KAI !GARIB MUNICIPALITY

KAI !GARIB
MUNISIPALITEIT-MUNICIPALITY

IT SECURITY POLICY

IT Security Policy
Approval and Version Control

Approval Process:	Position:	Date:
Recommended by CFO	J. KRAPOHL	29-06-2015
Recommended by IT Steering Committee	J. KRAPOHL	29-06-2015
Approved by Council		29-06-2015
Effective		
Review Frequency: One a year (i.e. Annually)		
Version Number		

KAI !GARIB
Munisipaliteit/Municipality
29 JUN 2015
REGISTRASIE
REGISTRY

TABLE OF CONTENTS

1. INTRODUCTION

Computers enable employees of Kai !Garib Municipality to conduct the organisation's day-today 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 Kai !Garib 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 Kai !Garib 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, Kai !Garib Municipality.

2. OBJECTIVES

The objectives of the IT Security Policy are to:

2.1. Clarify to all users their responsibilities regarding the security of Kai !Garib Municipality's information and computing resources.

2.2. Define the potential risks and dangers for Kai !Garib Municipality in the event of misappropriation and abuse of computing equipment by users.

2.3. 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 Kai !Garib Municipality IT environment.

2.4. Regulate the professional and effective use of computing equipment within Kai !Garib Municipality, as well as between Kai !Garib Municipality and its external entities.

2.5. Establish a standard for the creation of User ID's and strong passwords, the protection of those passwords and the frequency of change thereof.

2.6. Identify the persons responsible for maintaining the security requirements.

2.7. Establish management direction, basis of procedures and requirements to ensure the appropriate protection of Kai !Garib Municipality's information and equipment resources by any means.

2.8. Ensure that the investment in information and equipment resources is properly managed.

2.9. Ensure that all systems are optimally utilised in its full capacity to the best advantage of Kai !Garib Municipality.

3. APPOINTMENT OF IT STEERING COMMITTEE

Kai !Garib Municipality shall appoint an IT Steering Committee that must meet at least four (4) times a year 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 Kai !Garib Municipality's computer networks with an organisation-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 Kai !Garib 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 Kai !Garib Municipality.

5. ADMINISTRATIVE CONTROLS

5.1. General Controls

5.1.1. The IT Officer will, on recommendation of the IT Steering Committee, issue guidelines on the use and application of Kai !Garib Municipality's network and shall monitor compliance with these guidelines, which must be strictly adhered to by all users of any IT systems.

5.1.2. The required administrative controls applicable to systems will be included in these guidelines and will comprise the following:

5.1.2.1. Physical controls over computer hardware, backups and software;
5.1.2.2. Access controls;
5.1.2.3. Data security controls; and
5.1.2.4. Internet and email usage controls.

5.2. Programming and Documentation Standards

5.2.1. Only the IT Officer, on recommendation of the IT Steering Committee, may liaise with IT software suppliers to provide developers for the development or modification of applications used by Kai !Garib Municipality.

5.2.2. The IT Officer shall keep a register of all such requests for amendment and/or enhancement of Kai !Garib Municipality software and hardware, and shall inform the relevant users of any changes.

5.3. Insurance

5.3.1. The Finance department shall ensure that appropriate and adequate insurance cover is obtained in respect of all components of Kai !Garib Municipality's IT operations.

5.4. Reporting

5.4.1. The IT Officer shall report to the CFO 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 month to which the report relates, and indicating how such problems have been or are being addressed.

5.5. Audits

5.5.1. The IT Officer, in consultation with the CFO, shall arrange audits of the IT systems on a periodic basis.

5.5.2. These audits may be conducted by either the internal or external auditors (or both), provided that sufficient budgetary provisions have been provided for.

5.5.3. 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 Kai !Garib 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 computer 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 Kai !Garib Municipality's officials.

