contrary to Municipality's best interest. Solicitation of non-Municipality business or any use of the Municipality's Internet for personal gain is prohibited.

- **Communications**

Each employee is responsible for the content of all text, audio or images that they place or send over the Municipality's e-mail/Internet system. No e-mail or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else or someone from another organization or entity.

All messages communicated on the Municipality's e-mail/Internet system should contain the employee's name.

Any messages or information sent by an employee to another individual outside of the Municipality via an electronic network (e g bulletin board, online service or Internet) are statements that reflect on theMunicipality. While some users include personal "disclaimers" in electronic messages, there is still a connection to the Municipality and the statements may be tied to theMunicipality.

All communications sent by employees via the Municipality's e-mail/Internet system must comply with this and other municipality policies and may not disclose any confidential or proprietary municipality information.

- **Software**

To prevent computer viruses from being transmitted through the Municipality's e-mail/Internet system, there will be no unauthorized downloading or installation of any unauthorized software. All software downloaded must be registered to Municipality. Employees should contact the Information Communication Technology department if they have any questions.

- **Security**

The Municipality routinely monitors usage patterns for its Internet communications. The reasons for this monitoring are many, including cost analysis/allocation and the management of the Municipality's gateway to the Internet. All Internet sites visited via the Municipality's Internet connection are traceable to the user. All messages created, sent or retrieved over the Municipality's Internet are the property of the Municipality and should be considered public information. The Municipality reserves the right to access and monitor all messages and files on the Municipality's Internet system. Employees must take note that electronic communications, which include both Internet and e-mail are not private and confidential data should accordingly be transmitted in other ways.

- **Violations**

Any employee, who abuses the privilege of the Municipality's facilitated access to the Internet, will be subject to corrective action up to and including termination of service. If necessary, the Municipality reserves the right to advise appropriate legal officials of any illegal violations.

COMPUTER USAGE GUIDELINES

- **Loss of data**

The ICT Department disclaims liability for the loss of data or interference with files resulting, either directly or indirectly, from its efforts to maintain the operation, privacy and security of the computer facilities. For additional information regarding procedures in place to protect system and user data, refer to the Municipality's Back-up Procedure.

- **Copyright policies**

Many copyrighted programs are made available on the Municipality's systems under license agreements with the publishers. These license agreements generally do not allow the Municipality computer users to make copies of these programs. Unless otherwise specified, users are not allowed to make personal copies of software stored on central systems.

- **Non-commercial use policy**

The Municipality's computer accounts are to be used for the Municipality related activities for which they are assigned. The Municipality's computing resources are not to be used for commercial activities.

January 2004

Information Communication Technology Disaster Management and Business Resumption Policy

Purpose

The purpose of this policy is to ensure that Information Communication Technology(ICT) resources of Council are managed and protected against and during service interruptions, natural disasters, accidents and intentional acts.

This policy describes four levels of service availability and steps to resume business processes in the event of disasters and other incidents.

Scope

This policy is subject to the Computer User Policy of Council and covers computer services and system managed by the Information Communication Technology department.

Disaster Management Process

1. Identify that a disaster or event has taken place
2. Save data
3. Save hardware, software and facilities
4. Resume original state and restore data

Definitions

For the purpose of this policy the following definitions will be used:

- *Natural disaster:*
    - Earthquake
    - Tornado
    - Flooding
    - Landslide
    - Volcanic eruption
    - Lightning
    - Smoke, dirt, dust
    - Sandstorm or blowing dust
    - Windstorm
    - Snow/ice storm

Accidents:

- Disclosure of confidential information
- Electrical disturbance
- Electrical interruption
- Spill of toxic chemical

System failure:

- Hardware failure
- Operator/user error
- Software error
- Telecommunications interruption

Intentional acts:

- Alteration of data
- Alteration of software
- Computer virus
- Bomb threat
- Disclosure of confidential information
- Employee sabotage
- External sabotage
- Terrorist activity
- Fraud
- Riot/civil disturbance
- Strike
- Theft
- Unauthorized use
- Vandalism

Risk assessment of disasters, accidents, acts and failures

The Information Communication Technology department will continuously monitor the current and future risks to the delivery of service and systems.

In the event of a perceived immanent disaster, accident, act or failure the Information Communication Technology department will implement the necessary steps to stop; or limit the impact of; such an event.

Information Communication Technology services and systems that can be affected by a disaster or event:

- Hardware availability
- Operating systems
- Local Area Network and Wide Area Network services
- Financial Applications
- Human Resource Applications
- In-house developed applications
- E-mail and Internet Service
- Firewall Service
- Office Application Service
- Website and Intranet Service
- Library system
- Back-up and restore service
- Printing service
- Databases
- Geographical Information Systems

Levels of availability per service or system

Level One:

- All services are available during operational business hours.
- Maintenance on the system is done after hours.

  I.e. a few users have unrelated issues that are dealt with individually

Level Two:

- All services are available during operational hours but limited intermittent unavailability exists.
- Maintenance, reconfiguration on the system is done in operational hours and can require the Information Communication Technology department to bring the system/service offline for limited period of time.

  I.e. groups of users have related issues that are dealt with globally

Level Three:

- Not all services are available and long periods of unavailability exist.

- Maintenance, procurement, reconfiguring on system will be done as a priority and can require the Information Communication Technology department to bring down the system for long periods of time.

I.e. A whole department cannot work and infrastructure relevant to that department can be unavailable, functional activities for that department have stopped. Procurement of equipment might be needed.

Level Four:

- No services are available and unavailability will exist for extended period of time.
- Maintenance, procurement, reconfiguration and recovery will be done as a priority without handling any other situations.

I.e. All departments cannot work; total infrastructure can be destroyed or unavailable. Procurement of equipment might be needed

Determining availability levels

Availability levels will be determined and affected by the Information Communication Technology department as the disaster or event investigation unfolds.

Backup and restore procedures

The restoring of data will be done in accordance with the backup and restoration procedure in Council.

Escalation procedure for resolving unavailability

In the case of level one availability the relevant user will be informed of the problem and the problem will be dealt with operationally.

In the case of level two availability the group of people without a service will be informed of the problem and the problem will be dealt with operationally.

In the case of level three availability the affected departmental head will be informed of the problem and the problem will be dealt with at management level.

In the case of level four availability the Municipal Manager will be informed and all the departmental heads of the problem and the problem will be dealt with at executive management level.

Storage of backup data and system configuration

The backup data and a complete system configuration manual are stored off-site in a fire proof safe.

The configuration manual and backup data will allow for a complete rebuild of the total system by an outside company in the event that the Information Communication Technology department and staff destroyed.