O.R. TAMBO
DISTRICT MUNICIPALITY

# INFORMATION & COMMUNICATION TECHNOLOGY (ICT) POLICY

Corporate Services Department

Information and Communication Technology Management

## Table of Contents

## DEFINITIONS AND ABBREVIATIONS

| | |
|---|---|
| Attachment | An electronic file that is included with an e-mail message. Attachments can be of any allowed file type. Since email is limited to simple text, attachments are used to send complex data such as documents, plans or spreadsheets |
| Backup | the process of copying active files from online disk storage to tape so that files may be restored to disk in the event of damage to or loss of data |
| Chain letter | A message sent to a number of people, asking each recipient to send a copy with the same request to a number of others. The message may be sent as part of a get-rich-quick scheme or to propagate a joke, an appeal or a protest. Chain letters can seriously degrade network performance and consume substantial storage space |
| Computer | A computer is a device that accepts information (in the form of digitalized data) and manipulates it for some result based on a program or sequence of instructions on how the data is to be processed |
| Computer virus | A computer virus is a program that interferes with, or damages the normal operation of the computer or software. Virus programs are designed to infect other computers by hiding within emails or programs |
| Copyright | Copyright is designed primarily to protect an artist, publisher, or other owner against any unauthorized copying of his works. The protection relates to reproducing the work in any material form, publishing it, performing it in public, filming it, broadcasting it, causing it to be distributed to subscribers, or making any adaptation of the work. A copyright supplies a copyright holder with a kind of monopoly over the created material, which assures him of both control over its use and the financial benefits derived from it |
| Employee | Someone employed by the O.R. Tambo District Municipality |
| Electronic Mail (email) | Message transmitted and received by computers through a network. An electronic-mail, or email system allows computer users on a network to send and receive text, graphics, sounds and animated images to other users |
| Firewall | A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users and other networks |

| | |
|---|---|
| HTTP | Hyper Text Transfer Protocol is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web (www) |
| Hard Disk | A hard disk is part of a unit, often called a "disk drive," that stores data and provides relatively quick access to that data on an electromagnetically charged surface or set of surfaces |
| HOD | Head Of Department |
| IT | Information Technology |
| ICT | Information and Communication Technology |
| ICTM | Information and Communication Technology Management |
| Junk mail | email sent to unsolicited recipients. E-mail that is unwanted and does not relate to OR Tambo District Municipality business |
| Listserver | A listserver is an online discussion group conducted through email. Users subscribe to the listserver that discusses a particular area of interest. Sending an e-mail to the list automatically causes the message to be forwarded to every subscriber. E-mail volumes from listservers can seriously affect network performance |
| MB | MegaByte – metric for measuring data sizes |
| Mail bomb | A huge number of e-mail messages sent to one destination or an email with an extremely large attached file. Mail bombs are sent to antagonise their recipients and to cause them problems by filling up their disks and overloading the e-mail system |
| Mailing list | The collective name for a group of e-mail addresses to which an e-mail message may be sent simply by referring to the name assigned to the group |
| Operating System | An operating system (sometimes abbreviated as "OS") is a program that, after being initially loaded into the computer when switched on, manages all the other programs in that computer |
| ORTDM | O.R. Tambo District Municipality |
| Password | A password is an unspaced sequence of characters used to determine that a computer user requesting access to a computer system is authentic and authorised |
| Personal e-mail | email sent or received that does not support official OR Tambo District Municipality business, or activities sponsored by the OR Tambo District Municipality |
| Piracy | Software piracy is the illegal copying, distribution, or use of software |

| | |
|---|---|
| Post office | The central place where mail is stored and from which it is routed to its destination |
| Program | A program is a specific set of ordered operations for a computer to perform desired transactions |
| Proxy | In an enterprise that uses the Internet, a proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service |
| Server | A server is a computer and or program that provide services to other computers and or programs (and their users) in a computer network |
| Software | Software is a general term for the various kinds of programs used to operate computers and related devices |
| Spam | Copies of the same message sent to large numbers of newsgroups or users on the Internet. People spam the Internet to advertise products as well as to broadcast some political or social commentary |
| Trap door | A trap door is a means of access to a computer program that bypasses security mechanisms |
| Trojan | In a computer, a Trojan is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk |
| User | Someone who has a right to use the computing facilities of the Municipality |
| VPN | Virtual Private Network |
| Worm | In a computer, a worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself |

## 1. BACKGROUND

It is the intent of this Policy to establish guidelines for the users of the ORTDM's computing facilities, including Computer Hardware, Computer Software, Printers, Fax Machines, Voicemail Facilities, Electronic Mail (email), Intranet Access, Internet Access, and other related ICT Systems and Infrastructure.

