KOUGA
local municipality
Prosperity through vision

INFORMATION TECHNOLOGY (IT) POLICY

Incorporating the following:

DATA & SYSTEMS SECURITY

NETWORK SECURITY

INTERNET, INTRANET, EXTRANET AND E-MAIL

(APPROVED BY COUNCIL ON 20 SEPTEMBER 2012)

Table of Contents

DATA AND SYSTEMS SECURITY POLICY

NETWORK SECURITY POLICY

INTERNET, INTRANET, EXTRANET AND E-MAIL POLICY

1. Preamble

Information and information systems are critical and vitally important to the Municipality. Without reliable information the Municipality could be adversely affected, both financially and reputation wise. Therefore, this Policy states the minimum requirements and the responsibility that all employees, temporaries, contractors and management must comply with in order to secure the Municipality's information.

This Policy sets out the approach taken to manage information security to ensure that information assets are properly protected against a variety of threats such as error, fraud, embezzlement, sabotage, terrorism, extortion, privacy violation, service interruption, theft and natural disaster, whether internal or external, deliberate or accidental.

KOUGA Municipality Management has a duty to preserve, improve, and account for all information and information systems. They must additionally make sure that information assets are protected in a manner that is at least as secure as other organizations in the same industry handling the same type of information. To achieve this objective, annual reviews of the risks to the Municipality's information assets will be conducted. Similarly, whenever a security incident or audit finding indicates that the security of information or information systems is insufficient, management must promptly take remedial action to reduce the Municipality's exposure.

The Municipality's information must be protected in a manner appropriate to its sensitivity, value, and criticality. Security measures are therefore used regardless of the media on which information is stored, the systems that process it, or the methods by which it is moved. This protection includes restricting access to information based on the need-to-know principle.

Decision-making within the Municipality is also critically dependent on information, as Management need to be able to rely on the integrity of information in terms of accuracy, timeliness, relevance, completeness, confidentiality, criticality, etc. The awareness of and fine-tuning of such information is an important information management activity.

Information security requires the participation and support from all staff (including consultants, contractors, and temporaries) who will be provided with sufficient training and supporting procedures / policies to allow them to properly protect and manage the Municipality's information assets.

It is the responsibility of all Municipal staff to report any software malfunctions, security incidents, suspected viruses, faults, weaknesses or threats observed or suspected to systems or services to the Helpdesk, Network Administrator or Manager responsible for information/system security as soon as possible to enable the volumes and costs of incidents and malfunctions to be quantified and monitored.

2. Purpose of the Policy

This document defines the Policy of the Municipality for the application of information security to protect the Municipality's corporate information, information systems and applications against all threats, which could endanger their confidentiality, integrity and availability.

The objective of information security is to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents. The purpose of this Policy is to protect the Municipality's information assets in terms of Confidentiality, Integrity and Availability.

3. Scope

This Policy applies to all offices and users of information within the Municipality. It applies across hardware platforms, to all departments, business units and to all partners, staff and contractors of the Municipality.

4. General Guidelines

All Managers within the Municipality are responsible for ensuring that personnel within their Departments receive and understand the IT Policy of the Municipality. Staff are required to sign an Acceptance of Conditions of Policy.

Clients and stakeholders that access the Municipality's IT facilities are required to sign an Acceptance of Conditions of Policy.

The Management of the Municipality's IT facilities rests with the IT section and can involve third party contractors as service providers for the Municipality. Where this is so, the service provider must sign an Acceptance of Conditions of Policy.

Non-Municipal employee's access to the Municipality's IT facilities is subject to the IT policy. Consultants employed in a permanent capacity by the Municipality are classified as Municipal employees for the purposes of this Policy.

Part time contractors and consultants who may have access to Municipal IT facilities, infrastructure, systems and information will be required to sign an Acceptance of Conditions of Policy.

5. Information Security Definitions

Information security encompasses the management processes, technology and assurance mechanisms that will allow departments to trust their transactions, ensure that the information is usable and can appropriately resist and recover from failures due to error, deliberate attacks or disaster; and that confidential information is withheld from those who should not have access to it.

6. High Level Information Security Principles

6.1 Protection

The Municipality's information must be protected in a manner commensurate with its sensitivity, value, and criticality. Security measures must be employed regardless of the media on which information is stored (paper, overhead transparency, computer bits, etc.), the systems, which process it (microcomputers, firewalls, voice mail systems, etc.), or the methods by which it is moved (electronic mail, face –to -face conversation, etc.). Such protection includes restricting access to information based on a need –to -know basis. Municipal Management must devote sufficient time and resources to ensure that information is properly protected.

6.2 Risk Management

Managers are ultimately responsible to ensure that the information is protected in a manner that is acceptable to higher management. To achieve this objective, risks should be identified by conducting regular risk analysis and, to take corrective measures where applicable.

6.3 **Information Management**

Decision-making within the Municipality is also critically dependent on information and information systems. Management is expected to know the nature of information they use for decision -making (accuracy, timeliness, relevance, completeness, confidentiality, criticality, etc.). The awareness of and fine -tuning of such information attributes is an important information management activity.

