BELA-BELA LOCAL MUNICIPALITY

Chris Hani Drive, Bela- Bela, Limpopo. Private Bag x 1609
BELA-BELA 0480
Tel: 014 736 8000 Fax: 014 736 3288
Website: www .belabela.gov.za

OFFICE OF THE MUNICIPAL MANAGER

Information and Communication Technology

Usage Policy

TABLE OF CONTENT

POLICY AUTHORITIES

Compiled by	D Nkuna
Designation	Divisional Manager IT
Signature	
Date	
Supported by	
Designation	
Signature	
Date	
Approved by	
Designation	
Signature	
Date	
Effective Date	From date of approval

1. MANDATE OF THE ICT DIVISION

1.1 The Information and Communications Technology (ICT) Division has the mandate to deliver services, support and maintain ICT infrastructure, for the Municipality to realise its mandate.

2. OBJECTIVE OF THE POLICY

2.1 The objective of this policy is to outline the acceptable use of computer equipment within the Municipality. These rules are in place to protect the employee and the Municipality. Inappropriate use exposes the Municipality to risks including malware attacks, compromise of network systems and services, and legal issues.

2.2 Furthermore, the policy defines principles for appropriate utilisation of ICT facilities within the Municipality. These include:

a. User Access Management
b. Password Usage
c. Network Usage
d. E-Mail usage
e. Internet Usage
f. Hardware Procurement

3. APPLICABILITY OF THE POLICY

3.1 This policy applies to all employees of the Municipality, including Contractors and Consultants, who use ICT services and assets.

3.2 This policy is supported by a range of security controls documented within operating procedures, technical controls embedded in information systems.

3.3 This policy applies to all equipment that is owned or leased by the Municipality.

4. TERMS AND DEFINITIONS

Term	Definition
Distributed Environment	Refers to a network environment, or topology, in which decision making, file storage and other network functions are not centralised but instead are found through the network. This type of environment is typical for client-server applications and peer-to-peer architectures.
Framework	A logical structure for classifying and organising complex information. (Federal Enterprise Architecture Framework)
Hardware	(1) Physical equipment, including workstations (personal computers), servers, mainframe, peripheral equipment, etc. (2) Contrast with software, which consists of programs (coded instructions that model certain procedures and rules).
Information	Data (usually processed data) that is useful to a decision-maker (Wainright Martin et al: 1999: 688). Any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual forms.
Information System	Interrelated components working together to collect, process, store, and disseminate information to support decision-making, coordination, control, analysis, and visualisation in an organisation (Laudon, et al. 1998:7).
Information and Communication Technology (ICT)	The hardware, software and communications infrastructure used for Information Systems services. It encompasses all forms of technology used to create, store, exchange, communicate and use information in its various forms (data, voice, images, video, multimedia presentations, etc). It applies to the acquisition, processing, storage and dissemination of all types of information using computer technology and telecommunication systems.

5. ACRONYMS

COBIT	Control Objectives for Information Technology
ICT	Information and Communication Technology
ITIL	Information Technology Infrastructure Library

6. REFERENCES

6.1 International Guidelines

a. Control Objectives for Information Technology (COBIT)

6.2 International Standards

b. Information Technology Infrastructure Library (ITIL)

c. ISO/IEC 17799: Edition 1, 2000 – Information Technology – Code of practice for Information Security Management

6.3 National Policy

d. Constitution of the Republic of South Africa, Act 108 of 1996

f. The Electronic Communications and Transactions (ECT) Act 25 of 2002

g. National Strategic Intelligence Act 2 of 2000 applicable for South Africa

h. Regulation of Interception of Communications Act 70 or 2002

i. State Information Technology Act 88 of 1998

7. POLICY STATEMENT

7.1 ICT systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP, are the property of the Municipality.

7.2 These systems are to be used for official business purposes in serving the interests of the Municipality in the course of normal operations.

7.3 Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

7.4 While ICT desires to provide a reasonable level of privacy, users should be aware that the data they create on the systems remains the property of the Municipality.