| **Policy Particulars** | |
|---|---|
| Date of Approval by Municipal Manager / WORKING GROUP: | |
| Date of Adoption by Council: | |
| Commencement Date: | |
| Revision History: | |
| Review Date: | Annually |
| Policy Application | All users of the OR Tambo District Municipality's computing facilities |
| Responsibility - Implementation & Monitoring: | IT Manager, Corporate Services Director |
| Responsibility - Review & Revision: | ICT Manager, Director - Corporate Services, Municipal Manager |
| Reporting Structure: | IT Manager »ICTM Director » Director – Corporate Services » Municipal Manager » Council |

## 2. OBJECTIVES

The purpose of this policy is to provide guidelines and conditions of reasonable and acceptable use of the ORTDM's computing facilities in a controlled manner not to extend over their degradable values. Also to protect the Municipality and its employees using a social contract that constitutes reasonable use of these resources.

ORTDM provides ICT facilities to its employees for the purpose of conducting its business and does permit a limited amount of personal use of these facilities. However, these facilities must be used responsibly by everyone, since misuse by even a few individuals has the potential to negatively impact productivity, disrupt business and interfere with work and rights of others. Therefore, all employees are expected to exercise responsible and ethical behaviour when using the ORTDM's ICT facilities. Any action that may expose ORTDM to risks of unauthorized access to Data, Disclosure of Information, Legal liability, and potential System Failure/s is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.

The following topics are covered within this policy:

- Acceptable Usage
- Domain Network Access Rights and Privileges
- System Passwords
- Intranet and Internet Usage
- Email Usage
- Information Storage
- Data Backup and Restore
- Information Security

## 3. POLICY

Users of ORTDM's computing facilities are required to comply with all policy statements referred to in this document. Users also agree to comply with applicable National, Provincial, and Local Laws and to refrain from engaging in any activity that would subject the ORTDM to any liability. ORTDM reserves the right to amend this policy at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with applicable Provincial and Local Laws. To protect the integrity of ORTDM's computing facilities and its users against unauthorized or improper use of those facilities, and to investigate possible use of those facilities in violation with of ORTDM rules and policies, ORTDM reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove, or otherwise alter any data file or system resource which may undermine the authorized use of any computing facility or which is used in violation of ORTDM rules or policies. ORTDM also reserves the right to periodically examine any system and other usage and authorization history as necessary to protect its computing facilities.

## 4. SCOPE

This policy applies to all ORTDM employees and to all employees of ORTDM’s subsidiaries and affiliated organisations. It is the responsibility of all operating units to ensure that this policy is clearly communicated, understood and followed. This policy also applies to all contractors, and vendors/suppliers providing services to ORTDM that uses ORTDM’s ICT facilities. The ORTDM employee who contracts for these services is responsible to provide the contractor/vendor/supplier with a copy of these policies before any access is given.

This policy covers the usage of all of the ORTDM’s ICT resources, including, but not limited to:

- All computer related equipment, including desktop Personal Computers (PCs), Mobile / Portable PCs, Terminals, Workstations, Personal Digital Assistant (PDA), Wireless computing devices, Telecommunications equipment, Voice and Data Networks, Databases, Printers, Photocopiers, File Servers, Shared computers and all computing and networking infrastructure to which this equipment is connected
- All electronic communications equipment, including Telephones, Pagers, Radio communicators, Voicemails, emails, Fax machines, PDAs, Wired or Wireless communications devices and services, Internet, Intranet and other online services
- All software including purchased and licensed business software applications, ORTDM written applications, employee or vendor/supplier written applications, computer operating systems, firmware, and any other software residing on ORTDM owned equipment
- All intellectual property and other data stored on ORTDM equipment
- All of the above are included whether they are owned or leased by ORTDM or are under the ORTDM's possession, custody, or control
- These policies also apply to all users, whether connected directly to ORTDM’s network or via remote connections using ORTDM equipment or their own equipment

## 5. WHO IS AFFECTED BY THIS POLICY

This policy is applicable to all users authorised to use ORTDM’s ICT facilities. This means all employees that are employed permanently, contracted or temporally. It also include Councillors and Chiefs who serve in the ORTDM Council. All these employees, Councillors and Chiefs will be referred to as "**users**" in the rest of this document. Individuals that are dismissed and no longer in the employ of the Municipality, Councillors and Chiefs that have resigned fron the ORTDM Council are not included and not entitled to the use of ORTDM’s computing resources. This policy applies to all Service Providers using the ORTDM's ICT facilities and to their employees. If one has been dismissed or suspended or resigned as mentioned above, he or she must return any equipment given to him or her immediately. The Council shall not release any funds due to the user if there is no proof that the equipment has been returned. When the user is deceased, the Corporate Services Department will make reasonable attempts to recover the equipment from the family of the deceased.