6.4 **Co-operation**

Information security requires the participation of and support from all information users. All users (employees, consultants, contractors, third parties and temporaries) must be provided with sufficient training and supporting reference materials to allow them to properly protect and otherwise manage Municipal information assets. Training materials should communicate that information security is an important part of the Municipality. Training and documentation with respect to information security is the responsibility of the Network Administrator in conjunction with a service provider (where applicable).

6.6 **Organization**

Guidance, direction, and authority for information security activities are centralized for the entire organization in the office of the Network Administrator. The office is responsible for establishing and maintaining organization -wide information security policies, standards, guidelines, and procedures. Compliance checking to ensure that organizational units are operating in a manner consistent with these requirements is the responsibility of the Internal/External Audit Department. Investigations of system intrusions and other information security incidents are the responsibility of the Manager responsible for information and systems security.

6.7 **Privacy**

All messages sent over Municipal computer and communications systems are the property of the Municipality. To properly maintain and manage this property, Management reserves the right to examine all data stored in or transmitted by these systems. Since the Municipality's computer and communication systems are provided for business purposes, workers should have no expectation of privacy associated with the information they store in or send through these systems. In recognition of the privacy requirements as stated in the

Constitution of South Africa, personal information will not be disclosed to any third party unless explicitly required through legal processes.

6.8 Third Parties

As a condition of gaining access to the Municipality's computer network, every third party must secure its own connected systems in a manner consistent with the Municipality's requirements. The Municipality reserves the right to audit the security measures in effect on these connected systems without warning. The Municipality also reserves the right to immediately terminate network connections with all third party systems not meeting such requirements.

7. Generally Applicable Policies

The following Policy statements constitute the core of the Municipality's Information Security Policy for information and will be supported by information security directives and standards as needed from time to time.

7.1 Classification

Information must be categorized into levels of sensitivity and protected in accordance with appropriate requirements as part of the risk management process. The sensitivity classification standard must be used throughout the Municipality to ensure that the level of protection is commensurate with the controls required (security mechanisms) to protect the information against disclosure (confidentiality), modification (integrity) and / or destruction (availability and use).

7.2 Confidentiality

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

Unless authorized by Management, information may not be made available or disclosed to unauthorized individuals, entities or processes.

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

7.3 **Availability**

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

All information assets should be protected against:

(i) Destruction, damage or contamination

(ii) Denial of authorized / legitimate access

(iii) Delay of use or access

(iv) Natural disasters

(v) Computer virus infections

7.4 **Integrity**

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

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

7.5 **Non-Reputation**

All access to the Municipality's technology resources is subject to positive identification and authentication of the user before access is granted.

Measures must be implemented to ensure the non-repudiation of all financial transactions in accordance with official legislation and regulations. Processes must be implemented to allow for the non-repudiation of origin regarding sensitive E-Mail.

7.6 **Accountability**

Measures must be implemented to ensure that it is possible to determine who is responsible for an action, when and from where. The measures must be in accordance with the security requirements as determined by the Departmental Manager.

7.7 Access Control

All data and information will be protected and safeguarded against unauthorized access. Access to technology resources will only be granted in line with the user's specific responsibilities (need-to-have principle).

7.8 Authentication

Measures must be implemented to uniquely identify or verify IT users, peripherals and / or programs and to assure individual accountability. The authentication mechanisms must be in accordance with the classification of the information that requires protection and may for example take the form of passwords, tokens, or biometric identification devices.

All users will access the Municipality's information systems through at least the use of a unique user identification number and secret password. As a first line of defense, users should select passwords that are not easily guessable nor should personal passwords be shared with any other user.

7.9 Reporting of Security Incidents

All known vulnerabilities – in addition to all suspected or known violations – must be reported in an expeditious and confidential manner to the Office of the Network Administrator or Manager responsible for security. Unauthorized disclosure of the Municipality's information must additionally be reported to the involved information owners. Reporting security violations, problems or vulnerabilities to any party outside the Municipality without prior written approval of the Office of the Network Administrator is strictly prohibited.

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

7.10 Exceptions

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

1. **General Requirements**

Ownership - The Kouga Municipality Council is the owner of the policy.

Applications for remote access services will only be allowed to personnel and clients or contractors, based on a valid business need. All applications must be approved in writing by the applicant's Manager, and handed to the Manager responsible for IT security. The Manager will consider all applications for approval after consideration of the risk. Periodic access reviews will be conducted with the assistance of HR to ensure incumbents are still in the Municipality's employ. All accesses must be reviewed at least annually by the applicant's manager and where applicable, terminated / suspended.

As part of the application process and before access is allowed, the applicant should sign an Acceptance of Conditions of the IT Policy.

A central register must be maintained by the IT Department of all users with dial-in / remote accesses, also indicating the access authorities to facilitate auditable processes.

To minimize the risk of compromising security, all users of the remote access services must receive training before access is allowed. The training should include what is allowed and what is not allowed during sessions.

In order to ensure compliance in terms of software, hardware and security requirements, the computer used for the remote access should be provided by the Municipality. The use of private (home) computers may only be allowed if based on a valid business need and must be processed as a deviation from this Policy. The Manager/Department responsible for IT security shall maintain a central register of all the deviations.