7.5 Employees are responsible for exercising good practice regarding the reasonableness use of ICT systems.

7.6 For security and network maintenance purposes, ICT may monitor equipment, systems and network traffic at any time.

7.7 Employees must be aware that all data transmitted or received on computer equipment, are not private and are subject to viewing, downloading, inspection, release, and archiving by the Municipality at all times.

7.8 The ICT Division has the right to inspect any and all files stored in areas of the network, officials Laptop, desktops or storage media in order to assure compliance with ICT policies.

7.9 A formal procedure shall be followed to give users access rights to ICT facilities.

8. ROLES AND RESPONSIBILITIES

8.1 The ICT Division shall:

a. Provide, maintain, improve and secure the computer network, equipment and communication facilities of the Municipality.

b. Ensure the confidentiality of trade secrets, client information, employee information and confidential information generally, contained on ICT infrastructure.

c. Inform and educate users on the access to and use of ICT infrastructure;

d. Identify and address the potential risks associated with the use of ICT in the workplace.

e. Endeavour to promote productivity through the use of quality ICT infrastructure

f. Not allow private laptops onto municipal network, or copy any Municipality related data to private laptops.

8.2 The user shall:

a. Not share logon usernames or disclose passwords to any other party;

b. Ensure the confidentiality of trade secrets, client information, employee information and confidential information generally, contained on ICT equipment issued to the user.

c. Not intentionally bypass the security mechanisms of the equipment or any third party security system or web site, without obtaining prior written approval from the Manager: ICT.

d. Not use ICT resources for downloading, storage, forwarding or accessing data unrelated to official business (e.g. video clips, music files or graphics, SPAM) of the Municipality;

e. Not intentionally or negligently burden ICT infrastructure with data not related to official business;

f. Not install or use any unauthorised configuration items (software or hardware) without approval from the ICT Division.

9. USER ACCESS MANAGEMENT

9.1 Allocation of access rights

a. There shall be a formal user registration procedure for granting access to requested information systems and networks.
b. Access rights to external consultants or contractors must be authorised by the by the Manager: ICT.
c. Access rights to privileged systems must be formally screened and authorised by the Manager: ICT.
d. Logon names shall be unique to each user and standardised.
e. ICT Division shall review all user access rights periodically, and renewed or revoked when appropriate. The results of this review must be communicated to the affected users where feasible.

f. ICT Division shall also review all user accounts with administrative rights on the active directory, Payday and MunSoft financial applications quarterly and the results of such review shall be kept as evidence

9.2 Movement, Retirement, Suspension, and Termination of Employees

a. Once notified by the Human Resource Division of a dismissal, suspension or resignation of an employee the ICT Directorate will take the following action:

i. Dismissal – access rights will be disabled immediately
ii. Suspension – access rights will be disabled immediately until reinstatement
iii. Resignation – access rights will be disabled on last day of work.
iv. Transfer to other Municipalities – access rights will be disabled on last day of work.
v. Disabled accounts will be permanently deleted after three months.

b. In the event of an on the spot suspension/termination from service, the Human Resource Management Division should inform the ICT Division to disable all access to ICT facilities.

c. Inactive account not being utilised shall be deleted

d. The ICT Division will compile list of all employee movements within the Municipality on a quaterly basis. Access rights will be reviewed and amended appropriately.

10. PASSWORD USAGE

10.1 Employees who negligently or intentionally share their passwords or accounts with anyone else for any reason will be held responsible for any resulting misuse of the system by others.

10.2 Password Management

a. Passwords must be changed as per ICT set interval.

b. The systems shall allow only 3 attempts for incorrect logons where after the user account shall be locked.

c. Only authorised administrators shall be allowed to unlock a user account.

d. The user will be responsible for ensuring that the password remains secure. The user will be held accountable should the password be compromised due to negligent actions such as, writing a password down and leaving it accessible to others.

f. Computers will automatically be locked if there is no activity on that computer.

g. The chosen password should comply with any of the following:

i. Must not be the same as the username.
ii. It is not recommended to use names of relatives, significant dates, or names of objects in the vicinity.
iii. ICT shall ensure that passwords are encrypted.