6.1. Hardware

6.1.1. Where personal computers have been allocated to officials, such officials shall accept that these computers must be used to fulfil operational functions within the organisation and that their use is restricted to such official functions only.

6.1.2. All computers fitted with locking cases must be kept locked at all times.

6.1.3. No hardware may be installed or removed by any municipal official without prior consent and authorisation or direction from the IT Officer.

6.1.4. No hardware may be removed by any official from municipal premises without the prior written authority of the IT Officer in consultation with the CFO. 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.

6.1.5. 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 attend to the required repairs or replacement of the equipment, but subject to the necessary provision having been made in the budget.

6.1.6. 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. Wherever possible, screen previews should be used rather than physical printing. Original toners and inkjet cartridges must be used when printing is necessary, as not only may the compatible or refilled products void Kai !Garib Municipality's warranty in respect of the equipment, but they can also (in given circumstances) damage the printers.

6.2. Software Authorisation and Licensing

6.2.1. 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.

6.2.2. Only authorised and licensed software listed on the approved software listing may be loaded onto Kai !Garib Municipality's computers, and this may only be implemented with the consent and supervision of the IT Officer.

6.2.3. The IT Officer shall further ensure that this authorised 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 Kai !Garib Municipality and as the need for new or additional software arises.
Caution: No software may be downloaded through the Internet or via email. Also, pirated software by any official will not be permitted whatsoever.

6.2.4. Standard Applications

6.2.4.1. A new user is entitled but not limited to the following standard applications upon receiving a new computer or if the user is new to the municipality:
6.2.4.1.1. Antivirus Software;
6.2.4.1.2. Acrobat Reader;
6.2.4.1.3. MS Office Home and Business or MS Office Professional, where necessary;
6.2.4.1.4. Internet

6.2.5. Specialised Applications

6.2.5.1. A user is entitled to the municipality's applications once duly authorized
6.2.5.1.1. IMIS
6.2.5.1.2. SEBATA

6.3. Computer Manuals

6.3.1. The originals of software, hardware, systems manuals and guides shall be kept by the IT Officer with relevant licenses and discs.

6.3.2. The IT Officer shall further ensure that the manuals and release notes are updated with each new release installed on the systems.

6.4. Computer Room

6.4.1. Only the IT Officer and authorised personnel shall ordinarily have access to the computer room.

6.4.2. The server cabinet and computer room shall be kept locked.

6.4.3. Access to the computer room is via biometric (finger print) and keypad access.

6.4.4. The IT Officer shall ensure that adequate fire prevention and extinguisher systems are installed in the computer room, and that this equipment is regularly checked and maintained.

6.4.5. No official may tamper with such equipment, and no official may remove any such equipment from the computer room other than for the purpose of having it tested or serviced.

6.4.6. The IT Officer shall ensure that a properly designed, maintained and operated air conditioning system is installed in the computer room.

6.4.7. The IT Officer shall ensure that the servers within the server cabinet are raised in the event of flooding.

6.4.8. 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

7.1.1. Access control is necessary to restrict unauthorised 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 authorised, i.e. the access of such user to the system must be properly authenticated.

7.1.2. Access to the IT network comprises three steps:

7.1.2.1. Physical access to a workstation;
7.1.2.2. Access to the system; and
7.1.2.3. Access to specific commands, transactions, programmers and data within the system.

7.2. Physical Access to Systems

7.2.1. After the bona fide user has switched on his or her computer, the user must enter a password to gain further access to systems.

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

7.3.1. The IT Officer shall set access level priorities in accordance with the job descriptions of the officials concerned and to comply with further specific requirements of the officials from the relevant business unit.

7.3.2. Access level and amendment priorities shall be set out in writing by the IT Officer.

7.4. User Passwords

7.4.1. 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 Kai !Garib Municipality's entire network.

7.4.2. All Kai !Garib Municipality's employees, consultants and temporary staff with access to the organisation'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.

7.4.3. All officials, to whom user passwords have been allocated, must ensure that these passwords are properly safeguarded.

