MAKHUDUTHAMAGA
MUNICIPALITY

INFORMATION TECHNOLOCY (IT) POLICY

2008

Contents

1 Objectives and scope

1.1 Objectives

This document states the policy of Makhuduthamaga Municipality for the application of IT security management disciplines to protect its data, hardware and applications against all threats, which could endanger their confidentiality, integrity and availability.

1.2 Scope

This policy applies to all users of applications and the IT systems within. It also applies across all hardware platforms, to all Managers, Divisional Heads, staff, Councillors and contractors of the Makhuduthamaga Municipality.

This policy is mandatory for all offices of Makhuduthamaga Municipality including satellite offices (remote sites) where the Makhuduthamaga Municipality computer system has been installed. All Managers, Divisional Heads, Councillors, staff members and contractors will be required to sign a statement on a yearly basis acknowledging their understanding of and compliance with the policy.

1.3 Policy statement

Computer system resources and associated data are business critical assets requiring a high level of protection. Makhuduthamaga Municipality's policy that sufficient measures should be taken to protect these assets against accidental or unauthorized modification, disclosure or destruction, as well as to assure the confidentiality, integrity and availability of its automated data processing activities.

1.4 Non-compliance

Non-compliance with the standards and policies covered in this statement will be dealt with according to disciplinary Procedures Collective Agreement.

2 Accountability for assets

2.1 Objective

To maintain appropriate protection of municipal assets.

2.2 Policy statement

It is the responsibility of each Manager, Divisional Head, employee, Councillor and contractor to ensure that all the municipality's assets or assets used to access the Municipality's IT infrastructure are adequately accounted for. Information or changes in ownership, allocation of these assets, changes in configuration and usage outside of the Municipality's premises must be communicated to the Head of Division IT.

In order to protect the Municipality's assets adequately, identification should be made of all assets for which the Head of Division IT has security responsibility. All major IT assets should be accounted for as accountability for assets helps ensure that adequate security protection is maintained. An inventory of assets must be maintained to ensure that effective security protection is implemented.

2.3 Requirements

Critical IT assets should be identified and appropriately documented. Critical assets include:

- Network interconnection components (routers, switches, hubs etc.)
- Servers (mail, file, web etc.)
- External connection components (modems, remote access servers)
- Security components (authentication servers, firewalls)

Appropriate documentation concerning the Municipality's critical IT assets must be available and should cover:

- Identification: every critical IT asset should be uniquely identified. The identification scheme used for this must ensure that:
    - The location of the IT asset is known
    - The supplier of the IT asset is known (supplier information must be available)
    - Maintenance contracts for the IT assets are identified.
    - Persons responsible for the assets are known.
- Configuration: Information on its configuration should be available for every configurable critical IT asset. Technical configuration documentation should be included and supported by business requirements explaining why the IT asset has been configured as such.

- Linkages (where appropriate): Information on links with other critical IT assets should be included.

The IT Division should keep an IT inventory register that should be updated with all additions to IT assets. All critical IT assets should be entered individually indicating the following:

- **Model and type** : the model and type of the IT asset;
- **Serial number** : the serial number of the IT asset;
- **Identification** : a unique identification number (where relevant);
- **Location** : the location of the IT asset;
- **Supplier** : the supplier’s name.

The above is mandatory for all critical IT assets but encouraged for all other IT assets.

3 Personnel responsibility for security incident reporting

3.1 Objective

To ensure proper and timely reporting and subsequent resolution of all security incidents.

3.2 Policy Statement

Security incidents need to be identified, recorded, escalated where appropriate and resolved. All Departmental Managers, Divisional Heads and employees should be aware of and follow the procedure for reporting the different types of incidents (security breach, threat, weakness or malfunction) that might impact the security of the municipality's assets.