## 6. POLICY STATEMENTS

### 6.1 ACCEPTABLE USAGE

ORTDM procures, support and maintains Computers, Information Systems and Communications Infrastructure to run effectively with the intentions for use by its employees. These resources provide administrative services, communications and Internet services to Local, National and International communities and are subject to requirements of legal and ethical behaviour.

The use of the ORTDM's ICT facilities, for both ORTDM business and limited personal use is a privilege but not a right, extended to various ORTDM employees.

(a) The employees of the ORTDM and/or any other person specifically designated by the Municipal Manager shall use the computing facilities provided by the Municipality

(b) Every person using the ORTDM’s ICT facilities shall treat all computer software, literature and/or manuals supplied by the ORTDM’s ICTM Unit for use on its facilities as being the property of, and confidential to the ORTDM

  i. Such software, literature and / or manuals shall not be copied or disseminated in any form, given, sold and / or passed in any way to another person or organisation without the prior permission from the Municipality, which permission shall not unreasonably be withheld

  ii. Such copies of software, literature and / or manuals must be returned to the municipality when no longer required by the user

(c) These resources are provided to facilitate the performance and productivity of ORTDM’s employees administratively

  i. Every allocation of computing resources is made on the understanding that it shall be used responsibly for the purpose for which it was requested or any other approved ORTDM’s business activity and shall be used only by or on behalf of those persons for whom the request was made

ii. Any use of computing resources by another person not allocated to must be authorised by the ICTM Unit or the Municipal Manager

(d) No user shall deliberately jeopardize the integrity of or meddle in any way with the computing facilities, information systems and information stored, to which he/she has no right and normal operation

(e) Every user who uses ORTDM's computing facilities shall observe the instructions that are issued by the ORTDM's ICTM Unit, specifying ways in which the facilities shall be used

i. In absence of specific instructions to the contrary, all computing facilities issued by the ICTM Unit shall be used only in the manner approved and supported by the Municipality

(f) Any user who, upon investigation appears to violate such conditions of use in a manner that is likely to tarnish the integrity of the Municipality may be prevented from further use of these facilities by the Municipality

(g) The conditions of use may be changed from time to time. Changes to these conditions will be effective from 5 days after notice has been given to all users.

## 6.2 DOMAIN NETWORK ACCESS RIGHTS AND PRIVILEDGES

A network is a means of connecting devices in order to enable communication and access to the network is fundamental to allow this to happen. Guidelines and permission must be given to allow and govern how these devices connect to the network

(a) The ORTDM network is accessible via 3 ways: Wired, Wireless & Remotely

(b) The ORTDM network will be accessible internally through wired and wireless network access devices

(c) All network devices must be provided for, configured and installed by the ICTM Unit of ORTDM

(d) All devices must logon and be a member of the ORTDM logical domain and directory services

(e) All qualifying users will be allocated with laptop or desktop computers where necessary and these equipment will configured to access the ORTDM's network

    i. applications or requests for provision of computing equipment must be made in writing and approved by relevant authority

(f) All user devices such as desktops, laptops and printers must connect to the network using a properly configured network interface

(g) All user devices such as desktops and laptops that are allowed to connect with wireless network cards must have a security code

(h) ORTDM will allow Virtual Private Network (VPN) method to connect to the ORTDM network for remote users on approval by the ICTM Unit

(i) All devices connected to the network must get allocated a unique Internet Protocol (IP) address

(j) Unshielded Twisted Pair (UTP) cables must be used to connect user devices that use a wired connection

(k) Fibre cables must be used to connect network devices such as switches

(l) Secured wireless hotspots will be created within the ORTDM network

(m) ORTDM has a right to scan the network to check devices connected on it's network

(n) ORTDM has a right to monitor and manage devices connected on it's network

(o) Devices connecting using the VPN method must have an antivirus installed and updated, the latest Service Pack

(p) Applications or requests to use the network must be motivated and recommended in writing and approved by relevant authority.

