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

Information Security Policy

TABLE OF CONTENT

POLICY AUTHORITIES

Compiled by	D Nkuna
Designation	Divisional Manager IT
Signature	
Date	
Supported/Not Supported	ML Mashishi
Designation	Acting Corporate Services Manager
Signature	
Date	
Approved/Not Approved	MM Maluleka
Designation	Municipal Manager
Signature	
Date	
Effective Date	

1. MANDATE OF THE ICT DIRECTORATE

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 This policy has the following objectives:

a. To protect the Municipality's information by safeguarding its confidentiality, integrity and availability.

b. To establish safeguards to protect the information resources from theft, abuse, misuse and any form of damage.

c. To establish responsibility and accountability for Information Security in the Municipality.

d. To encourage management and employees to maintain an appropriate level of awareness, knowledge and skill to allow them to minimise the occurrence and severity of Information Security incidents.

e. To provide suitable coverage of International Standards ISO 17799 and related information security best practices.

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 and other controls that will be advised to employees from time to time by ICT Division through information security standards, procedures and guidelines.

4. TERMS AND DEFINITIONS

Term	Definition
Governance	The mechanisms an organisation uses to ensure that its constituents follow its established processes and policies. It is the primary means of maintaining oversight and accountability in a loosely coupled organizational structure. A proper governance strategy implements system to monitor and record what is going on, takes steps to ensure compliance with agreed policies, and provides for corrective action in cases where the rules have been ignored. (http://looselycoupled.com/glossary/governance)
Incident	Any event which is not part of the standard operation of a service which causes, or may cause, an interruption to, or a reduction in, the quality of that service
Standard	Guideline documentation that reflects agreements on products, practices, or operations by nationally or internationally recognised industrial, professional, trade associations or governmental bodies.
System	An integrated composite that consists of one or more of the processes, hardware, software, facilities and people, that provides a capability to satisfy a stated need or objective (ISO12207, 1995:5)
User	An individual utilising Information Systems to achieve the business goals required to realise the mandate.

5. ACRONYMS

COBIT	Control Objectives for Information Technology
ICT	Information and Communication Technology
ICTSC	Information and Communication Technology Steering Committee
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. PRINCIPLES

7.1 This policy addresses the associated risks to the information assets and includes risks such as:

a. Uncontrolled access, connections, and unintentional user errors

b. Security of the information systems compromised by unsupported business practices

c. Ensuring the integrity and validity of data

d. Poor operating procedures

e. Malicious code and viruses

f. Uncontrolled system or data changes

g. Internet and public domain access

h. Breach of legislation or non-compliance with regulatory or ethical standard

7.2 The implemented controls shall be reviewed annually or if the need arises and adjusted where necessary.

8. APPLICATION

8.1 Information Security Policy Statements

a. This section contains formal policy requirements each followed by a policy statement describing the supporting controls and supplementary guidance.

i. Information Security

- Roles and responsibilities for information security governance shall be identified and a Risk Committee shall be established.
- Third parties will be identified and managed in accordance with a legal contract to ensure that no unauthorised access is gained to the Municipality – both logically and physically.

Senior Management Commitment to Information Security

- Senior management should fully supports and commits to the enforcement of all aspects of security throughout the Municipality.

ii. Asset Management

- All physical and information assets shall be classified according to their criticality to the Municipality, enabling an appropriate level of protection. Assets will be handled in line with its identified criticality.
- Information Asset Owners shall be identified and held accountable for the protection of assets under their authority.

iii. Employee Security

- Security education, training and awareness programmes will be conducted to ensure that employees are aware of security threats and concerns and are equipped to apply the security principles at all times.

iv. Physical and Environmental Security

- Physical and environmental controls shall be in place to protect the Municipality and its supporting information processing facilities from unauthorised access, intentional or accidental damage or interference.

v. Communications and Operations Management

- All operational procedures shall be documented and implemented to ensure correct and secure operations in the Municipality and its supporting information processing facilities, communication facilities and networks. Exchange of information will be managed to prevent the loss, modification or misuse of information.
- All breaches of security shall be reported and managed accordingly.

vi. Access Control

Access (both locally and remotely) to computers, systems and networks shall be granted in line with requirements. This access will be managed and monitored to ensure that no unauthorised access is gained. The use of mobile computing facilities will be managed to ensure protection of these facilities.

vii. Disaster Recovery Management

- Business continuity management plans and procedures shall be established and maintained to facilitate the normal functioning of critical business activities in the event of failures or disasters.

viii. Data Classification

- **Sensitive information**: Information in this category may not be distributed without consideration of its sensitive nature.