3.3 Reporting and evaluation of security incidents and weaknesses.

All IT security incidents should be reported according to the procedures as laid down and adjusted from time to time by the Head of Division IT. Personnel should understand their responsibility for reporting security incidents as quickly as possible. (A security incident is any incident which may affect or has affected:)

- The confidentiality of the Municipality's information (electronically stored)
- The integrity of the municipality's data
- The availability of the municipality's IT systems

The Head of Division IT should evaluate and record all incidents reported. These incidents include:

- Virus incidents
- Resource/network attacks
- Operational Incidents
- Loss Incidents

3.4 Actions and follow up

Reporting of security incidents must result in specific counter-measures taken by the Head of Division IT. Any action taken as a result of a security incident reported should at the minimum specify:

- What the action is
- Who will own the action
- When the action is expected to be resolved.

4 Physical and environmental security

4.1 Objective

To prevent unauthorized access to, damage to, interference with and interruption of IT services.

4.2 Policy statement

Departmental Managers, Divisional Heads and all employees should ensure that equipment containing municipal information is physically secure at all times.

IT facilities supporting critical or sensitive municipal activities should be housed in secure areas. These areas should be accessible only by properly authorized individuals and protected from intentional and accidental damage. Data can be compromised through the careless disposal of equipment. All items of equipment containing storage media, including fixed hard disks, should be checked to ensure that any sensitive data and licensed software are removed or overwritten prior to disposal.

4.3 Security standards for IT rooms

4.3.1 Space and layout

There must be sufficient physical space available for the equipment housed both current and planned. The equipment must be best located in terms of:

- operational functionality and use
- air circulation
- health and safety and
- maintenance access to the equipment.

Bulky and heavy equipment must be housed in floor standing cabinets.

4.3.2 Work practices

Everyone entering an IT room must:

- be authorized
- maintain cleanliness of the room; and
- dispose of all rubbish

Staff responsible for maintaining the room must ensure that a copy of these practices is displayed in the room.

Cabling must be kept tidy and designed not to cause any work hazards. Cable trays should be used where possible. Cables should also be terminated in floor standing cabinets and labelled for easy identification.

Risks or hazards must be clearly marked.

4.3.3 Security

The IT Office must be physically secure and access will be through an electronic system which provides a log of successful and failed attempts at entry together with a lock and key system. All failed attempts should be investigated and appropriate measures taken to address these. The entrance to the IT Office should also be fitted with a security burglar door.

All windows to the IT Office should be locked at all times.

4.3.4 Power

The supply of appropriately rated power outlets must be adequate to ensure safe and secure connections from the equipment to source. Overload protection must also be supplied.

When any changes are made to equipment within the IT Office the electrical loading must be checked to confirm that the supply remains adequate.

All equipment located in IT Office must have UPS protection and, where it is practical to do so, generator backup. The UPS must be capable of supporting all the equipment inside the IT office.

Power backup for equipment in IT Office must, as a minimum, consist of a local UPS with sufficient capacity to provide power backup for long enough to power down all equipment in the room.

4.3.5 Fire

All IT Offices which have a fire risk must be protected by an early warning mechanism for fire consisting of smoke detectors or heat detectors integrated into the building fire alarm system. On activation the system must raise an audible alarm and cut the power supply to the room.

All IT Offices should have an automatic fire extinguishing system that can be activated out of hours and manually when staff is present. All other IT rooms should as a minimum have CO2 hand held extinguishers available at the entry point to the room where practical.

All IT Offices must comply with all relevant health and safety legislation and have good access to appropriately signed fire exits.

4.3.6 Air Conditioning

IT Server rooms must have an air conditioning system that operates 24 hours a day seven days a week. It should be designed to keep the room within the IT manufacturers' recommended specifications for temperature and humidity throughout the year.

IT Office should have air conditioning appropriate to:

- the practicality of having a system installed;
- the severity of temperature and humidity extremes; and
- equipment is located in the room

4.3.7 Environmental control and monitoring

It is desirable to monitor temperature, humidity, power and cleanliness in IT Offices so that potential problems with air conditioning equipment and power supplies can be anticipated.

4.3.8 Lighting

Adequate lighting must be provided.

4.3.9 Cleaning

A periodic program of specialist cleaning should be in place for all IT rooms. The frequency of cleaning must be appropriate to the environment and include under floor and above ceiling cleaning where there is a raised floor and false ceiling.

Staff using the rooms must keep them rooms clean and free of unnecessary contamination.