The remote client (computer used to access the Municipality's network) must have anti-virus software and the correct level of security patches as prescribed by the IT function from time to time. A process must be formulated by the IT function to ensure the regular update of the software/patches.

Under no circumstances may the access privileges be transferred to another user without following the official normal application procedure.

No user may be provided with access privileges that exceed those than would otherwise be afforded if working in the office (least access / authorization principle). For example if the request was to have access to the mailbox/calendar, no other access may be provided.

To prevent an open session from being misused by unauthorized persons, all sessions must automatically be logged-off after 30 minutes of inactivity.

The users are responsible for both logical and physical security mechanisms to the computer that is used to obtain the remote access. Due to the risk of theft, users are advised to encrypt stored data for protection. The Municipality's security requirements must be communicated to users during the training session.

Comment: Logical access control refers to the measures taken to prevent an unauthorized person to get access to your computer whereas physical mechanisms relates to the physical measures taken (first and second perimeter of defense).

Confidential information stored on remote computers must be protected against unauthorized access.

Formal agreements with clients, partners, contractors or third parties is a requirement and must include the principle that required minimum standards compliance must be verifiable/auditable if remote access is provided.

2. **Authentication Requirements**

Authentication servers must be configured to enforce the Municipality's password standards. Strict physical and logical access control to the authentication servers and communication equipment must be enforced.

As a minimum requirement, a unique user ID and difficult to guess password must be used for authentication.

Users having power access privileges (e.g. to execute remote maintenance tasks and access to sensitive information and / or critical resources), may only be allowed access through the Municipality's accepted authentication mechanisms. (Sensitive information is defined as information that if disclosed, will seriously and adversely affect the Municipality, its business partners and / or clients and will constitute a serious compromise in the status of the Municipality's operational security).

A forced password change must be implemented on the first sign-on session (to change the initial password) and thereafter every thirty (30) days. The IT function should implement a process to ensure the secure communication of the initial password.

No double sessions with the same authentication information may be allowed.

To confirm the origin of the connection, dial-back features must be implemented if token-based authentication is not utilized.

Authentication information between the users and the authentication servers must be protected with encryption.

Users no longer requiring the access (e.g. change in job description or transfer) must be immediately removed from the system. Line management must reconsider the access privileges of users who resign as soon as possible after formal notice of the resignation. Special attention should be given to audit logs to ensure that the accounts are no longer active.

All changes to existing and new user accounts/profiles must follow a formal change management process.

In support of the information security strategy to protect, detect and re-act, all available audit logs and alert facilities must be enabled with monitoring and review processes in place. The reports must be reviewed by the IT support/security function and, where applicable, investigated / escalated to the manager responsible for IT security.

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

3. **Clear Screen and Clear Desk Policy**

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

All waste paper, which has any sensitive or important Municipal information or data on, must be shredded or placed in the secure shredding boxes located in some areas. Under no circumstances should this type of waste paper be thrown away with normal rubbish in the bins under each desk.

Whenever the user leaves their desk and the PC is switched on, it is essential that the user ALWAYS 'locks' their screen by pressing 'Ctrl Alt Delete' and then enter to confirm that they wish to 'lock' their workstation. (Alternatively the Windows key in conjunction with the L can be pressed). Remember that the user will need their password to sign on. Users should use the screensaver password function to activate after 5 minutes of inactivity.

Locking the screen not only prevents someone else from using the PC, which is logged on in the user's name, but it also prevents someone from reading sensitive information on the screen.

4. **Passwords**

Passwords must **NEVER** be disclosed to anyone. If the user suspects that the confidentiality of the password has been compromised, the user must change it immediately and inform the Network Administrator.

Passwords must be changed every thirty (30) days; the authentication server must be set to automatically expire passwords after thirty (30) days.

Passwords should be made up of characters using:

Alpha (alphabetical letters), numeric (whole numbers), upper & lower case and symbols.

They should have a minimum length of Seven (7) characters.

Never use any dictionary words, acronyms, birthdays, sequential numbers, family names, football teams; dates etc, as software tools can easily crack these (must not be easily guessable).

Passwords should not be written down unless protected in some or other form (e.g. by using a sort of encryption and locking it away).

The authentication server/system will maintain a list of up to twelve (12) previous passwords used per user and each new password should contain at least 3 changes. The objective of this rule is to prevent users re-using the same password over and over.

5. **Access Control Policy**

Access to systems will only be granted where there is a clearly established business need, which is consistent with the roles and responsibilities of those granted access.

Staff must not attempt to bypass the physical security mechanisms (turn-stiles & trapdoors), or electronic (logical) security measures.

The physical security steps taken are the first line of defense against unauthorized access to the Municipality's information assets.

6. **Virus Protection**

The IT function must always ensure that computers are equipped with an approved anti-virus software package.

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

Train users not to open suspicious looking E-Mail. Always confirm the bona fides of the originator if uncertain about the contents.

Users should check with the Helpdesk before forwarding E-Mail about new viruses to colleagues. In many instances it is a false alarm with the intent to cause panic thereby flooding the network with unnecessary messages.