7.4.4. Under no circumstances may the employee share any user password with colleagues.

7.4.5. Passwords are used for various purposes at Kai !Garib Municipality. Some of the more common uses include: user level accounts, web accounts, email accounts, screensaver protection, application logins and logins to IT Hardware.

7.4.6. 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 Kai !Garib Municipality:

7.4.6.1. 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.

7.4.6.2. Passwords must not be inserted into email messages or other forms of electronic communication.
7.4.6.3. Passwords should not be a word in any language, slang, dialect or jargon.
7.4.6.4. Do not use the same password for Kai !Garib Municipality accounts as for other non-organisational access (e.g. personal account, option trading, benefits, etc.).
7.4.6.5. Users must not use the "Remember Password" feature for applications (e.g. Internet Explorer, etc.), and must not write passwords down.
7.4.6.6. Users must not store passwords in a file on any computer system (including laptops or similar devices).
7.4.6.7. Users must avoid using the same password for multiple applications.
7.4.6.8. 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.
7.4.6.9. If a user is requested to provide their password details to the IT Officer, they must ensure that they monitor the actions performed. Thereafter, the user should change their password immediately once the IT Officer has left.
7.4.6.10. Where possible, systems have been configured to follow Kai !Garib Municipality standards. The organisation's requirements for password settings should be as follows:
7.4.6.10.1. A minimum of seven (7) characters in length;
7.4.6.10.2. Must be changed every 42 days;
7.4.6.10.3. A password history of twelve (12) generations should be maintained;
7.4.6.10.4. Password complexity must be enabled and consist of alphanumeric and special characters;
7.4.6.10.5. User accounts are set to lockout after 3 unsuccessful login attempts; and
7.4.6.10.6. Users should not use their usernames as passwords.

7.4.7. 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.

7.4.8. 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.
7.4.8.1. Personal details, such as spouse's name, license plate, ID number or birthday, must not be used.
7.4.8.2. Words in a dictionary, derivatives of user ID's and common character sequences such as "123456" must not be used as well.
7.4.8.3. 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.
7.4.8.4. Users must not use cyclical passwords. For example, users should not add a numeric at the end of the password in sequence.
7.4.8.5. Passwords must not consist of all identical numeric or alphabetic characters, such as: "1111111" or "aaaaaaa".

7.4.8.6. Employees must never share their passwords with anyone, including the IT Officer, administrative assistants or secretaries.
7.4.8.7. All passwords are to be treated as sensitive organisational information.

7.4.9. Users must take note of and adhere to the following "Don'ts":
7.4.9.1. Do not reveal a password over the phone to anyone.
7.4.9.2. Do not reveal a password in an email message.
7.4.9.3. Do not talk about a password in front of others.
7.4.9.4. Do not hint at the format of a password (e.g. "my family name").
7.4.9.5. Do not reveal a password on questionnaires or security forms.
7.4.9.6. Do not share a password with family members or colleagues.
7.4.9.7. Do not reveal a password to co-workers while on vacation.

8. DATA SECURITY CONTROL

8.1. Privileges and Exposure

8.1.1. Access by users to Kai !Garib Municipality's IT systems shall be restricted in accordance with the job descriptions of officials concerned.
8.1.2. 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

8.2.1. Backup procedures will be determined by the IT Officer and communicated to all relevant users accordingly.

8.2.2. Backup procedures shall be adhered to by all users on the system.

8.2.3. To protect Kai !Garib Municipality's information resources from loss or damage, users are responsible for backing-up information stored on their machines.

8.2.4. Backups will be stored in a secure site.

9. INTERNET

9.1. Use of Internet

9.1.1. Internet access and related IT resources are provided to Kai !Garib Municipality at significant cost and are made available primarily for business use.

