Okhahlamba Local Municipality

INFORMATION COMMUNICATION AND TECHNOLOGY

SECURITY POLICY

2016/2017

TABLE OF CONTENTS

1. INTRODUCTION

Computers enable employees of Okhahlamba Local Municipality to conduct the organisation's day-to-day business activities more effectively and efficiently. In addition, computers also allow employees greater access to organisational resources and information. In order to promote a working environment that is conducive to teamwork and productivity, it is essential that all users understand their roles and responsibilities with regards to Information Technology (IT) security and adhere to the security requirements of Okhahlamba Local Municipality. IT security is therefore characterised as the preservation of:

- **Confidentiality** – Ensuring that information is only accessible to those individuals who are duly authorised to have access to it.
- **Integrity** – Safeguarding the accuracy and completeness of information and processing methods.
- **Availability** – Ensuring that authorised users have access to information and associated assets as and when required.

As such, municipalities have different uses for their respective IT systems. The installation of Okhahlamba Local Municipality's IT network represents a significant IT investment and so IT equipment must be utilised in the best interest of, and be of benefit to, Okhahlamba Local Municipality.

2. OBJECTIVES

The objectives of the IT Security Policy are to:

- Clarify to all users their responsibilities regarding the security of Okhahlamba Local Municipality's information and computing resources.
- Define the potential risks and dangers for Okhahlamba Local Municipality in the event of misappropriation and abuse of computing equipment by users.
- Maintain an appropriate level of physical and logical security to safeguard IT systems and resources against unauthorised use, modification, disclosure or loss to preserve the integrity of the Okhahlamba Local Municipality IT environment.
- Regulate the professional and effective use of computing equipment within Okhahlamba Local Municipality, as well as between Okhahlamba Local Municipality and its external entities.
- Establish a standard for creation of User ID's and strong passwords, the protection of those passwords, and the frequency of change thereof.
- Identify the persons responsible for maintaining the security requirements.
- Establish management direction, basis of procedures and requirements to ensure the appropriate protection of Okhahlamba Local Municipality's information and equipment resources by any means.
- Ensure that this investment in information and equipment resources is properly managed.
- Ensure that the system is optimally utilized in its full capacity to the best advantage of Okhahlamba Local Municipality.

3. APPOINTMENT OF IT COMMITTEE

Okhahlamba Local Municipality shall appoint an IT Steering Committee that must meet at least quarterly to discuss IT-related improvements or changes in the IT environment and infrastructure.

4. SCOPE

This policy applies to all employees, consultants and temporary staff who access Okhahlamba Local Municipality's computer networks with an organization-owned or personal workstation and are responsible for an account (or any form of access that supports or requires a User ID and a password) on any system that resides at any Okhahlamba Local Municipality facility, has access to the network, or stores any non-public organisational information. All employees need to be aware of security risks and vulnerabilities in order to create

organisation-wide security consciousness. Therefore, security awareness and training programmes shall be initiated and each employee shall be required to receive the necessary Information Security awareness and training provided by Okhahlamba Local Municipality.

5. ADMINISTRATIVE CONTROLS

5.1. General Controls

The IT Officer (or his nominee) will, on recommendation of the IT Steering Committee, issue guidelines on the use and application of Okhahlamba Local Municipality's network and shall monitor compliance with these guidelines, which must be strictly adhered to by all users of any IT systems. The required administrative controls applicable to the system will be included in these guidelines and will comprise the following:

- Physical controls over computer hardware, backups and software;
- Access controls;
- Data security controls; and
- Internet and email usage controls.

5.2. Programming and Documentation Standards

Only the IT Officer, on recommendation of the IT Steering Committee, may liaise with IT software suppliers to provide programmers for Okhahlamba Local Municipality's use and to have such programmers developed further or amended. The IT Officer shall keep a register of all such requests for amendment and/or enhancement of Okhahlamba Local Municipality's software and hardware, and shall inform the relevant users of any changes.

5.3. Insurance

The Finance Department shall ensure that appropriate and adequate insurance cover is obtained in respect of all components of Okhahlamba Local Municipality's IT operations.

5.4. Reporting

The IT officer shall report to the IT Committee on the general use and application of the IT network, indicating in such report whether existing administrative controls need to be reviewed or amended, specifying operational problems of material importance which have arisen during the quarter to which the report relates, and indicating how such problems have been or are being addressed.