When staff members are required to use their home personal computer for official Municipal duties, the PC should have an anti-virus program installed. The program should be updated regularly to ensure that provision is made for the latest viruses.

7. **Account Policies**

7.1 **Password**

Enforce password – Twelve (12) passwords will be remembered by the system. This will prevent the user from using the same password continuously. Should a user forget his/her password the system administrator must be contacted.

Maximum password for expiry - Thirty (30) days, after which the user must enter and confirm a new password.

Minimum password length - Seven (7) Characters that must include at least one uppercase alpha numerical, one lowercase alpha numerical and one numeric symbol. Special characters are also allowed, but are optional.

7.2 **Account Lockout**

Account lockout threshold - Three (3) invalid logon attempts will be permitted after which the user account will be locked out. To reset the account the system administrator must be contacted.

Account lockout duration - Permanent. To reset network administrator must be contacted.

7.3 **General**

Enforce user logon restrictions - Enforced. Coupled to account logon hours.

Maximum tolerance for computer clock synchronization - Five (5) minutes

8. **Local Policies**

8.1 **Audit Policy**

Audit account logon events - Attempts will be logged on success and failure to logon to the network.

Audit account management - Success and failure will be monitored daily.

Audit directory service access - Success and failure will be monitored daily.

Audit logon events - Success and failure will be monitored daily.

Audit object access - Success and failure will be monitored daily.

Audit policy change - Success and failure will be monitored daily.

Audit privilege use - Success and failure will be monitored daily.

Audit process tracking - Success and failure will be monitored daily.

Audit system events - Success and failure will be monitored daily.

8.2 **Security Options**

Automatically log off users when logon time expires - Logon hours will be between 07H00 and 17H00. After this time period users will be logged off by the system. Any user

that works after these hours must apply to the IT section for permission to change logon times.

Do not display last user name in logon screen – Enabled.

Prevent users from installing printer drivers – Enabled.

Prevent users from installing software – Enabled.

WWW Browser access - All browsers shall be configured to access the Internet via proxy servers or via a site-proxy server, which is configured to access the Internet. No other form of access to sites on the Internet is permitted. This includes connections to alternative service providers by means of a dial-up modem, leased data line, private microwave link, radio modem or any other form of access method. Users shall be held liable for breaches of security, loss of data or the compromise of information caused by unsafe browsing practices.

Firewall – A firewall will be installed to protect the Municipality's internal networks and systems from external attack and penetration attempts. The creation of a demilitarized zone is preferred, but not mandated. This policy may be revised should the Municipality experience a high incidence of penetration attempts. The firewall should be configured to provide at least the following:

Network Address Translation (NAT)

Proxy services

Port blocking and control

Packet sniffers

Intrusion Detection and virus attack protection

WWW management features

Logging of audit information

Custom rule formulation and configurations

9. **User Policy**

The access provided by the Municipality is not to be used to access any material of a sexual, violent, destructive or potentially harmful nature. The system must be used in a moral and ethical manner.

Due to system limitations, remote access connections may not be used for a period longer than 8 hours per day.

Unless specifically specified, the Municipality does not offer technical support for personal (home) computers.

Passwords must be kept secret and may under no circumstances be disclosed or transferred to another user without following the official application process.

Users are expected to report all breaches or suspected breaches of security to the Manager of IT and their immediate Manager.

The account may not be used to conduct any illegal activities. It is the responsibility of Management to ensure that the security policies are effectively communicated to users in order to establish accountability.

The computer must be kept updated with the latest Municipal accepted anti-virus agent. The Municipality employees can obtain a copy from the IT Department.

Users will be held accountable for actions committed under the specific user profile.

Users may not leave their computers unattended with an open session. Users should either sign-off, activate a password screensaver, or lock the screen if the computer is unattended and still signed on.

Users must respect copyright, trademark, licenses and related legislation.

The service must be used in a manner that does not interfere or disrupt other network users, services and / or equipment.

10. **Legal and Regulatory Requirements**

Although the personal use of the Municipality's information systems is allowed within limits, abuse of these systems and the use of obscene, racist or otherwise offensive statements are strictly prohibited.

The Municipality will function within the constraints of and comply with statutory laws and regulations. Where applicable, international laws will also apply (i.e. VISA MasterCard Standards).

11. **Disciplinary Code of Practice**

Refusal to adhere to this policy will be considered as misconduct and depending on the circumstances and seriousness of the offense, disciplinary action may take, inter alia, one of the following forms:

Disciplinary Counselling

Verbal Warning

Written Warning

Termination of Service; or

Summary Dismissal

Action	1st Occurrence	2nd Occurrence	3rd Occurrence
Changing any configuration settings to bypass security or any other control mechanism thereby exposing the Municipality's information assets to unauthorized-, -modification, -destruction, -corruption or -disclosure of confidential information.	Final Warning	Dismissal	
Allowing another user to access the Municipality's network with your account details and password.	Written Warning	Final Written Warning	Dismissal
Using the account of another user to obtain unauthorized access to data, files or network services.	Written Warning	Final Warning	Dismissal
Any attempt to test or bypass security mechanisms or processes.	Final Warning	Dismissal	