(q) A unique network username and password will be allocated to each network user in line with the password standards as outlined in this policy

(r) Periodic access reviews will be conducted with the assistance of Human Resource Unit to ensure incumbents are still in the municipality's employ

(s) All users who are no longer in the employ of the municipality will be denied access to the ORTDM network

(t) To prevent an open session from being misused by unauthorised persons, all sessions must automatically be logged-off after 10minutes of inactivity

(u) Users having power access privileges (e.g. to execute remote maintenance tasks and access to sensitive information and / or critical resources), may only be allowed access through the Municipality's accepted authentication mechanisms

(v) Users no longer requiring the access (e.g. change in job description or transfer) must be immediately removed from the system

i. line management must reconsider the access privileges of users who resign and inform the ICTM Unit as soon as possible after formal notice of the resignation

(w) All users that are not active on the network for more than ninety (90) days will be disabled from the network

i. special attention should be given to audit logs to ensure that the accounts which are no longer active are deleted

(x) The Municipality reserves the right to suspend / cancel any account(s) that acted in contradiction to this policy or any other procedural requirement as formulated from time to time

### 6.3 SYSTEM PASSWORDS

Passwords are an important aspect of computer security and are required for the protection of user accounts. The ORTDM must establish a standard for the creation of strong passwords, minimum time between changes to ensure the protection of all passwords

(a) All passwords must be unique and not easily guessable

(b) Passwords must have a minimum length of 6 characters, can have upper and lower case characters and may contain numbers or may be numbers only

(c) When numbers only, passwords may not be repetitive numbers, e.g. 22 or 33 and may not be sequential in order, e.g. 1234 or 4321

(d) Passwords can have a combination of digits, punctuation characters as well as letters

(e) The ICTM Unit should implement a process to ensure the secure communication of the initial password

(f) A forced password change must be implemented on the first sign-on session (to change the initial password) and thereafter every Sixty (60) days

(g) Password must not repeat the previous five (5) passwords

(h) Logon accounts will be locked out for thirty (30) minutes after three (3) unsuccessful attempts to logon

(i) Passwords must not be shared with anyone even users from the same section or department

(j) Passwords are confidential information

(k) Passwords must not be written down, if so, they must be kept in a safe place

(l) Users must positively identify themselves for changing of password through helpdesk

(m) A Network Access or Password Change Application form is recommended for all password changes

(n) Users must not give their passwords to anyone including the Helpdesk and or ICTM Unit staff members

  i. If passwords are given to any other user for whatever reason, they must be changed immediately thereafter

## 6.4 INTRANET AND INTERNET USAGE

The ORTDM provides the Intranet and Internet Services to be used as an effective, secure and productive tool. It must educate individuals who may use these services with respect to their responsibilities associated with such use to prevent the occurrence of inappropriate, unethical or unlawful usage of these services. It must establish prudent and acceptable practices regarding the use of the Intranet and Internet

(a) Intranet and Internet access will be provided to all users

  i. Users are required to submit a written request to the ICTM Directorate via their Immediate Superiors or Heads of Departments

  ii. The request will include the name of the individual requiring access and must be signed by both Applicant and Immediate Superior or HOD

(b) Users must not use the Intranet and Internet to download and distribute entertainment software, games or pirated software

(c) Users must not download image, audio and video files unless they are related to their work, this will be done with the authorization of management

(d) Users should not attempt to access or visit sites featuring Pornography, Terrorism, Racial, Unethical and Derogatory content

(e) All files downloaded from the Internet must be scanned for viruses using the approved ORTDM's Anti-virus software

(f) All software used to access the Internet shall be configured to use HTTP, Firewall and Proxy Server

(g) Internet usage will be monitored and recorded at all times by ICTM Unit

(h) No employee may use the Internet facilities to deliberately propagate any Virus, Worm, Trojan or Trap door programs

(i) Employees must not upload any software licensed to the ORTDM or data owned by the ORTDM without authorization from the Immediate Superior or HOD

(j) Users must not reveal confidential information pertaining to ORTDM on the internet

### 6.5 EMAIL USAGE

Email is a quick and efficient tool for communicating with people inside and outside the ORTDM. However, the ORTDM must protect itself and its employees from legal implications internally and externally by regulating the use of email in order to provide users with an acceptable standard of service. It must provide clear standards for acceptable etiquette and usage of email.

(a) The email system belongs to the ORTDM

(b) The email system must be used for authorised official purposes

(c) Limited use of personal email is permitted and must not affect user's performance negatively

(d) Users are encouraged to read and delete personal emails

(e) Personal email advertisements must be sent to the relevant designated electronic notice boards

(f) Users must not use the email system for mass mailing, chain letters or junk mail

(g) Users must not knowingly send computer virus threats via the email system

(h) Users must not distribute illegal or pirated software and copyright material

(i) Only official emails are permitted to be sent to the internal distribution groups