10.3 Employees who have any reason to believe or suspect that someone else is using their password must immediately notify ICT Division.

11. NETWORK USAGE

11.1 Network Access Management

a. Users requesting access to the network and resources (including e-mail and Internet) should fill in the user form.

b. ICT will ensure that users are only provided with direct access to the networked resources that users have been specifically authorised to use. Users are not allowed to modify network hardware or devices. Only administrators are allowed to configure network devices.

c. Users are not allowed to install software that provides or manipulates network. Under no circumstances should users install any software on the systems unless otherwise authorised by ICT.

d. Users are to use network protocols that are approved by ICT.

e. ICT shall provide firewalls for secured access between the department network and worldwide network. Attempts to by-pass the firewall are strictly prohibited.

f. No personal hardware or devices are allowed on the network unless authorised by ICT.

12. E-MAIL USAGE

12.1 The ICT Division shall:

a. Protect the department from e-mail transmissible malicious software and viruses.

b. Notify the sender, if an outgoing e-mail could not be sent; and notify the addressee(s), if an incoming e-mail was rejected.

c. Ensure that all outgoing e-mails have the standard legal disclaimer at the bottom of the message.

d. Educate users to ensure that they understand the messages, memos, notices, announcements, etc. with regard to security threats in using the e-mail facility.

12.2 An e-mail user shall:

a. Include a meaningful subject line before sending messages

b. Not disguise or attempt to disguise own identity when sending an e-mail, and shall not forge or attempt to forge any e-mail message

c. Ensure sending message to the right person(s)

d. Keep all e-mail messages brief and formulated appropriately

e. Email should be used for business purpose only no chain massages should be circulated

f. Notify the sender if you were not the intended recipient

g. Not intentionally send any malicious material, such as a virus infected file, either internally or externally which might compromise the ICT systems and/or operations of the municipality

h. Report any suspicions which may either lead to enhancement or compromise of the e-mail system security and/or operation to ICT

i. Not access (or try to access) a colleague's e-mail or use his/her e-mail account without the permission of the allocated user

j. Ensure that the size of e-mail message(s) and its attachment does not exceed the limit as set by ICT.

k. Not send message(s) which could be regarded as unsolicited, derogatory, defamatory or libellous and/or compromising the information security of the Municipality.

m. ICT shall issue procedure in terms of user groups to be created and managed.

l. Not send any material of pornographic nature or any other offensive material (images depicting graphic violence, for instance) and report any received material of pornographic nature or offensive material.

13. INTERNET USAGE

13.1 Internet access shall conform, inter alia, to the following:

a. Employees may not use the Municipality's systems to access or download material from the Internet which is inappropriate (literature inciting violence against foreign nationals, for example), offensive, illegal (for instance, pirated software), or which jeopardises security.

b. The Internet is meant to be used for business purposes – this means research, procurement, authorised software updates and other legitimate business activities authorised by the ICT

c. ICT should ensure that the network infrastructure is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall or antivirus.

d. The ICT Division shall use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet by employees. At all times, the following classes of web traffic shall be prohibited:

i. Illegal sites – child pornography, etc
ii. Music and video downloads
iii. Downloads that may compromise the security of the Department
iv. Committing crime and terrorism
v. Distribution of spam
vi. Participating in online gambling
vii. Spreading malware
viii. Accessing adult content (pornography)

ix. Advertising
x. Dating and chat
xi. Playing online games
xii. Radio and video streaming
xiii. Podcasting

14. HARDWARE PROCUREMENT

14.1 Hardware acquisition channels are restricted to ensure that ICT has a complete record of all hardware that has been procured so as to support, and maintain such hardware accordingly.

14.2 Under no circumstances should personal or unsolicited hardware be added to the network.

14.3 ICT shall be the sole authority on standardisation of hardware.

14.4 The lifespan of all ICT hardware equipment procured shall be a minimum of three years.

15. POLICY COMPLIANCE

15.1 Violation of this policy, and referenced policies, may lead to restriction of access to (or usage of) the Information Technology infrastructure and/or disciplinary action as per the Human Resources Management Policies.