5.5. Audits

- The IT Officer, in consultation with the Municipal Manager, shall arrange audits of the IT systems on a periodic basis. These audits may be conducted by either the internal or external auditors (or both), provided that sufficient budgetary provisions have been provided for.
- The findings of such audits may be included in the audit report to the IT Steering Committee, or if findings are significant then they must be reported to the Audit committee.

6.   PHYSICAL CONTROLS

Physical controls with regards to the Okhahlamba Local Municipality IT network relate to measures which must be put into place to ensure the physical security and protection of all relevant computer hardware, software, manuals and the server room. The physical controls are required to provide protection against natural hazards, as well as the risks of theft and/or negligence on the part of Okhahlamba Local Municipality's officials.

6.1.   Hardware

- Where personal computers have been allocated to officials, such officials shall accept that these computers must be used to fulfill operational functions within the organization, and that their use is restricted to such official functions only.
- No hardware may be installed or removed by any municipal official without prior consent and authorization or direction from the IT Officer.
- No hardware may be removed by any official from municipal premises without the prior written authority of the Director Corporate Services or IT Officer. The IT Officer shall keep such written authority on file, and the official who wishes to remove the relevant hardware must have a copy of such authority for inspection when required.
- Any malfunctioning computers must be immediately reported to the IT Officer by the official to whom such equipment has been allocated, and the IT Officer shall immediately attend to the required repairs or replacement of the equipment, but subject to the necessary provision having been made in the budget.
- Given the significant cost of laser and ink jet printing, officials to whom the use of printers has been allocated must ensure that all printing is kept at a minimum or rather in fast draft print quality. Where multiple copies of a particular document are required, the original shall be printed and photocopied. Wherever possible, screen previews should be used rather that physical printing. Original toners and inkjet cartridges must be used when printing is necessary, as not only may the compatible or refilled products void Okhahlamba Local Municipality's warranty in respect of the equipment, but they can also (in given circumstances) damage the printers.

6.2.   Software

- The IT Officer shall maintain a list of approved software to be used on the IT network, as well as the number of licenses owned and the number of copies of such software loaded onto the system. Only authorized and licensed software listed on the approved software listing may be loaded onto Okhahlamba Local Municipality computers, and this may only be implemented with the consent and supervision of the IT Officer. The IT Officer shall further ensure that this authorized list, referred to as the "Approved Software List", is reviewed and updated periodically in order to address any new software which is released into the market that may be relevant to Okhahlamba Local Municipality and as the demand for new or additional software arises.
- **Caution:** No software may be downloaded through the Internet or via email without the approval of the IT Officer or the relevant Head of Department. Also, pirated software by any official will not be permitted whatsoever. As such, here are examples of approved software:
- **Standard Applications** – A new user is entitled to the following standard applications upon receiving a new computer or the user is new to the institution:
    o   Microsoft Office Suite;
    o   Antivirus Software;

- o Acrobat Reader; and
- o WinZip.
- **Specialized Applications** – A user is entitled to the following specialized applications once duly authorized:
  - o Window Outlook Mail;
  - o VIP;
  - o Sage Pastel;
  - o Dolfin;
  - o BAUD; and
  - o GIS.

6.3. Computer Manuals

The originals of software, hardware, systems manuals and guides shall be kept by the IT Office with relevant licenses and discs in a fireproof locked cabinet. The IT Officer shall further ensure that the manuals and release notes are updated with each new release installed on the systems.

6.4. Server Room

- Only the IT Officer and authorised personal shall ordinarily have access to the server room.
- The server cabinet and server room shall be kept locked by the IT Officer and the keys shall be kept as follows:
  - o One set of keys in the Off-site storage location, Traffic Department, *Refer to Okhahlamba Local Municipality Disaster Recovery Plan*;
  - o One set with the IT Officer;
  - o One set with the Director Corporate Services and Chief Financial Officer
- The IT Officer shall ensure that adequate fire prevention and extinguisher systems are installed in the server room, and that this equipment is regularly checked and maintained. No official may tamper with such equipment, and no official may remove any such equipment from the server room other than for the purpose of having it tested or serviced.
- The IT Officer shall ensure that a properly designed, maintained and operated air conditioning system is installed in the server room.
- The IT Officer shall ensure that the servers within the server cabinet are raised in the event of flooding.
- The IT Officer shall regularly test or have tested the Uninterrupted Power Supply (UPS) in order to ensure that it is maintained in an operational condition.