(j) Attachments to email exceeding 2 MB size are not permitted, unless permission is obtained from the ICTM Unit

i. Microsoft Office, Open Office, Adobe Acrobat and compressed file attachments are permitted

ii. Other file formats require permission from the ICTM Unit, which permission shall not unreasonably be withheld

iii. All attachments must be saved under "My Documents" folder

(k) Mailbox sizes are to be set to 500 GB for all users

(l) Each email must be appended with a disclaimer

(m) Users must not originate, store or forward emails that contain material that could be considered offensive, harassing or creating a hostile environment including discriminatory, intimidating, intolerant or derogatory remarks based on race, religion, gender, age, ethnic or social origin, sexual orientation, disability, physical condition, HIV status, conscience, belief, political opinion, culture, language, birth, pornography, gross depictions, satanic, militant, violent or extremist material

(n) If users receives these kinds of material, they should report to their Immediate Superiors or Manager or via grievance procedures

(o) Users are accountable for the content of all emails generated from their accounts

(p) Each user must have a unique password in order to use the email system

(q) Users may not send a message from another user's account without indicating clearly who they are

(r) Users are strongly discouraged from using other users' accounts for sending emails

(s) Managers may authorise their secretaries to read, write and send email messages on their behalf using a proxy facility. The proxy arrangement means that the secretary will also have access to the manager's personal email. Confidentiality is vested in the trust relationship between manager and secretary

(t) Users are expected to honour the confidentiality of other users' emails

(u) Users should exercise caution in using email to communicate confidential or sensitive matters

(v) ORTDM reserves the right to monitor email content, size and volume of sent and received messages

   i. No one may perform content monitoring without written authorization from the Municipal Manager
   ii. Software tools may be used to routinely scan all email for content filtering
   iii. ORTDM reserves the right to use results of monitoring reports to support disciplinary action or grievance

(w) Users must be aware that written messages may be viewed if the email of the person sent to is monitored

(x) Users should permanently delete old and unwanted emails

(y) Users must archive old emails and the email system will normally archive messages automatically after a set number of days

(z) All email messages sent out of ORTM's network must be accompanied by an email disclaimer

### 6.5.1 Email Disclaimer

This email transmission contains confidential information, which is the property of the sender. The information contained in this email or attachments thereto are intended for the attention and use only of the addressees. If you are not the intended recipient, you are hereby notified that any disclosure, copying or distribution of the contents of this email transmission, or the taking of any action in reliance thereon or pursuant thereto, is strictly prohibited. Should you have received this email in error, please delete and destroy it and any annexure thereto immediately. At no time may you act on the information contained therein. Under no circumstances will the OR Tambo District Municipality or the sender of this email be liable to any party for any direct, indirect, special or other consequential damages for any use of this email, or of any other hyper linked web site, including, without limitation, any lost profits, business interruption, loss of programs or other data on information handling systems or otherwise, even if the OR Tambo District Municipality or the sender of this email have been expressly advised of the possibility of such damages. Any agreements concluded with OR Tambo District Municipality by using electronic correspondence shall only come into effect once the OR Tambo

District Municipality indicated such contract formation in a follow up communication. No email correspondence sent to the OR Tambo District Municipality shall be deemed to have been received until the OR Tambo District Municipality has responded thereto. An auto-reply shall not constitute such a response. No warranties are made or implied that any employee of the OR Tambo District Municipality was authorised to make this communication. The OR Tambo District Municipality retains the copyright to all email messages sent from its communications systems. The views and opinions expressed in this email do not necessarily express or reflect the views and / or opinions of the OR Tambo District Municipality. This email disclaimer will at all times take precedence over any other email disclaimer received by employees utilising the communications facilities of the OR Tambo District Municipality.

## 6.6 DATA AND INFORMATION STORAGE

ORTDM provides storage for electronic data and information for users as ways of ensuring availability of electronic documents when needed. The idea of having central storage electronic data centre benefits users on mobility, accessibility, availability and security. This part of the policy provides guidelines on how users need to store electronic documents in the ORTDM's Electronic Data Storage Centre. It outlines where to store these documents, how to access them and how will these documents be secured by the ICTM Unit.

(a) The electronic storage system belongs to the ORTDM

(b) The electronic storage system must be used for authorised official purposes only

(c) Each user will be allocated a home folder in the File Server that is accessible via the ORTDM's network

(d) All official documents must be saved on local machines in the "My Documents" folder

(e) The "My Documents" folder must be synchronized with the user's dedicated home folder in the File Server

(f) Users are not allowed to store audio, video, executable, games, java applets and installers file types on both "My Documents" and the network accessible "Home" Folders

(g) ORTDM has the right to scan and delete file types that are not permitted in the electronic storage system without notice

(h) All content stored on ORTDM electronic storage space, computer hard drives and network drives belongs to ORTDM and are protected buy a copyright of ORTDM

(i) Users are not permitted to delete and format hard drives when they leave the employ of ORTDM

(j) ORTDM will only backup and restore the electronic data stored on the network accessible home folders for users

## 6.7 BACKUP AND RESTORE

The ORTDM's ICTM Unit must always backup data on all systems on daily, weekly, monthly and annual basis. It must ensure that there is minimum or no loss of data due to system failures or incidents of both natural and unnatural disasters. It must also provide guidelines to System Administrators on backup types and frequencies to establish prudent and acceptable practices regarding the backing up of systems.