Action	1st Occurrence	2nd Occurrence	3rd Occurrence
Abusing specific resources or services e.g. E-Mail or internet.	Written Warning	Suspension of remote access and final warning.	Dismissal
Loss of the Municipality's assets e.g. laptops due to neglect (eg. theft out of a car that was left unattended with valuable Municipal assets in the car).	Written Warning	Suspension of remote access privilege, final warning and replacement of computer.	Dismissal
Infecting the Municipality's network with viruses by neglecting to install and update or by removing the prescribed anti-virus agent on the remote computer.	Final Warning	Dismissal	
Failure to report unauthorized policy / standard deviations or security incidents	Warning	Final Warning	Dismissal
Loading illegal software, thereby infecting the Municipality with computer viruses or Trojan horses.	Final Written Warning/ Dismissal	Dismissal	
Failure to use the official anti-virus product on personal desktops and laptops.	Written Warning	Final Warning	Dismissal
Willfully downloading and/or opening of virus-infected files.	Final Written Warning	Dismissal	
Disabling, uninstalling or changing the original configuration of the Municipality's anti-virus product, unless specifically authorized to do so.	Written Warning	Final Warning	Dismissal
The configuration and use of unauthenticated shares	Written Warning	Final Written Warning	Dismissal

12. **Implementation Plan**

Subject	Channel / Actions
Top-down communication	Communication of Policy existence by members of the Information Technology Steering Committee (ITSC) to Managers of all Municipal Departments and third parties.
Awareness	Publication on Intranet and Bulletin Board System (if available). Prepare electronic presentation with security and operating requirements for users. Request new and existing users to acknowledge receipt of Policy and to sign Acceptance of Conditions of the IT Policy.
Management Issues	Determine current compliance to Policy and define gaps. Define plan of action to align with Policy. List residual risks and Management plans. Review and update dial-up connection processes. Continuous monitoring of compliance. Regular review and dissemination of policy.

NETWORK SECURITY POLICY

1. **Purpose**

The purpose of this Policy is to provide a solid foundation for the development, implementation and maintenance of secure practice within ***KOUGA*** Municipality's networking environment.

2. **Background**

Network security involves the protection of the Municipality from the threats posed by authorized and unauthorized network activity. The threats increase due to the interconnectivity of networks and the convergence of different network services (voice, data etc), making it difficult to draw boundaries around the Municipality and to apply controls for the protection of the internal assets.

There are obvious dangers that external connections may increase the risk of a security compromise, whilst being unaware of the risk. Network connections should therefore be protected at a level based on the risk. The assumption must be that connecting parties are to a certain degree hostile and have to be strictly controlled to ensure that the access, for which the connection was agreed, is maintained.

3. Scope

This Policy applies to all network administrators, technical and maintenance personnel, designers, users and the owner of the Municipality's network. The network security policy is considered as part of the Municipality's IT Policy.

4. Terminology

For the purposes of this Policy the following terminologies apply:

"Information Security" Information Security encompasses the Management processes, technology and assurance mechanisms that will allow the Municipality to trust their transactions, ensure that the information is usable and can appropriately resist and recover from failures due to error, deliberate attacks or disaster; and that confidential information is withheld from those who should not have access to it.

"Network Security" The protection of networks and their services from unauthorized modification, destruction or disclosure and providing the assurance that the network performs its critical functions correctly.

"Network Device" Any information technology and communication device used to form the infrastructure required for communication services (servers, routers, switches, bridges, firewalls, encryption devices).

"De-Militarised Zone (DMZ)" The frontline when protecting valuables (i.e. information assets) from direct exposure to an untrusted environment, or; a network added between a protected network and an external network in order to provide an additional layer of security.

"Sensitive Information" Any information that, if disclosed without appropriate authorization, will compromise the Municipality's security or business initiatives.

"Network Sniffing" The use of hardware and/or software mechanisms to analyze / monitor electronic communications (traffic) over a network.

"Operational Environment" The environment responsible for the implementation and maintenance of the day-to-day security activities.

"Communication Carrier" The infrastructure provided by a service provider (e.g. TELKOM) to interconnect communication devices.

"Computer Network" A range of computers connected by means of communication carriers.

"Data Traffic" Information in electronic format, which is communicated over a communications carrier.

"Access" Physical or logical access to information or information systems through a range of network devices.

5. Policy

5.1 General Policy Requirement

It is the policy of the Municipality to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of information. As a minimum, authentication, access control, privacy (confidentiality), integrity, availability and audit logging must be implemented as security services on the Municipality's network.

5.1.1 Authentication

All network devices, management stations and network users / administrators must have unique identifiers in accordance to a defined naming convention. Passwords must be implemented in accordance with the Municipality's password standards.

5.1.2 Logical access control

Access control mechanisms must be implemented on all network devices and management systems. Access may only be granted in line with the job responsibilities of Network Administrators (based on the "need-to-have" principle). External access to network devices and Management systems must be restricted to the minimum and where applicable, strict control mechanisms must be implemented.

5.1.3 **Privacy / Confidentiality**

All reasonable measures must be taken to ensure that internal and external communications between networks and network devices as well as client interfaces may not compromise security. Where applicable, encryption mechanisms must be implemented.