7. ACCESS CONTROL

7.1. General

Access control is necessary to restrict unauthorized user access to any portion of the IT network or to any particular component of the system. It is therefore necessary that the bona fide user, in order to gain access, must first be authorized, i.e. the access of such user to the system must be properly authenticated. Access to the IT network comprises three steps:

- Physical access to a terminal;
- Access to the system; and
- Access to specific commands, transactions, programmers and data within the system.

7.2. Physical Access to Terminals and Systems

After the bona fide user has switched on his or her computer, the user must enter that particular computer password to gain further access to terminals and systems accordingly.

7.3. Access to specific Commands, Transactions, Programs and Data within the System

The IT Officer or relevant Head of Department (HOD) shall set access level priorities in accordance with the job descriptions of the officials concerned and to comply with the specific further requirements of the officials of the Finance Department. Access level and amendment priorities shall be set out in writing by the IT Manager or relevant HOD.

7.4. User Codes and Passwords

a. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Okhahlamba Local Municipality's entire corporate network.

b. As such, all Okhahlamba Local Municipality employees, consultants and temporary staff with access to the organization's systems are responsible for taking the appropriate steps (as outlined below) to select, maintain and secure their passwords at all times and never use an account assigned to another user, as they will be held responsible for total use or misuse of their account. All officials, to whom user codes and passwords have been allocated, must ensure that these codes and passwords are properly safeguarded. Under no circumstances may the employee share any use code or password with colleagues.

c. Passwords are used for various purposes at Okhahlamba Local Municipality. Some of the more common uses include: user level accounts, web accounts, email accounts, screensaver protection, application logins and logins IT Hardware. All users should be aware of how to select strong passwords. Hence, the following password guidelines must be adhered to by all users on all servers and computers within Okhahlamba Local Municipality:

   o User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

   o Passwords must not be inserted into email messages or other forms of electronic communication.

   o Passwords should not be a word in any language, slang, dialect or jargon.

   o Do not use the same password for Okhahlamba Local Municipality accounts as for other non-organisational access (e.g. personal account, option trading, benefits, etc.).

   o Users must not use the "Remember Password" feature for applications (e.g. VIP, Internet Explorer, etc.), and must not write passwords down and store them anywhere that is easily accessible within their offices.

   o Users must not store passwords in a file on any computer system (including laptops or similar devices) without encryption.

   o Users must avoid using the same password for multiple applications.

   o If an account or password is suspected to have been compromised, the user must report the incident to the IT Officer and change all their passwords accordingly.

   o If a user is requested to provide their password details to any IT staff member, they must ensure that they monitor the actions performed by the staff member. Thereafter, the user should change their password immediately once the IT staff member has left.

d. Where possible, systems have been configured to follow Okhahlamba Local Municipality standards. The organisation's requirements for password settings should be as follows:

- o A minimum of seven (7) characters in length;
- o Must be changed every 30 days;
- o A password history of (twelve) 12 generations should be maintained.
- o User accounts are set to lockout after 3 unsuccessful login attempts;
- o Must contain at least one (1) special character (e.g. #, @, %, $, etc.);
- o Users should not use their usernames as passwords;

e. Additional Configuration settings for Active Directory Server

- o A minimum password age of 1 days;
- o Accounts should be set to lockout indefinitely (until IT Officer unlocks);
- o Accounts are set to lockout after 3 invalid log-on attempts.

f. Users must take note that for all activity performed using their user name and password, they will be held accountable and may face disciplinary action in the event of misuse. It is therefore of utmost importance that users follow the guidelines below on password construction and safeguarding their password in order to minimise the threat of others obtaining their passwords.

- o A password should be created from a pass-phrase. For example, the phrase "security is vital to this company and me" might result in the password of "siv2Tcam!" by using the first letter of each word in the phrase, substituting the word "to" for the number "2", and adding the exclamation mark at the end to increase complexity.
- o Personal details, such as spouse's name, license plate, ID number or birthday, must not be used.
- o Words in a dictionary, derivatives of user ID's and common character sequences such as "123456" must not be used as well.
- o Passwords should not be based upon month / year combinations such as "jan09" or "april2009". Hackers use these types of words in attempts to guess passwords.
- o Users must not use cyclical passwords. For example, users should not add a numeric at the end of the password in sequence.
- o Passwords must not consist of all identical numeric or alphabetic characters, such as: "1111111" or "aaaaaaa".
- o Employees must never share their passwords with anyone, including IT staff, administrative assistants or secretaries.
- o All passwords are to be treated as sensitive organisational information.

g. Users must take note of and adhere to the following "Don'ts":

- o Do not reveal a password over the phone to anyone.
- o Do not reveal a password in an email message.
- o Do not talk about a password in front of others.
- o Do not hint at the format of a password (e.g. "my family name").
- o Do not reveal a password on questionnaires or security forms.
- o Do not share a password with family members or colleagues.
- o Do not reveal a password to co-workers while on vacation.