4.4 Security access to IT rooms

The Head of Division IT should know all locations containing IT equipment. For this purpose a list of IT rooms and authorized staff should be kept, including staff and contractors granted temporary access.

The Head of Division IT should grant authorisation for accessing the IT Office for the following purposes:

- Operation, housekeeping, testing or storing of equipment within the room;
- Maintenance of or upgrades to IT equipment or environmental facilities within the room; and
- Management or audit

A register of all IT rooms keys issued and the holder thereof should be kept. The holders of the keys should sign the key register at the time that the keys are issued to them. In the event of loss or theft of any key immediate steps should be taken to prevent such key from being used again.

4.4.1 Rules for Departmental Managers, Divisional Heads, Councilors and Staff members

The following rules should be followed on accessing the IT server rooms:

- The IT officer must ensure that the list of people authorized to enter them is kept up to date.
- All holders of IT room's keys are totally responsible for those keys and should not give them to anyone else.
- A person entering a secure room will not permit anyone not authorized to do so to enter the room.
- IT rooms must never be left unattended unless they are fully secured to prevent unauthorized entry.
- The Manager of temporary staff requiring access to secure areas is responsible for ensuring that the person is aware of and complies with this procedure.
- Any person suspecting any form of security breach must report the event to the Head of Division: IT. This includes but is not limited to unauthorized entry, doors left open, locks not working, doors left unlocked or not closing properly, fire exit break glass broken, security codes divulged to unauthorised personnel, lost security IT server room keys.

- Anyone noticing suspect or unknown personnel in an IT server room must immediately either challenge the individual directly, or report the incident to the Head of Division: IT.

Any instances leading to security breaches resulting from staff not following the above guidelines may be considered a disciplinary matter.

4.5 Security of Removable Media

4.5.1 Backup Media

4.5.1.1 Storage

All data backup tapes must be stored in a secure location and this environment must be conducive to storage of magnetic media and operational use of computer equipment. If this is not possible then backup media must be allowed time to re-acclimatise to operational conditions before use.

4.5.1.2 Lifetime

Media in use for performing backups and archives should not exceed the manufacturer's recommendations on the useful lifetime.

4.5.1.3 Off-site storage

All backup media taken off-site should be logged in and out to ensure that all copies of data can be located, if required, and off-site depositories can be audited.

4.5.2 Media in transit

Computer media can be vulnerable to unauthorised access, misuse or corruption during transportation. The following controls should be applied to media in transit between sites:

- reliable transport or couriers should be used with adequate insurance cover;
- packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications;and
- Media should be held in secure containers and tamper proof packaging that reveals any attempt to gain access.

4.5.3 Archives

Archives will be performed as ad hoc backups and will have a specified retention period, an owner and be securely stored with proper identification linked back to a media reference library or similar as described below.

4.5.4 Identification of media

All formal backup and archive media must be clearly labelled. The label will contain a clear link to reference information recorded about the media in a reference library, database or manual set of backup / archive log records. The type of information recorded will be:

- a cross reference number back to the media;

- cycle revision number - if in a rotation cycle; and
- date the backup was performed - unless this can be referenced back to the rotation cycle in the logs;

The systems used to record the reference information about backup and archive media must be stored securely and if necessary with any off-site copies of the media so that reference can be made back to media in the event of disaster.

4.5.5 Recovery of data

As a matter of course, operational staff must regularly test the backup/archive tapes to ensure that the tapes can be read and can be relied upon for emergency use when necessary. If normal procedures do not use backup tapes for restores on a fairly regular basis then routine random tests should be performed at least weekly.

4.5.6 Electronic media disposal

Municipal and end user floppy disks, CDs and all forms of tape media must be destroyed by a process that ensures that data cannot be recovered at the end of the destruction process. An IT equipment and media disposal register should be kept where all IT equipment and media disposals are recorded. The register should indicate what steps were taken to ensure that the guidelines as contained in this policy have been complied with including the removal of all licensed software and the authorisation for such disposal.

Hard disks in servers and PCs that are to be removed by a third party for replacement or maintenance, should be either removed and destroyed or low-level formatted prior to re-use internally or by third parties who are subject to strict confidentiality clauses in their contracts.