5.1.4 **Integrity**

Mechanisms / procedures must be in place to ensure the integrity of all network devices and traffic. Real time alerts should be generated for all configuration / permission changes that can lead to a breach in security.

5.1.5 **Audit logging / accountability**

Audit information, including alerts generated for failed logon attempts, must be available for all network devices and management systems.

5.1.6 **Availability**

Network(s) and network services must be available as and when required and capable of handling the network traffic requirements.

5.2 **Network Management**

The Manager responsible for Information Technology must assign overall responsibility for network activity and appoint a network owner. It is the responsibility of the network owner to, among others, ensure compliance with this Policy and to provide monthly feedback with regard to the state of compliance as part of the Municipality's information security risk management process. The Network Administrator will fulfill this role.

Network strategy, standards, principles, guidelines, architectures, procedures, design, configuration, equipment, software, inventories and cabling information must be formally documented, kept up to date and reviewed annually. Only authorized personnel may be allowed access to this information / documentation in accordance with the sensitivity / security classification.

Human resources and infrastructure that are critical to the continuity of network services should be identified and single points of failure must be minimized.

All external connections to the Municipality's network must be preceded with a risk analysis and at a minimum be protected by a firewall or similar type of device. Non IP network connections must be secured by definition characteristics and / or specific configurations to restrict access capabilities and to meet the security requirements. The connections must be reviewed periodically via a traceable process. Where applicable, internal networks (i.e. LAN's), where sensitive information is processed, must also be protected commensurate to its sensitivity.

All external connections / third parties to the network should be assigned an owner, approved by the network owner and the head of the business unit, individually identified and recorded. (Please refer to the detailed policy on third party connections).

In order to provide a clear picture of the network and to minimize unwanted connections, network access control must be centrally approved by the network owner or a responsible person as appointed by him/her.

The Municipality's network should preferably be protected by creating a DMZ. No sensitive information may be stored in the DMZ.

Services obtained from internal or external service providers must be defined in formal agreements. The agreements must specify the requirements for security controls. Mechanisms must be in place to measure adherence to these requirements.

Only network services required specifically for business purposes are allowed and all unnecessary network services must be disabled.

Formal set-up standards must be agreed to and no network device may be deployed in the operational environment with default / factory password settings or any other configuration that poses a threat to security. For example open FTP ports or broadcasting configuration information over the network.

Formal processes must be implemented to ensure that all applicable security patches are kept updated.

Methods and procedures must be implemented whereby network security issues are dealt with in a consistent manner. The results must be archived for future reference purposes.

5.3 Traffic Management

Network devices must be configured to prevent unauthorized access. The configuration(s) must be reviewed at least annually or after significant changes and health checked at least once every quarter. Unauthorized changes must be handled as a breach of security.

With the exception of pre-approved operational network sniffing or monitoring devices, no other network sniffing or monitoring devices may be installed / activated without the explicit authorization of the IT Manager.

Measures must be implemented to ensure the network filtering devices cannot be bypassed and can only be accessed from designated workstations or specified IP addresses via authorized secure channels (for example SSL).

Divulgence / broadcast of information about the network must be restricted to the absolute minimum.

Traffic flowing over the network must be afforded the same protection / security characteristics as when stored in accordance with the classifications of the information.

5.4 Network Operations

Service levels between service providers and the Municipality must be agreed to and continuously and formally monitored to ensure an acceptable level of service. All unusual entries / activities must be investigated and reported to appropriate line management for corrective action.

Pre authorized intrusion detection mechanisms should be employed as protection against possible attacks (depending of budget and availability of technical skills) .

Effective incident response, business continuity and disaster recovery planning processes must be implemented.

Network changes must be documented, formally accepted by the network owner and follow an accepted IT change management policy and standard.

Physical access to network devices must be restricted to authorized personnel. Service providers and / or contractors with no service record / history, must remain under constant observation when allowed access to restricted areas.

To reduce the risk of data in transit being intercepted, special care must be taken to protect network cables from tampering or disruption.

Back-up versions of essential network information and software (including communications software and utilities, network control tables / settings, configuration diagrams and inventories and device configurations) must be taken at such intervals required for the continued availability of the network. The back-ups should be protected from loss, damage and unauthorized access by storage in a fireproof safe on-site and copies off-site.

Remote maintenance must be controlled by restricting access rights and logging all activity. Diagnostic ports on network equipment must be protected by access controls.

Access to network devices that are primarily used for security services must be approved by the Manager for Secure Services. Access to any other network devices must be regulated via a formal process to request and authorize access. Record must be kept regarding the authorized access and a process implemented to ensure the timeous revocation of redundant access. The controls must be in the form of formal and traceable processes.

Internal or external remote maintenance sessions to devices that form the security barrier (the security objects used for protection) may not be allowed unless protected / controlled through a secure channel (e.g. SSL for Telnet)

No modems may be connected to the network without the prior approval of the applicant's Manager and the Manager responsible for IT security. A register of all approved modems must be maintained by the IT Department.

No user may simultaneously be connected to another network by using a modem while still connected to the Municipality's network.