8.   DATA SECURITY CONTROL

8.1.   Privileges and Exposure

As stated above, access by users to Okhahlamba Local Municipality's IT systems shall be restricted in accordance with the job descriptions of officials concerned. Users are responsible for the protection of sensitive information by ensuring that only officials whose duties require such information are allowed to obtain knowledge of such information while it is being processed, stored or in transit.

8.2.   Backups

Backup procedures are in place with respect to information saved on personal computers. Backup procedures will be determined by the IT Officer, and communicated to all relevant users accordingly. These procedures shall be adhered to by all users on the system. Backups will be stored in a secure site.

9. INTERNET AND EMAIL

9.1. Use of Internet

- Internet access and related IT resources are provided to Okhahlamba Local Municipality at significant cost and are made available primarily for business use. Users who have access to the Internet shall use this access solely in connection with official responsibilities, including communicating with clients, working related partners, local and provincial government agencies, providers of goods and services to Okhahlamba Local Municipality, and to also research relevant topics and obtain business related information which is of use to Okhahlamba Local Municipality. Limited personal use on approved sites may be authorized when such access will be to the best advantage of Okhahlamba Local Municipality only.

- All users who have access to the Internet shall conduct themselves honestly and appropriately, and respect copyrights, software licensing rules, property rights, privacy and the prerogatives of others. Specifically, officials who use the Internet shall ensure that intellectual property of others is protected and that Okhahlamba Local Municipality's resources are not misused, that information and data security (including confidentiality where applicable) are at times respected, and that the Internet is not used for any form of abuse.

- Every official using the Internet facilities of Okhahlamba Local Municipality shall identify himself or herself honestly, accurately and completely. Officials using the Internet shall do so only when this is required to fulfill their official responsibilities and/or when they are authorized to do so.

- Whenever an official downloads any file from the Internet, such a file must be scanned for viruses before it is run or accessed. If the official is uncertain as to the procedure to be followed, such official shall immediately seek assistance of the IT Officer.

9.2. Authority to Speak on the Behalf of Okhahlamba Local Municipality

Only those officials who are duly authorized by the Municipal Manager to speak to the media, to analysts, in public gatherings or send external emails on behalf of Okhahlamba Local Municipality may do so.

9.3. Integrity of Okhahlamba Local Municipality's Image

- Officials who are authorized to speak on behalf of Okhahlamba Local Municipality, as set out in 9.2 above, shall ensure that they honor the image and integrity of Okhahlamba Local Municipality at all times, do not engage in any unauthorized political advocacy, and refrain from the unauthorized endorsement by Okhahlamba Local Municipality of any commercial product or service not sold or provided by Okhahlamba Local Municipality itself.

- Moreover, such officials must ensure that, where inputs are provided on behalf of Okhahlamba Local Municipality to any news group or chat room, such inputs have been grammar and spell-checked, and that the inputs reflect the corporate view of Okhahlamba Local Municipality (where applicable) rather than the personal opinions of the writer.

9.4. Security

- Prompt disciplinary action shall be instituted against any official who attempts to disable, defeat or circumvent any firewall, proxy, Internet address screening programmed or any other security systems installed by the IT Officer or any IT suppliers to assure the safety and security of Okhahlamba Local Municipality's IT network.

- Any officials who obtain a password or user code (ID), which allows access to the Internet and/or the organization's IT network, shall keep such a password and user code confidential, except if any occasion arises where any authorized

technical support official requires knowledge of such password or user code in order to solve a computer related problem. As set out in 7.4. (b) above, the present policy strictly prohibits the sharing of user codes and passwords between employees. Furthermore, logging onto the IT network or Internet with one's personal user code and password, and then allowing another user to use or work on the Internet or the IT network, shall be viewed as an attempt to bypass official security procedure, and is strictly prohibited and will be dealt with accordingly.

- Every authorized user shall sign all IT Security Policy Compliance Agreements provided to them by the IT Officer before attempting to gain access to the Internet and/or the network.
- The IT Officer will review all Internet activities and analyze the relevant usage patterns. Thereafter, appropriate action will be taken on the user wherever any abuse of the system is evident.