(a) Incremental Daily backups will be performed on all Systems from Monday to Thursday

(b) Full Weekly backups will be performed on all Systems every Friday

(c) Full Monthly backups will be performed on the last day of each month

(d) During the month of December, a full Monthly backup will be performed before the last date of the Official Municipal Shut-Down

(e) Full Annual backups will be performed on all Systems on the 30th of June each year

(f) Daily backup media will be kept for 1 week and rotated every week

(g) Weekly backup media will be kept for a monthly and will be rotated every month

(h) Monthly backup media will kept for 1 year and will be rotated annually

(i) Annual backup media will be and kept for 5 years and will not be rotated

(j) System Administrators and or Backup Operators will sign a backup register for each Backup

(k) All Full Backups will be kept off-site in a secure environment

(l) All backups tapes must be tested for data restoration before taken away to the Off-Site storage

(m) Regular data restoration tests must be done on all Daily backups before they are sent to storage

(n) The ORTDM will have a Disaster Recovery Centre when critical systems will be replicated for Disaster Recovery

(o) System Administrators will develop a clear Backup Procedure to be followed when performing each backup

(p) Data restoration will be done at user's request

(q) Data restoration request form must be signed before any data can be restored

(r) System Administrators will perform Data restoration

(s) System Administrators will develop a clear Data Restoration Procedure to be followed when performing each data restore

## 6.8 DATA AND INFORMATION SECURITY

ORTDM must provide security to protect the Municipality's electronic data and information against all threats that could endanger its Confidentiality, Integrity and Availability. These security systems must ensure Business Continuity, minimise business damage and prevent or minimise incidents of data and or information loss and or theft.

(a) Information Security encompasses the management processes, technology and assurance mechanisms that will ensure that:

  i. departments trust the transactions they do on information systems

  ii. information stored is usable and available at all times

  iii. stored data and information can appropriately resist and recover from system failures due to errors, deliberate attacks, natural and unnatural disasters

  iv. confidential information is withheld from those who should not have access to it

(b) Employees, Clients and stakeholders that access the municipality's data are required to sign Security and Confidentiality undertakings accepting the conditions as set out in this policy

(c) The management of the network rests with the ICTM Unit and can involve third party contractors as service providers for the municipality

i. Where this is so, the service provider must sign a Security and Confidentiality undertaking accepting the guidelines and rules as set out in this policy

(d) Access to the Municipality’s network by Non-Municipal employees is subject to this security guidelines and rules as set out in this policy

(e) Contractors and Consultants employed in a permanent capacity by the municipality are classified as municipal employees for the purposes of this policy

(f) Part-time Contractors and Consultants who may have access to Municipal facilities, ICT infrastructure and Information Systems will be required to sign a Confidentiality and Security undertaking

### 6.8.1 High Level Information Security Principles

**(a) Protection**

ORTDM’s information must be protected in a manner commensurate with its sensitivity, value, and criticality

i. Security measures must be employed regardless of the media on which information is stored (paper, overhead transparency, computer disks, etc.), systems used to process it (computers, servers, firewalls, voice mail systems, etc.), or the methods by which it is moved (electronic mail, face-to-face conversation, etc.)

ii. Such protection includes restricting access to information based on a need-to-know basis

iii. Municipal manager must devote sufficient time and resources to ensure that information is properly protected

**(b) Risk Management**

Municipal manager is ultimately responsible to ensure that information is protected in a manner that is acceptable to Senior Management and Leadership of the ORTDM

i. to achieve this objective, risks should be identified by conducting regular risk analysis and, to take corrective measures where applicable

**(c) Information Management**

Decision-making within the ORTDM is also critically dependent on Information Systems and Information stored in these systems

i. Management is expected to know the nature of information they use for decision making (accuracy, timeliness, relevance, completeness, confidentiality, criticality, etc.)

ii. The awareness of and fine-tuning of such information attributes is an important information management activity

**(d) Co-Operation**

Information security requires the participation of and support from all information users

i. All information users (employees, consultants, contractors, third parties and temporaries) must be provided with sufficient training and supporting reference materials to allow them to properly protect and otherwise manage municipal information assets

ii. Training materials should communicate that information security is an important part of the municipality

iii. Training and documentation with respect to information security is the responsibility of the ICTM Unit