5.5 **Risk Management**

A formal risk analysis must be carried out at least annually for networks that support critical business applications. The results of risk analysis must include a clear indication of key risks, an assessment of their potential business impact and recommendations for the actions required to reduce risk to an acceptable level.

The security status of the network must be subject to thorough, independent and regular security audit / review. Agreed recommendations from security audits / reviews should be implemented and reported to top management.

With the exception of Internal Audit, no unauthorized or clandestine audit or risk analysis may be conducted without the prior approval of the network owner.

A risk analysis must be done and the results formally considered before the implementation of technology that could negatively affect the security of the network. (The introduction of wireless networks serves as an example).

A process must be implemented to ensure compliance with new or existing local and international statutory requirements.

6. Reporting

Unless specifically and formally approved by the IT Manager, any deviation from this Policy is strictly prohibited.

7. Summary of main responsibilities

Following is a summary of the main responsibilities as derived from the policy document:

Responsibility	Owner			
	IT Manager	Network Administrator	Managers of other Municipal Departments	Human Resources
Formulate Network Strategy	✓			
Implementation of Policy	✓	✓	✓	✓
Awareness	✓		✓	
Policy Update / Revision	✓	✓		
Compliance Monitoring	✓	✓	✓	
Monitor Reports	✓	✓		

Responsibility	Owner			
	IT Manager	Network Administrator	Managers of other Municipal Departments	Human Resources
Management Information	✓	✓		
Reporting of Security Incidents	✓	✓	✓	✓
Formulation of Operational Processes	✓	✓		
Formulation of Technical Network Standards	✓	✓		
Risk Analysis	✓	✓		
Centralised Access Control	✓			
Network Inventory	✓	✓		
Network Security Device Management	✓	✓		
Approval of Third Party Connections	✓			
Network Contingency Planning (including disaster recovery)	✓	✓		
Compliance reviews from a management perspective	✓		✓	
Independent ad hoc review	✓	✓		

8. **Disciplinary Code of Practice**

The Municipality views the implementation of this Policy in a serious light and will not hesitate to act against violators. Non-compliance to this Policy is grounds for disciplinary actions up to and including summary dismissal.

INTERNET, INTRANET, EXTRANET AND E-MAIL POLICY

1. **Preamble**

The growth of the Internet and E-Mail as primary communications channel is increasing every year. The Internet and E-Mail provides access to information and services that would previously been very difficult to obtain. In addition, National and Provincial Government are encouraging the use of the Internet as a means to improve the accessibility of government services to all.

By providing organisations and employees access to the Internet and E-Mail in the normal course of their daily duties increases the risks faced by organisations on multiple levels. The security of the Municipal systems and information must be ensured at all times. The Internet greatly increases the risk of security breaches, theft of confidential information and incidental or unintentional discloser of confidential information, which can result in legal proceedings by the aggrieved party.

Furthermore, in a similar way that the telephone improved communications, but was also subject to wide spread abuse by employees, so to can the Internet and E-Mail be subjected to abuse. The cost of which must be borne by the Municipality in terms of cost and loss of productivity. The intention of an E-Mail Policy is to provide guidelines for the use of the electronic media and where abuse occurs, sets out the punitive measures that can be taken against an employee. The Internet and E-Mail Policy also controls the content that can be accessed over the Internet and prohibits the transmission of harassing and sexually explicit material.

The Internet and E-Mail Policy also specifies the security measures and safeguards that should be applied by the IT Department and the employee alike.

2. General Definitions and Meaning of Terms

The term “Municipality” includes the ***KOUGA*** Municipality with all its Departments.

The group term “Internet” includes Internet, Extranet, Intranet and E-Mail services. Where a specific word, such as E-Mail, is used it is for clarification and does not necessarily exclude the others of the grouping.

3. Policy Objectives

This Policy shall:

(i) Indicate the Municipality's requirements and standards regarding the implementation, usage, management and administration of Internet access.

(ii) Demarcate the roles and responsibilities of participating organisational Units.

(iii) Promote awareness among Municipality Internet users regarding the procedures, costs and risks involved in accessing the Internet.

(iv) State the Municipality's position in the event of non-compliance with the Internet Policy by any Municipality Internet user.

(v) Define guidelines, standards and procedures for the Municipality divisions providing information or services on the Internet.

4. Scope of Policy

The scope of this Policy shall be bound by the controlled and secure usage of the Municipality’s infrastructure and supplied Internet channels by the Municipality and its clients and shall include:

4.1 Internet

The Municipality Internet shall be used as another delivery channel to offer communication and information to Municipality constituents and potential constituents and, work related World Wide Web (www) access for Municipality employees.

4.2 Intranet

The Municipality Intranet is devoted to the Municipality’s Departments and/or business units to make internal communication more efficient and effective.

4.3 **Extranet (Specialised direct links)**

The Municipality Extranet, or extended Internet, shall be used by the Municipality to form a tight electronic communications channel relationship with its government structures or the private sector in the case of e-procurement and e-governance.

4.4 **E-mail**

The Municipality supplied E-Mail service is to make both external and internal work related communication more efficient and effective. Both internal and externally based browser (for example “Hotmail.com”) and client (for example “Microsoft Outlook”) E-Mail shall, if accessed by using Municipality’s infrastructure and supplied Internet channels, be deemed to be governed by this Policy.