5 System access control

5.1 Objective

To ensure that access to computer services and data is based on business requirements, and that access granted is consistent with job descriptions and required.

This area covers a wide area of activities: such as

- Business requirements for access control should be defined and documented. System owners should provide the IT department with a clear statement of the business requirements for system access, so that the IT department can control access to IT services and data.

- Procedures addressing user access should cover all stages in the life-cycle from initial registration of new users to their de-registration once access is no longer required. Users should have access only to those functions and information that they require to perform their duties

- Management should periodically conduct a formal review of users' access rights. Special attention should be given to privileged access rights that allow users to override system controls.

- Employees should follow good practices to protect password integrity in the initial selection and ongoing use of passwords.

- Network services, remote and external connections to the network should be centrally controlled and the access privileges provided should be limited to those services required for business purposes.

- All network logons should require a unique user ID and password to ensure that only authorized users gain access to the network.

- The use of powerful system tools should be limited to those who need them and such use should be closely monitored.

5.1.1 Security requirements for IT projects

An analysis of security requirements must be carried out at the requirements analysis stage of each business application development project. Statements of business requirements for new business applications, or enhancements to existing business applications must specify the requirements for security controls. Such specifications normally focus on the automated controls to be incorporated in the system, but the need for supporting manual controls must also be considered. These considerations must also be applied when evaluating software for business applications.

Security controls must reflect the business value of the information assets involved, and the potential business damage that might result from the failure or absence of security.

5.1.2 User & access rights

A formal user registration and deregistration process should be in place and must operate effectively. It should include appropriate authorisation procedures, a periodic check for redundant ID's and procedures for their removal. The procedure should ensure that user access rights to the municipality's systems, data and business applications are:

- In line with the user needs (need to know principle)
- Clearly defined in a formal access request;
- Authorised by the user's Manager or Departmental Head or his delegated official
- Timely changed when a user's responsibilities are changed; and
- Timely removed when a user leaves the municipality

5.1.3 Password, user ID and access rights administration

Formal standards for password management, user ID's and user access rights should be in place and implemented.

Controls should be in place to provide:

- Reasonable assurance that the use of system utilities is limited to authorized individuals and monitored;
- Reasonable assurance that access to program source code is limited to properly authorized individuals;
- Reasonable assurance that sensitive systems identified are isolated appropriately,and
- Adequate guidance for end user responsibility for password management should be in place and operating effectively.

Passwords should comply with the following:

- Passwords should be at least 8 characters long;
- Password changing should be enforced with a minimum frequency of every 30 days;and
- Intruder detection should be enabled to out further login attempts after 3 failed attempts;
- Where possible within the Network Operating System the following should also be enforced:
    - Password re-use should be prevented for an agreed number of changes;
    - A mixture of alphanumeric and numeric characters or a complete pass phrase should be required; and
    - There should be a list of banned 'trivial' passwords, enforced automatically.

The password management process should include:

- Secure delivery of initial and temporary password;
- Immediate forced password change;
- Positive identification procedures in emergency situations; and
- Positive acknowledgement of password receipt.

5.1.4 Security monitoring

Security monitoring should be performed on a regular basis following a formal procedure for regular security monitoring. Security monitoring should include:

- Periodic checks on redundant use ID's;
- Periodic checked on user access privileges;
- Periodic checks on security access logs; and
- Periodic checks on the use of powerful user ID's.

6 System development and maintenance

6.1 Objective

To ensure that security is built into IT systems

6.2 Policy statement

It is the Municipality’s IT policy that an adequate change control process should be implemented to provide reasonable assurance that any changes made to the municipality’s systems and applications in the operational environment are always identified, properly authorized, tested, approved, implemented and documented.

At the minimum, the change control process should include the following eight components:

- Initiation and approval of a change or development project
- Product development; Requirement analysis; Development Approach; Module Testing; system testing;
- End user acceptance testing; and
- Release planning.

6.3 Initiation and approval of a change or development project

Any software changes or new developments must be formally initiated through formal change requests. All change requests issued should be checked for validity, duplicates and formally approved by the appropriate personnel. Only formally approved change request forms should be considered as triggers for initiating development projects.