9.5. Electronic Mail (Email)

- Only authorized officials shall use the available email facility.
- The IT Officer shall scan all emails for any inappropriate content or offending words or phrases.
- All copies of emails shall be kept as records.
- Only authorized officials shall be permitted to receive attachments through the email system, and such attachments shall be scanned by the IT Officer to ensure that they are related to responsibilities of the official concerned.
- The IT Officer shall maintain a list of prohibited and blocked email, and shall update and amend such list as circumstances require.

9.6. Internet Browser

As indicated in 9.4 and 9.5 above, Okhahlamba Local Municipality reserves the right to track all visited sites.

9.7. Unacceptable Practices

- No official may display any kind of sexually explicit material on any organizational system. Furthermore, no sexually explicit material may be archived, stored, distributed, edited or recorded using any of Okhahlamba Local Municipality's resources.
- The IT Officer shall have the right to block access from within Okhahlamba Local Municipality's networks to all Internet sites identified as inappropriate. If any user is connected to a site which contains sexually explicit or otherwise offensive material, such user must immediately disconnect from the site concerned, regardless of whether such site has previously been deemed acceptable by any screening or rating programmers.
- Okhahlamba Local Municipality's IT related facilities, and especially its Internet facilities, may not be used knowingly by any official to violate the laws and regulation of the Republic of South Africa or any other nation, or the laws and regulations of any province or municipality. The use of any municipal resources or illegal activities shall be ground for the immediate dismissal of the official concerned, and the Council and it's official undertake further to cooperate with any legitimate law enforcement agency in this regard.
- No employee may knowingly use Okhahlamba Local Municipality's IT facilities and resources to download or distribute pirated software or data.
- No official may knowingly use the Internet facilities to propagate any viruses, worms, Trojan horses or trap doors (i.e. malicious code).

- No official may knowingly use Okhahlamba Local Municipality's Internet facilities to disable or overload any computer or network or to circumvent any system intended to protect the privacy or security of another user.
- No employee with authorized Internet access may upload any software licensed to Okhahlamba Local Municipality or data owned or licensed to Okhahlamba Local Municipality without prior authorization of the IT Officer.
- No official may create a communication link requiring dial-out access from any computer which is also connected to the IT network.
- No official may use any software which is not provided or approved by the IT Officer or relevant Head of Department (HOD).
- Only the IT Officer or relevant Head of Department (HOD) shall authorize the provision of email addresses to authorized users.

9.8. Ownership and Classification of Data

Any Okhahlamba Local Municipality data that is created, sent, printed, received or stored on systems owned, leased, administered or authorized by Okhahlamba Local Municipality is the property of Okhahlamba Local Municipality and its protection is the responsibility of Okhahlamba Local Municipality's owners, designated custodians and users. As such, data shall be classified as either: Confidential, Sensitive or Public.

i. **Confidential:** Sensitive data that must be protected from unauthorized disclosure or public release.

Examples of "Confidential" data may include but are not limited to:
- Personally Identifiable Information, such as a name in combination with Identification Number (ID) and/or financial account numbers
- Employee records
- Intellectual Property, such as copyrights, patents and trade secrets

ii. **Sensitive:** Sensitive data that may be subject to disclosure or release.

Examples of "Sensitive" data may include but are not limited to:
- Operational information
- Personnel records
- Information security procedures
- Research
- Internal communications

iii. **Public**. Information intended or required for public release. However, any data owned or under the control of the South African Government must comply with the national classification authority and national protection requirements.

Furthermore, authorized officials who don't participate in Internet chats and news groups shall refrain from revealing confidential municipal information, client data and any other material covered by existing council policies and municipal procedures with regards to confidential information. Officials, who release protected information through the Internet whether or not it is advertent, shall be subject to all the applicable penalties in terms of Okhahlamba Local Municipality's existing data security policies and procedures.

10. OFFICIAL WEBSITE

The IT Officer shall be responsible for the maintenance and SEBATA INTERMAP shall be responsible for the design of Okhahlamba Local Municipality's website. Each Head of Department shall ensure that all information required by the Municipal Finance Management Act, as well as any other relevant legislations and Council Policies, is promptly and appropriately submitted to the IT Officer for display on the official website. The IT Officer shall (in consultation with the relevant Heads of Department) further decide on any other information to be made available on the website. Only the IT Officer and Heads of Department shall be authorized to amend, add and delete information on the official Okhahlamba Local Municipality website.