  - Private information is personal information, including personal intellectual property, which is accessible only by its owner and those to whom the owner directly entrusts it, except under exceptional circumstances.
    Examples: Intellectual property, email;

  - Confidential information is Municipality information normally handled in the same manner as private information, but may be accessed by other authorised employees under limited additional circumstances.
    Examples: ID number, date of birth, medical records, education record, financial record;
  - Internal information is Municipality information that is intended for distribution within the Municipality.

- **Public Information**: Information in this category is distributed without restriction.
  Examples: Marketing materials, Municipality website
- **Top Secret**: shall be applied to information, the unauthorised disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.
  Example: Compromise of complex cryptologic and communications intelligence systems.
- **Secret**: shall be applied to information, the unauthorised disclosure of which reasonably could be expected to cause serious damage to the national security.
  Example: Revelation of significant intelligence operations.

ix. Information Handling

- Unauthorised disclosure of sensitive information is prohibited.
- Unauthorised tampering or alteration of sensitive information is prohibited.
- Unauthorised destruction or disposal of sensitive information is prohibited.
- Laws and policies governing information retention must be complied with.

- When confidential information is being transported or stored, it must be protected from unauthorised disclosure, modification, or destruction.
- When possible, confidential information must be protected with sufficient publicly vetted encryption algorithms while in transit and at rest.
- If encryption is not possible appropriate compensating controls must be considered and implemented.
- Before access is granted to confidential information, a signed non-disclosure agreement must be on file for that individual or organisation.
- When appropriate, criminal and reputational background checks must be conducted.
- Confidential information being transported to or stored with a third party outside of the Municipality network or physical premise must be approved by the Information Owner.
- Confidential information, both digital and physical, must be disposed properly to prevent unauthorised disclosure.

x. Identity and Access

- Anonymous identities should be avoided, and are prohibited when accessing confidential information unless an exception is granted by the Information owner.
- Information users will be given the minimum level of access to systems and information that their duties require.
- Human Resources Management division must report change of an employee employment status or role to ICT.
- Remote access to the network or systems is will be strictly granted and monitored
- Passwords, pass-phrases, and private keys (physical and private digital) must be protected, and may not be shared.

xi. Information Compromise

- Should it be suspected that "sensitive" data has been accessed by an unauthorised party or has been used improperly by an authorised party, then the discovering individual must report the incident immediately to ICT Division.

- Should a password, pass-phrase, or key be believed to have been compromised, it must be changed immediately. If that password authorises access to sensitive information, the incident must be reported to ICT.

xii. ICT Infrastructure

- Unauthorised eavesdropping, redirection, sniffing, and tapping of network traffic or systems is prohibited.
- ICT infrastructure must be protected from theft, intrusion, malicious code, and abuse.
- ICT infrastructure must be regularly patched for security and stability.
- Locations that house digital and paper copies of confidential data must have appropriate physical preventative, detective, and deterrent controls.
- ICT infrastructure must be reinforced with appropriate redundancy, backup, and disaster recovery plans and technologies.
- A "defence in depth" or layered security strategy must be applied to information, network, and system architecture and design whenever possible, especially pertaining to sensitive information.

xiii. Assessment and Compliance

- Risk assessments must be regularly conducted to reveal security posture, and to identify vulnerabilities and weaknesses in software, infrastructure, policy, procedure and practices
- Employees must participate in information security awareness that will be provided by the ICT.
- Controls shall be in place to ensure compliance with legal, legislative, regulatory or contractual obligations and any other security requirements.

9. ROLES AND RESPONSIBILITIES

9.1 The Risk Committee shall:

a. Ensure that the necessary information security controls are implemented and complied with as per this policy

9.2 The ICT Division shall:

a. Approve and authorise information security procedures

b. Ensure that all users are aware of the applicable policies, standards, procedures and guidelines for information security

c. Ensure that policy, standards and procedural changes are communicated to applicable users and management

d. Evaluate information security potential risks and introduce counter measures to address these risks

e. Revise the information security policy and standards for effective information security practices

f. Facilitate and coordinate the necessary information security procedures within the Municipality

g. Report and evaluate changes to information security policies and standards

h. Coordinate the implementation of new or additional information security controls

i. Review the effectiveness of information security measures and implement remedial controls where deficits are identified

j. Coordinate awareness strategies and rollouts to effectively communicate information security mitigation solutions

10. POLICY COMPLIANCE

10.1 Violation of this policy, may lead to restriction of access to the ICT facilities or disciplinary action.

10.2 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 will be the responsibility of that user or that individual. The penalty, thereof, will be determined by the Municipality disciplinary process.

10.3 The Municipality may use any legislation relevant to the usage or protection of Information Systems (or information), in prosecuting the person who has violated this policy.

11. POLICY REVIEW

11.1 This policy shall be reviewed on an annual basis by the ICT Division 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