15.2 The Municipality may use any legislation relevant to the usage or protection of ICT infrastructure, in prosecuting the person who has violated this policy.

15.3 Any damage, security breach or loss of information which can be deemed to have been caused by negligence or intention on the part of the user or any identified individual shall be the responsibility of that individual. The penalty, thereof, shall be determined by the Human Resource Management disciplinary process.

16. POLICY REVIEW

16.1 This policy will be reviewed on an annual basis or if necessarry by the Manager: ICT to:

a. Determine if there have been changes in International, National or Internal references that may impact on this policy.

b. Determine if there are improvements or changes in the ICT process that should be reflected in this policy

17. ANNEXURE A: ACCEPTABLE USE EXAMPLES

The following scenarios are intended to provide examples of acceptable and unacceptable uses of computing resources, based on the Acceptable Use Policy. These examples are not comprehensive but are merely illustrations of some types of acceptable and unacceptable use.

17.1.1 AUTHORISED USE

Acceptable:

a. While using a colleague's computer from off site, you connect to the Municipality Network to check your email. When you have finished, you log off of your account, closing any browser windows you may have used.

Unacceptable:

a. While someone else is using a computer, you want to check your email. You ask them to log in, giving them your password to type in for you.

b. While traveling on vacation, you ask a staff person to check your email for you by giving them your password.

c. A colleague is on sick leave, and he/she was receiving responses for an event. Rather obtaining formal approval to access their email, you attempt to gain access to their account by guessing their password.

d. After having your computer hacked, you decide to download and run hacking tools yourself to help your friends out by checking for vulnerabilities on their computers.

17.1.2 FAIR SHARE OF RESOURCES

Acceptable:

- You conduct a telephone conference with remote office using your telephone.
- You use a shared printer in the office that you are authorised to use.

Unacceptable:

- You use your computer connected camera to display what is happening in your room 24 hours a day, 7 days a week on the Internet, and list the site on major search engines to ensure large number of visitors.
- While using a computer, you alter its setup, so that each time it starts up, your favourite programs are started automatically.
- As an employee, you store your photos, music, movies or unauthorised software on ICT resources (either on your workstation or file server).

17.2.3 ADHERENCE TO LAWS

Acceptable:

- Storing legitimately-obtained audio or video files for official use.
- Displaying a legally reproduced copy (with copyright notice) of any recorded material.

Unacceptable:

- Taking a CD you own, you make copies of songs onto your computer, and set up sharing to allow others to access those songs from your computer.
- Playing a video in an office for entertainment purposes, or for its cultural or intellectual value unrelated to official business of the Municipality.

17.2.4 OTHER INAPPROPRIATE ACTIVITIES

- While running for political office, you use your official email account to send out email about your candidacy to colleagues, promoting you as a candidate.
- Using a computer connected to the network, you establish a commercial business, selling products or services over the Internet.
- You download, store, print and/or display materials that could be perceived by others as contributing to an intimidating, hostile, or sexually offensive working environment.
- You send out unauthorised and unsolicited email messages to other colleagues in the Municipality.

17.2.5 PRIVACY AND PERSONAL RIGHTS

Acceptable:

- As part of an investigation into an employee's potential misuse of the network for copyright violations, permission is granted from an appropriate authority for ICT to log into that employee's computer and check files that are stored on the hard disk.

Unacceptable:

- While checking the email system for possible problems, an ICT person has to open a mailbox owned by someone else. In doing so, he or she reads the subject lines, finds one that looks interesting, and opens the email message.

17.2.6 USER COMPLIANCE

Acceptable:

- When requesting access to ICT resources, an individual reads relevant policies to familiarise themselves with acceptable use of ICT facilities.
- As virus alerts and other news are sent from ICT, an individual takes appropriate action to protect his or her computers from those threats.

***Unacceptable*:**

- When requesting access to ICT resources, an individual does not bother to read relevant policies to familiarise themselves with acceptable use of ICT facilities the policy or acknowledging responsibility for following ICT policies.
- As virus alerts and other news are sent from ICT, an individual sets up an email filter to send the information directly to the Junk Mail folder.