6.4 Product development

Product development should include the following components:

- Requirements analysis;
- Developments approach (methodology, standards);
- Module testing; and
- System testing.

6.5 Requirements analysis

Security counter measures are substantially cheaper and more effective if incorporated in application systems at the requirements specifications and design stages. All security requirements, including the need for fallback processing, should be identified at the requirements phase of a project, justified, agreed and documented as part of the overall business case for and information system.

6.6 Development approach

Changes made to software must be performed in a separate environment from the production environment. A development methodology, containing standards and guidelines for system development by IT officials should be available and strictly followed. Control should be in place to assure that support programmers are given access only to those parts of the system that are necessary for their work.

6.7 Module testing

Every individual programmer is responsible for the performance of module tests on the programs developed. Module tests need to be performed in an environment separate from the production environment. It does not, however, need to be formally approved by appropriate personnel

6.8 System testing

System testing should be performed in a separate environment from the production environment. Formal system test plans and scripts should be drawn up based upon the results of the requirements analysis. System testing usually requires test data to be as close as possible to the live data. Test data should be protected and controlled. The use of live personal data should be avoided. If such data is used it should be depersonalized before use. System test results should be formally reported and approved by the appropriate personnel.

6.9 Acceptance testing

Acceptance testing should be performed by end users in a separate environment from the production environment. Formal acceptance test plans and scripts should be drawn up based upon the results of the requirements analysis. Acceptance testing usually requires test data to be as close as possible to the live data. Test data should be protected and controlled. The use of live personal data should be avoided. If such data is used it should be depersonalized before use. Acceptance test results should be formally reported and approved by the appropriate personnel.

6.10 Release planning

Formal procedures for the implementation of new product releases should be available and must ensure that only tested and formally approved programs are taken into production environment. Special attention should be given to:

- End user sign-off including sign off for specific security requirements

- Technical change management; program transfer from test to production environment only to be executed by authorized officials.

7 End user computing policy

7.1 Objectives

This document states the policy with respect to the use of computer resources by the municipality's users

7.2 Policy statement

Computer system resources and associated data are business critical municipal assets. Sufficient measures should be taken to ensure that all the end users use these assets appropriately without unduly exposing the municipality to security threats. All end users should be made aware of the supporting security standards and procedures related to End User Computing and violation of the security standards, may lead to the disciplinary action up to and including termination of employment.

7.3 Internet use

Users of the municipality's information technology resources should take note that these assets are intended for business use and the exploration of the internet should not have a detrimental effect on the business activities of the municipality. Incidental, occasional personal use is permissible so long as:

- It does not consume more than a trivial amount of system resources; and
- It does not interfere with the productivity of the individual.

7.3.1 Internet usage standards

- Users are expected to respect the privacy of others;
- To respect the legal protection provided by copyright and license to programs and data;
- To respect the integrity of computing systems, users may not harass other users or infiltrate a computer system and/or damage or alter the software of a computer system;
- The municipality may at any time determine as to whether particular uses are or are not consistent with the municipality's business needs and may block traffic to particular internet sites;
- Malicious use of any computer or computer system is not allowed, use should be consistent with guiding ethical statements and accepted community standards;
- The internet may not be used to violate applicable laws or regulations;
- The use of the internet or any other network in a manner that precludes or significantly hampers its use by others is not allowed; and

- Users are not allowed to transmit any material either as the message or as attachments to a message, that in the municipality's sole discretion, is unlawful, obscene, malicious, threatening, abusive, libelous, hateful or encourages conduct that would constitute a criminal act or give rise to civil liability or unrest or a breach of a municipal policy. Among those that are considered offensive are any messages that contain sexual implications, racial slurs, gender specific comments, defamatory statements or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.

7.3.2 Anti-virus measures

Anti-virus programs should be active at all times when a computer is utilizing any municipality network resources. Internet file downloads from unverified sources should be scanned for viruses before being opened as should suspect data from any other source.

7.3.3 Monitoring of Internet use

The municipality reserves the right to examine, at any time, without prior notice, e-mail, personal files and any other information that may be stored on municipal computers or network. The municipality can also monitor Internet usage through reviewing sites visited by users and examining files that are downloaded.