9.1.2. Users who have access to the Internet shall use this access solely in connection with
official responsibilities, including communicating with clients, working with related partners, local and provincial government agencies, providers of goods and services to Kai !Garib Municipality, and to also research relevant topics and obtain business related information which is of use to Kai !Garib Municipality.

9.1.3. Limited personal use on approved sites may be authorised when such access will be to the best advantage of Kai !Garib Municipality only.
9.1.4. 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.

9.1.5. Officials who use the Internet shall ensure that intellectual property of others is protected and that Kai !Garib 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.

9.1.6. Every official using the Internet facilities of Kai !Garib Municipality shall identify himself or herself honestly, accurately and completely.

9.1.7. Officials using the Internet shall do so only when this is required to fulfil their official
responsibilities and/or when they are authorised to do so.

9.1.8. 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.

9.1.9. Live streaming of video and / or audio signals over the Internet is prohibited.

9.2. Internet Browser

9.2.1. Kai !Garib Municipality reserves the right to block and track all visited sites.

10. AUTHORITY TO SPEAK ON THE BEHALF OF KAI !GARIB MUNICIPALITY

10.1. Only those officials who are duly authorised by the Municipal Manager to speak to the media, to analysts, in public gatherings or send external emails on behalf of Kai !Garib Municipality may do so.

11. INTEGRITY OF KAI !GARIB MUNICIPALITY'S IMAGE

11.1. Officials who are authorised to speak on behalf of Kai !Garib Municipality, as set out in section 10.1 above, shall ensure that they honour the image and integrity of Kai !Garib Municipality at all times, do not engage in any unauthorised political advocacy, and refrain from the unauthorised endorsement by Kai !Garib Municipality of any commercial product or service not sold or provided by Kai !Garib Municipality itself.

11.2. Officials must ensure that, where inputs are provided on behalf of Kai !Garib Municipality to any news group or chat room, such inputs have been grammar and spellchecked, and that the inputs reflect the view of Kai !Garib Municipality (where applicable) rather than the personal opinions of the writer.

12. SECURITY

12.1. Prompt disciplinary action shall be instituted against any official who attempts to disable, defeat or circumvent any firewall, proxy, Internet address screening programme or any other security systems installed by the IT Officer or any IT suppliers to assure the safety and security of Kai !Garib Municipality IT network.

12.2. Any officials who obtains a password, which allows access to the Internet and/or the organisation's IT network, shall keep such a password confidential, except if any occasion arises where any authorised technical support official requires knowledge of such password in order to solve a computer related problem.

12.3. As set out in 7.4 above, the present policy strictly prohibits the sharing of passwords between employees.

12.4. Logging onto the IT network or Internet with one's personal 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.

12.5. Every authorised 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.

12.6. The IT Officer will review all Internet activities and analyse the relevant usage patterns. Thereafter, appropriate action will be taken on the user wherever any abuse of the system is evident.

13. ELECTRONIC MAIL (Email)

13.1. Only authorised officials shall use the available email facility.

13.2. The IT Officer shall scan all emails for any inappropriate content or offending words or phrases.

13.3. All copies of emails shall be kept as records.

13.4. Only authorised officials shall be permitted to receive attachments through the email system.

13.5. The IT Officer shall maintain a list of prohibited and blocked email, and shall update and amend such list as circumstances require.

13.6. Kai !Garib Municipality reserves the right to monitor, access, retrieve, read, and/or disclose employee communications sent via the email system.

14. UNACCEPTABLE PRACTICES

14.1. No official may display any kind of sexually explicit material on any organisational system. Furthermore, no sexually explicit material may be archived, stored, distributed, edited or recorded using any of Kai !Garib Municipality's resources.

14.2. The IT Officer shall have the right to block access from within Kai !Garib 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.

14.3. Kai !Garib Municipality's IT related facilities, and especially its Internet facilities, may not be used knowingly by any official to violate the laws and regulations of the Republic of South Africa or any other nation, or the laws and regulations of any province or municipality.