**(e) Organisation**

Guidance, direction, and authority for information security activities is centralised for the entire organisation in the ICTM Unit

i. The Unit is responsible for establishing and maintaining organisation-wide information security policies, standards, guidelines, and procedures

ii. Compliance checking to ensure that organisational units are operating in a manner consistent with these requirements is the responsibility of the Internal/external Audit Department

iii. Investigations of system intrusions and other information security incidents are the responsibility of the manager responsible for information and systems security

**(f) Privacy**

All information sent over municipal computer and communication systems is the property of the ORTDM

i. O.R Tambo District Municipality has to properly maintain and manage this property, Management reserves the right to examine all data stored in or transmitted by these systems

ii. Since ORTDM's computer and communication systems are provided for business purposes, workers should have no expectation of privacy associated with the information they store in or send through these systems

iii. In recognition of the privacy requirements as stated in the Constitution of South Africa, personal information will not be disclosed to any third party unless explicitly required through legal processes

**(g) Third Parties**

As a condition of gaining access to the ORTDM's computer network, every third party must secure its own connected systems in a manner consistent with the municipality's requirements

i. ORTDM reserves the right to audit the security measures in effect on these connected systems without warning

ii. The municipality also reserves the right to immediately terminate network connections with all third party systems not meeting such requirements

**(h) Classification**

Information must be categorised into levels of sensitivity and protected in accordance with appropriate requirements as part of the risk management process

i. The sensitivity classification standard must be used throughout the municipality to ensure that the level of protection is commensurate with the controls required (security mechanisms) to protect the information against disclosure (confidentiality), modification (integrity) and / or destruction (availability and use)

(Sensitive information is defined as information that if disclosed, will seriously and adversely affect the municipality, its business partners and / or clients and will constitute a serious compromise in the status of the municipality's operational security)

**(i) Confidentiality**

The confidentiality of all data, depending on classification and information security directives, will be protected before transmission over networks, and where indicated during the storage of such data

i. Unless written authorisation by Management, information may not be made available or disclosed to unauthorised individuals, entities or processes

ii. Measures should be implemented to protect information against unauthorised access, disclosure, copying, sniffing, eavesdropping and /or theft of information assets

**(j) Availability**

The continued availability and usability of services in accordance with business requirements must be ensured by implementing appropriate measures to prevent and recover from the loss of data due to acts of persons, system failures and / or disasters

i. All information assets should be protected against destruction, damage or contamination, denial of authorised / legitimate access, delay of use or access, natural and unnatural disasters and computer virus infections

**(k) Integrity**

The integrity of all data, depending on classification and information security directives, will be protected at all times before transmission over networks, and where indicated, also during the storage of such data

i. All information assets should be protected against threats to data integrity including unauthorised modification, destruction, and misrepresentation of data and / or computer virus infections

**(l) Non-Repudiation**

All access to the municipality’s technology resources is subject to positive identification and authentication of the user before access is granted

i. Measures must be implemented to ensure the non-repudiation of all financial transactions in accordance with official legislation and regulations

ii. Processes must be implemented to allow for the non-repudiation of origin regarding sensitive e-mail

**(m) Accountability**

Measures must be implemented to ensure that it is possible to determine who is responsible for an action, when and from where

i. The measures must be in accordance with the security requirements as determined by the departmental manager

**(n) Access Control**

All data and information will be protected and safeguarded against unauthorised access

i. Access to technology resources will only be granted in line with the user's specific responsibilities (need-to-have principle)

**(o) Authentication**

Measures must be implemented to uniquely identify or verify users of ICT facilities and to assure individual accountability

i. The authentication mechanisms must be in accordance with the classification of the information that requires protection and may for example take the form of passwords, tokens, or biometric identification devices

ii. All users will access ORTDM's information systems through at least the use of a unique user identification name or number and secret password

iii. As a first line of defence, users should not use passwords that are easily guessable nor should personal passwords be shared with any other user

iv. Authentication servers must be configured to enforce the municipality’s password standards

v. Strict physical and logical access control to the authentication servers and communication equipment must be enforced

### 6.8.2 Virus Protection

(a) The ICTM Unit must always ensure that computers are equipped with an approved Anti-Virus (AV) software package

(b) The AV package must be server based with a minimum approved update interval

(c) Updates to local computers must happen transparently to each user and be forced

(d) Check removable media for viruses before they are opened and stored on the computer (the anti-virus software should be set up to automatically perform the task)

(e) User must be trained not to open suspicious looking email and always confirm the bona fide's of the originator if uncertain about the contents