7.3.4 Internet security awareness

As the Internet is an insecure public domain no municipal information may be sent through the Internet unless it is specifically classified as public domain information.

Unless prior approval has been obtained no employee may set up connections that allow non-municipal employees access to the municipal systems information.

7.3.5 Non-compliance

The municipality reserves the right to audit compliance with this policy from time to time. Disciplinary action for non-compliance may include dismissal. The Municipality also reserves the right to suspend or permanently remove a user's access to some or all of the electronic services specified in this policy.

7.4 Use of Electronic Mail Facilities

This policy is established with regard to access and disclosure of internal and external electronic communication messages (e-mail) created, sent received or stored, via the Internet or the municipality's intranet, by its employees, Managers, Divisional Heads and contractors using the Municipality's e-mail systems.

It is the responsibility of each Manager, Divisional Head and employees to ensure that use of the Municipality's e-mail system complies with the guidelines as set out in this policy.

The e-mail system is the Municipality's property and all copies of messages created, sent, received or stored on the system are and remain the property of the Municipality. The

Municipality maintains its e-mail system solely for business purposes and may not be used to engage in improper or illegal activity. Incidental, occasional personal use is permissible so long as:

- It does not consume more than a trivial amount of system resources
- It does not interfere with the productivity of the individual (both sender and receiver)

Common courtesy and respect for the reader's dignity should always be observed in e-mail content. This is particularly necessary when expressing displeasure, dissatisfaction, or similar sentiments. Abusive or obscene language is forbidden.

7.4.1 General Requirements

The following actions and uses of the e-mail system are **expressly forbidden**:

- Sending of unsolicited bulk mail messages of a personal nature;
- Propagation of chain letters;
- Subscription to mailing lists, discussion groups, a list-server, or other such bulk mailing services, for private purposes;
- Subscription to third party mail systems and use of such mail systems from company premises, unless directly related to a business need or objective;
- Transmitting any material either as the message or as attachments to a message, that in the municipality's sole discretion, is unlawful, obscene, malicious, threatening, abusive, libelous, or hateful, or encourages conduct that would constitute a criminal act or give rise to civil liability or unrest or a breach of company policies. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender specific comments, defamatory statements or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.
- Employees are not authorised to retrieve or read any e-mail messages that are not addressed to them. Employees shall not use any password or code, access a file, or retrieve any stored information, unless authorised to do so by an appropriate supervisor.

7.4.2 E-Mail Disclaimer

Users may not transmit personal opinions as those of the municipality, nor make any statement that may be construed to be a municipality statement. The following disclaimer should be included as a suffix to all e-mail messages to addresses external to the municipality:

E-Mail Disclaimer.

The information contained in this communication is confidential and may be legally privileged. It is intended solely for the use of the individual or entity to whom it is addressed and others authorised to receive it. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking action in reliance of the contents of this information is strictly prohibited and may be unlawful. is neither liable for the proper, complete transmission of the information contained in this communication nor any delay in its receipt.

7.4.3 Attachments to e-mail Messages.

Attachments to e-mail messages should be used sensibly. Transmission of large volumes of data in a message can have a drastic effect on the general level of service provided to all other users. If it is necessary to include attachments then these should be restricted to less than 10Mbytes in size when using internal mail, and 6 Mbytes in size when using the Internet addresses. Files larger than recommended above should be broken into separate "chunks" (usually zipped) and then transmitted as separate e-mail messages.

7.4.4 Size of the user's mailbox

The size of every user's mailbox is limited to 40Mb on the exchange server. When the user's mailbox reaches:

- 30Mb, a message will be displayed requesting the user to be clear the mailbox;
- 35Mb, the user will not be able to send messages, but will be able to receive them;
- 40Mb, the user's account will be disabled.

7.4.5 Non-compliance

The Municipality reserves the right to audit compliance with this policy from time to time. Any disciplinary action, arising from breach of this policy, will be taken according to the municipality's defined disciplinary code and procedures. Disciplinary action may lead to dismissal.