14.4. The use of any municipal resources or illegal activities shall be grounds for the immediate dismissal of the official concerned, and the Council and its officials undertake further to cooperate with any legitimate law enforcement agency in this regard.

14.5. No employee may knowingly use Kai !Garib Municipality's IT facilities and resources to download or distribute pirated software or data.

14.6. No official may knowingly use the Internet facilities to propagate any viruses, worms, Trojan horses or trap doors (i.e. malicious code).

14.7. No official may knowingly use Kai !Garib 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.

14.8. No employee with authorised Internet access may upload any software licensed to Kai !Garib Municipality or data owned or licensed to Kai !Garib Municipality without prior authorisation of the IT Officer.

14.9. No official may create a communication link requiring dial-out access from any computer which is also connected to the IT network.

14.10. No official may use any software which is not provided or approved by the IT Officer.

14.11. Only the IT Officer shall authorise the provision of email addresses to authorized users.

15. OWNERSHIP AND CLASSIFICATION OF DATA

15.1. Any Kai !Garib Municipality data that is created, sent, printed, received or stored on systems owned, leased, administered or authorised by Kai !Garib Municipality is the property of Kai !Garib Municipality and its protection is the responsibility of Kai !Garib Municipality's designated custodians and users.

15.2. Data shall be classified as either: Confidential, Sensitive or Public.

15.3. **Confidential:** Sensitive data that must be protected from unauthorised disclosure or public release based on local or governmental law (e.g. the Promotion of Access to Information Act, No. 2 of 2000) and other constitutional, statutory, judicial and legal agreements. Examples of "Confidential" data may include but are not limited to:

15.3.1. Personally Identifiable Information, such as a name in combination with Identification Number (ID) and/or financial account numbers
15.3.2. Employee records
15.3.3. Intellectual Property, such as copyrights, patents and trade secrets

15.4. **Sensitive:** Sensitive data that may be subject to disclosure or release under the Promotion of Access to Information Act, No. 2 of 2000, but requires additional levels of protection. Examples of "Sensitive" data may include but are not limited to:

15.4.1. Operational information
15.4.2. Personnel records
15.4.3. Information security procedures
15.4.4. Research
15.4.5. Internal communications

15.5. Public: Information intended or required for public release as described in the Promotion of Access to Information Act, No. 2 of 2000. However, any data owned or under the control of the South African Government must comply with the national classification authority and national protection requirements.

15.6. Sensitive Information, from the time it is created until the time it is destroyed or declassified must be labelled (marked) with an appropriate information classification designation. Such markings must appear on all manifestations of the information (hardcopies, floppy disks, CD-ROMs, etc.).

15.7. Authorised officials who 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.

15.8. Officials, who release protected information through the Internet whether or not it is inadvertent, shall be subject to all the applicable penalties in terms of Kai !Garib Municipality's existing data security policies and procedures.

16. WIRELESS SECURITY

16.1. All wireless Access Points / Base Stations connected to the Kai !Garib Municipality network must be registered and approved by the IT Officer.

16.2. Access Points / Base Stations must be subject to periodic penetration tests and audits.

16.3. All wireless Network Interface Cards (i.e., PC cards) used in laptop or desktop computers must be registered with the IT Officer.

16.4. All access points (APs) must be logically secured to prevent unauthorised access to the AP configuration environment.

16.5. AP devices must be configured to only allow pre-defined authorised administrators to make configuration changes.

16.6. AP's must be physically secured to protect the AP against physical manipulation.
16.7. All wireless LAN access must use Kai !Garib Municipality approved vendor products and security configurations.

16.8. All computers with wireless LAN devices must utilise Kai !Garib Municipality approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic.

16.9. Wireless implementations must maintain point to point hardware encryption of at least 64 bits.

16.10. Wireless implementations must support a hardware address that can be registered and tracked, i.e., a MAC address.

16.11. Wireless implementations must support and employ strong user authentication.

16.12. The SSID shall be configured so that it does not contain any identifying information about the Kai !Garib Municipality, such as the Kai !Garib Municipality division title, employee name, or product identifier.