11. PROTOCOLS

11.1. Reporting Security Incidents

- If an IT Security incident or breach is suspected or noticed by any employee, then it is the obligation of that employee to immediately notify the IT Officer.
- Users are required to note and report any suspected security threats and/or weaknesses in and around IT systems and services. Critically, users must not attempt to prove a suspected weakness within a system, as testing weaknesses might be interpreted as a potential misuse of the system, which could lead to disciplinary action thereafter.
- The IT Officer is tasked with the security responsibility of Okhahlamba Local Municipality and must report all instances of a breach of security.
- When a breach of security occurs, the existing channels must be used to report it. It is the responsibility of the IT Officer to ensure that all breaches of security are reported.

- Breaches of security must at all times be dealt with using the highest degree of confidentiality in order to protect the ISO concerned and prevent him or her from being unnecessarily done an injustice to.

11.2. User Names

- All users must have proper usernames and passwords that will grant them access to the network and network services available for Okhahlamba Local Municipality. The username and password must be in accordance with standards used in all other government levels and departments to ensure a standardized network that can be easily managed and supported. As such, this standard incorporates the user's full name and first letter of user surname for the Network (e.g. John Smith's ID would be: JSmith).
- In the case of duplicate user names, the user's name will be placed vice versa of the above to make a user ID unique. No user is allowed to use the Administrator profile to gain access to the network unless that user is authorized to do so by the IT Officer.

12. PC SUPPORT

All support must be performed against a logged call with the details of the call that was logged. All network and PC support calls should be given priority and should be attended to as soon as is possible.

13.   DISASTER RECOVERY PLAN

The IT Officer, in consultation with the Municipal Manager and with the approval of Council, shall enter into such agreements with Okhahlamba Local Municipality's IT suppliers and/or with one or more other municipalities as necessary to ensure that the Okhahlamba Local Municipality Disaster Recovery Plan is in place, is operational, and is reviewed and tested at least once a year. The IT Officer shall prepare, review and update (as circumstances require) a list of persons who must be contacted by users in the event of any disastrous occurrence as set out in the Okhahlamba Local Municipality Disaster Recovery Plan. Such list shall be made available to all authorized users on Okhahlamba Local Municipality's IT Network, Shared Drive.

14.   TRAINING

The IT Officer shall liaise with various Heads of Departments and the Human Resources department with regards to the selection, training and monitoring of officials who have IT based and/or IT related responsibilities. The IT Officer shall coordinate, and where possible, shall provide the appropriate training to such officials as deemed necessary.

15.   ACCEPTANCE OF AND COMPLIANCE WITH THE IT SECURITY POLICY

Every employee who is allocated the use of any Okhahlamba Local Municipality IT equipment and/or authorized to access the Internet and/or Okhahlamba Local Municipality's computer network shall be provided with an email copy of the IT Security Policy by the IT Officer. All employees are required to read through the entire IT Security Policy and then sign the IT Security Compliance Agreement form (see Appendix A) attached to the policy in order to indicate that they have read, understood and accept to comply with this policy accordingly.

16.   ENFORCEMENT

Non-compliance, violation and disregard of this policy by any Okhahlamba Local Municipality employees, consultants and temporary staff shall result in disciplinary action and sanctions against the individual concerned and such sanctions may lead to termination of the individual's employment contract, depending on the circumstance and the gravity of the transgression. In the event of Okhahlamba Local Municipality incurring financial loss as a result of non-compliance, violation and/or disregard of this policy, Okhahlamba Local Municipality shall be entitled to institute legal proceedings to recoup the loss it has incurred from the individual and this shall be in addition to the disciplinary action that Okhahlamba Local Municipality would have taken against the individual.

17.   APPENDICES

A.   IT Security Policy Compliance Agreement

Appendix A

IT Security Policy Compliance Agreement

Employee Name (PRINTED):

_____

Department:

_____

I agree to take all reasonable precautions to assure that municipal internal information, or information that has been entrusted to the Okhahlamba Local Municipality by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with Okhahlamba Local Municipality, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Municipal Manager, who is the designated Information Owner.

I have access to an emailed copy of the Okhahlamba Local Municipality IT Security Policy, I have read and understood this policy, and I understand how it impacts on my job. As a condition of continued employment, I agree to abide by the policy and other municipal requirements, including non-disclosure of company information. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties. I also agree to promptly report all violations or suspected violations of IT policies and procedures to the designated IT Officer in charge.

Employee Signature: **Date:**

_____   _____

Information Security Officer Signature: **Date:**

_____   _____

DATE ADOPTED BY COUNCIL: …26…/…06……/…2013….