The Municipality reserves the right to suspend or permanently remove a user's access to some or all of the electronic communication services specified in this policy. Any user whose mailbox is suspended will need to consult with their Manager or Departmental Head or Head of Division. Depending on the severity of the infringement, the Municipal Manager would also need to be consulted before re-instatement of the e-mail account. The Manager or Departmental Head will then issue a written authorisation to the exchange administrator to re-instate the account.

The Municipality also maintains the right to review, audit, intercept, access, monitor, delete and disclose all messages created, received, sent or stored on the e-mail system for any purpose. By using the Municipality's e-mail system an employee recognizes the foregoing rights of the Municipality and consents to them.

7.5 Anti-Virus Security

This document states the policy for the protection of the municipality's data from accidental or unauthorised modification, loss, or loss of confidentiality by viruses, Trojan Horses and other malicious code.

7.5.1 Policy Statement

Municipal data is a business critical municipal asset and requires a high level of protection at all times. Measures will be implemented to protect this asset against accidental or unauthorised modification by malicious code. Steps will be taken by the IT division to provide as much security against viruses and other malicious code as is possible. However, reasonable precautions should be taken by every member of staff not to introduce unsupported or unverified software that may contain malicious code. Until data is copied to network servers, which is the responsibility of the IT division, the individual user is responsible for the care of the data on their machine.

All incoming software should be regarded as possibly infected no matter what the source, including shrink-wrapped disks, CDs, files downloaded from other networks and attachments in mail. On discovery of malicious code members of staff must report it to the IT division immediately and prevent the machine concerned from being used (including connection to the network) until it has been certified clean.

7.5.2 Requirements

The IT Division is responsible for determining the anti-virus software to be loaded on all the municipality's computers. End users are under no circumstances to:

- Disable the software;
- Load a different anti-virus package (unless authorised by the IT division); or
- Re-configure any settings on the software.

The IT Division is responsible for providing means for protecting information within their assigned area of management control. They are not responsible for the data on individual workstations or mobile PCs. This remains the responsibility of the user of that machine. End users should ensure that they log on to the server for an automatic anti-virus update at least once a week.

7.5.3 Enforcement

Any violation of standards, procedures or guidelines established in support of this policy shall be brought to the attention of management for appropriate action. Such violation will be regarded as misconduct and may result in disciplinary action being taken against those responsible.

7.6 Use of computer hardware and software

End users must be made aware of and acknowledge their responsibilities for the safe keeping of IT assets in their possession. This should be made before any use is made of such assets or possession taken thereof. A written declaration in this regard should be signed.

7.7 Allocation of movable IT resources

The movable computer (Notebook) resources are allocated to Departmental Managers. Any request for a notebook for other official other than a Departmental Manager, a formal written request with motivation should be done by the Departmental manager and submitted to the CFO in advance. Any official in possession of a notebook, camera will be subjected to signing of a prescribed laptop allocation form, approved by the Head of Division IT, and sign the same form (return) when leaving Council.

7.8 Use of movable IT resources

These assets, notebook, Camera, projector, etc still remain the property of the and all official to whom these have been allocated should take full responsibility for them. Official on leave should hand over these equipments to the IT Manager, unless if the official will need to utilize them for official use during leave.

For all presentations to be made, a request by the Departmental Managers or Divisional Heads or delegated official should be made at least 2 days in advance for the projector and/or pool notebook to the IT Manager.

7.9 Piracy policy

Only software approved by the IT Division may be copied on to any municipal computer equipment. Any illegal software can lead to disciplinary action being taken against the staff member.

7.10 Use of personal computer resources

No personal computer resources are allowed to be connected to the municipality's IT network unless specifically approved by the head of IT. Where such equipment is connected it should comply with the following conditions:

- At all times when such equipment is connected to the network of the municipality it will be treated in a similar manner as all municipal IT equipment;
- Only software approved by IT division can be installed on the equipment;
- Equipment to be used for official purposes when connected to councils network
- Confidential council data must be maintained and kept safe even if the equipment is off the network; and
- On resignation the equipment should be submit to IT section to ensure that all official data is transferred to the central server.

8 Short Title and commencement date

This policy shall be called the Information Technology (IT) policy and shall commence on 01 July 2008 or on the date of adoption by Council if that date is later than 01 July 2008.