17. OFFICIAL WEBSITE

17.1. The IT Officer shall be responsible for the maintenance of Kai !Garib Municipality's website, with the assistance of the service provider.

17.2. Each Head of Department shall ensure that all information required by the Municipal Finance Management Act, as well as any other relevant legislation and Council Policies, is promptly and appropriately submitted to the IT Officer for display on the official website.

17.3. 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.

17.4. Only the IT Officer can provide authorisation to the service provider, to amend, add and delete information on the official Kai !Garib Municipality website.

18. PROTOCOLS

18.1. Reporting Security Incidents

18.1.1. 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.
18.1.2. Users are required to note and report any suspected security threats and/or weaknesses in and around IT systems and services.
18.1.3. 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.

18.2. User Names

18.2.1. All users must have proper usernames and passwords that will grant them access to the network and network services available for Kai !Garib Municipality.
18.2.2. The username and password must be in accordance with the following standards:
18.2.2.1. Minimum length: 7 characters
18.2.2.2. Maximum age: 42 days
18.2.2.3. Composition: Alphanumeric and special characters and password complexity must be enabled;
18.2.2.4. Password history: 12 generations should be maintained
18.2.2.5. The screensaver setting should be set to 5 minutes of inactivity.
18.2.2.6. User accounts will be locked automatically if the user enters the incorrect password on 3 consecutive occasions.
18.2.3. On all systems, the standard naming convention incorporates the user's full surname and initial (e.g. Wesley Bok's ID would be: bokw@kgmun.gov.za)
18.2.4. In the case of duplicate user names, the user's surname and other initials will be used or may include numbers to ensure a user has a unique ID.

19. PC SUPPORT

19.1. All support must be performed by the IT Officer and he must be provided with the details of the problem.

19.2. All network and PC support calls should be given priority and should be attended to as soon as is possible.

20. DISASTER RECOVERY PLAN

20.1. The IT Officer, in consultation with the CFO and with the approval of Council, shall enter into such agreements with Kai !Garib Municipality's IT suppliers and/or with one or more other municipalities as necessary to ensure that the Kai !Garib Municipality Disaster Recovery Plan is in place, is operational, and is reviewed and tested at least once a year.

20.2. 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 Kai !Garib Municipality Disaster Recovery Plan.

20.3. Such lists shall be made available to all authorised users on Kai !Garib Municipality's IT Network.

21. IT TRAINING AND SECURITY AWARENESS

21.1. The IT Officer is responsible for providing security awareness training, on a periodic basis, to new and existing employees.

21.2. Training on applications used by the municipality will be provided to end users by the relevant service provider.

21.3. The Finance Department will facilitate the training between service providers and end users on applications used by the municipality.

22. ACCEPTANCE OF AND COMPLIANCE WITH THE IT SECURITY POLICY

22.1. Every employee who is allocated the use of any Kai !Garib Municipality IT equipment and/or authorised to access the Internet and/or Kai !Garib Municipality's computer network shall be provided with an email copy of the IT Security Policy by the IT Officer.

22.2. 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.

23. ENFORCEMENT

Non-compliance, violation and disregard of this policy by any Kai !Garib 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 Kai !Garib Municipality incurring financial loss as a result of non-compliance, violation and/or disregard of this policy, Kai !Garib 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 Kai !Garib Municipality would have taken against the individual.

24. APPENDICES

A. IT Security Policy Compliance Agreement

Appendix A
IT Security Policy Compliance Agreement

Employee Name: _____

Department: _____

I agree to take all reasonable precautions to assure that municipal internal information, or information that has been entrusted to the Kai !Garib Municipality by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with Kai !Garib 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 Kai !Garib 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 municipal 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:** _____

IT Officer Signature: _____ **Date:** _____