(f) Users should check with the ICTM Unit’s Service Desk before forwarding email about new viruses to colleagues

(g) In many instances it is a false alarm with the intent to cause panic thereby flooding the network with unnecessary messages

### 6.8.3 Reporting Security Incidents

All known vulnerabilities – in addition to all suspected or known violations – must be reported in an expeditious and confidential manner to the Office of the Information Security Officer or manager responsible for Information Security

i. Unauthorised disclosure of the municipality’s information must additionally be reported to the involved information owners

ii. Reporting security violations, problems or vulnerabilities to any party outside the municipality without prior written approval of the Office of the Municipal is strictly prohibited

iii. Any attempt to interfere with, prevent, obstruct, or dissuade an employee in their efforts to report a suspected information security problem or violations is strictly prohibited and cause for disciplinary action

### 6.8.4 Exceptions

Exclusions based on a valid business need could be motivated for and formally authorised, in which case record would be kept of the exclusions to facilitate effective management / control processes

### 6.8.5 General Requirements

**(a) Clear Screen and Clear Desk Policy**

i. At the end of each day, or when desks/offices are unoccupied, any ‘Management in Confidence’ or ‘Classified’ information must be locked away in either pedestals, filing cabinets or offices, which have been provided to all staff, as appropriate

ii. All waste paper, which has any sensitive or important municipal information or data on, must be shredded or placed in the secure shredding boxes located in some areas

iii. Under no circumstances should this type of waste paper be thrown away with normal rubbish in the bins under each desk

iv. Whenever the user leaves their desk and the computer switched on, it is essential that the user must ALWAYS ‘lock’ their screen by pressing ‘Ctrl Alt Delete’ and choose the ‘Lock This Computer’ option

v. Locking the screen not only prevent unauthorised use of the computer, which is logged on to the computer and the network using someone else’s user’s name, but it also prevents someone from reading sensitive information on the screen

### 6.8.6 Other Security Options

**(a) Automatically log off users when logon time expires**

i. Logon hours will be between 07H00 and 18H00. After this time period users will be logged off by the system

ii. Any user that works after these hours must apply to the ICTM Unit for permission to change logon times

**(b) Do not display last user name in logon screen must be enabled**

**(c) Prevent users from installing software including printer drivers must be enabled**

**(d) WWW Browser access**

i. All browsers shall be configured to access the Internet via proxy servers or via a site-proxy server, which is configured to access the Internet

ii. No other form of access to sites on the Internet is permitted

iii. This includes connections to alternative service providers by means of a dial-up modem, leased data line, private microwave link, radio modem or any other form of access method

iv. Users shall be held liable for breaches of security, loss of data or the compromise of information caused by unsafe browsing practices

**(e) Firewall**

i. A firewall is installed to protect the municipality's internal networks and systems from external attach and penetration attempts

ii. The creation of a demilitarised zone is preferred, but not mandated

iii. This policy may be revised should the municipality experience a high incidence of penetration attempts

iv. The firewall should be configured to provide Network Address Translation (NAT), Proxy services, Port blocking and control, Packet sniffers, Intrusion Detection and virus attack protection, WWW management features, Logging of audit information and Custom rule formulation and configurations

## 7. HOW THIS POLICY WILL BE APPLIED

(a) In certain instances parts of this policy can be applied automatically using technology

(b) Management reports will highlight possible violations

(c) The offender's manager will take disciplinary action in line with ORTDM policy

(d) Users may self-police the policy by reporting any violations via the grievance procedure

(e) The IT Manager and / or ICTM Director may issue a specific instruction

(f) Users may face disciplinary action if they violate this policy

(g) Managers should ensure that all their computer-using personnel, whether temporary, permanent or contract, are made aware of the contents of this policy

(h) Managers are required to apply the policy to all those who report to them

## 8. BREACH

(a) All users within the employ of the ORTDM who breach this policy shall be taken through a disciplinary process if they belong to the employ of the municipality and may be denied access to any computing facilities of the ORTDM temporarily or permanently.

(b) All users who are Councillors and or Chiefs serving in the ORTDM Council who breach this policy shall be reported to Council for Council to take appropriate action and shall be denied access to any computing facilities of the ORTDM temporarily or permanently.

(c) All users not employed by the ORTDM or serve as Councillors and or Chiefs in the ORTDM Council who breach this policy shall be taken through a be denied access to any computing facilities of the ORTDM temporarily or permanently.

## 9. OWNERSHIP

This policy is owned by the District Council and ICTM Department is responsible for its implementation.

## 10. VERSION CONTROL

| Version | Date | Author | Details |
|---|---|---|---|
| | | | |