5. **Ownership**

KOUGA Municipality Council is the owner of the policy.

KOUGA Municipality Information Technology (IT), or the Department responsible for IT, will execute and coordinate the maintenance of the Policy in consultation with relevant parties as mandated by Council from time to time.

6. **Approval**

Council shall approve this Policy on recommendation by IT, the IT Steering Committee (ITSC) and Human Resources (HR).

7. **Review**

The Policy must be reviewed at least annually. Any proposed interim alterations must be tabled via the Municipality IT Steering Committee (ITSC) for consideration and recommendation to Council.

8. **Implementation**

The Management of the Municipality are responsible for the implementation of the Policy in their own Departments. IT and HR will facilitate and co-ordinate the implementation thereof.

The Management of the Municipality as indicated below are responsible for drafting strategies, sub-policies and standards in support of this Policy.

Legal Department: Legal Guidelines/standards.

IT: Hardware/software architecture and standards for Internet access, request for Internet access procedures and the processing thereof, Internet Information protection, Security standards and infrastructure Charge-Out Procedures (if applied and implemented).

Any sub-policies/addendums must be derived from Municipalities policies and be in support of the Municipality's overall Internet philosophy. Such Sub-policies/addendums must be approved by Council, even though these additional documents may seem to conform to the Municipality's Policy.

9. Role Players

The major role players in the ***KOUGA*** Municipality Internet channels are:

KOUGA Municipality Information Technology Steering Committee (ITSC).

KOUGA Municipality Information Technology (IT) Management.

KOUGA Municipality Human Resources (HR).

The responsibilities of each role player in the total risk management process of ***KOUGA*** Municipality's Internet channels shall be:

9.1 Information Technology Steering Committee (ITSC)

Ensure that a ***KOUGA*** Municipality IT Policy exists.

To review the IT Policy.

To recommend the Policy to Council.

To obtain the approval of Council on the Policy.

9.1 Information Technology (IT) Management

To ensure adequate and cost effective management and control structures exist for the proper use of the Municipality's IT Services.

To compile and implement policies and procedures to effectively manage risks regarding the Internet.

To comply with their assigned responsibilities as contained in the IT Policy.

9.3 Human Resources (HR)

To assist with the implementation of the Policy.

To implement , where necessary, disciplinary actions as defined in the Policy.

10. **Policy Statements**

The following constitutes the core of the Internet/Extranet/Intranet Policy and will be supported by specific, detailed explanatory standards and/or procedures as defined by Policy role players.

The Internet resources provided in the work place at all times remains the property of the Municipality.

The resources so provided are intended to be used specifically for the employee's work and/or work related activities.

Incidental personal use is permissible so long as:

(a) it does not consume more than a trivial amount of resources,

(b) does not interfere with worker productivity,

(c) does not pre-empt any business activity and

(d) does not exclude the intent of this Policy.

The Municipality reserves the right to read any electronic mail message and attachment if it believes the situation warrants it. The employee should have no expectation of privacy in relation to information transmitted and/or stored on a Municipality provided resource. By signing the Internet/E-Mail Application form the employee waivers any right to invoke the provisions of the Interception and Monitoring Prohibition Act 127 of 1992.

10.1 **Unacceptable uses of the Internet and Kouga Municipality E-mail**

The Municipality's E-Mail and Internet access may not be used for transmitting, retrieving or storage of any communications of a discriminatory or harassing nature or materials that are obscene or X-rated. Sending of racially or sexually harassing message/files is also prohibited. No abusive, profane or offensive language is to be transmitted through the

Municipality's E-Mail or Internet system (including any messaging system such as Instant Messenger or any other messenger systems).

Electronic media may not be used for any other purpose that is illegal or against the Municipality Policy or contrary to the Municipality's best interest. Solicitation of non-Municipality business or any use of Municipality E-Mail or Internet for personal gain is prohibited. The use of E-Mail to participate in political activities, solicit political support or propagate political views is prohibited

Copyrighted material belonging to entities other than the Municipality, may not be transmitted by employees on the Municipality's E-Mail/Internet system. All employees obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with written permission of the copyright holder, or as a single copy for reference/back-up purposes only.

10.2 **Acceptable uses of the Internet and E-mail**

Every staff member has a responsibility to maintain and enhance the Municipality's public image and, to use E-Mail and access to the Internet in a responsible manner (Net etiquette).

Internet access is provided for business use only. Internet users have a responsibility to use the Internet appropriately in conducting the Municipalities business.

Each employee is responsible for the content of all text, audio or images that they place or send over the company's E-Mail/Internet system. No E-Mail or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else or someone from another company or Municipality. All messages communicated on the Municipality's E-Mail/Internet system must contain the employee's name.

Any messages or information sent by an employee to another individual outside of the company via an electronic network (e.g. bulletin board, online server or Internet) are statements that reflect on the Municipality.

All out-going E-Mail will have the ***KOUGA*** Municipality standard "disclaimer" attached (See Annexure A)

All Municipality employees are accountable, for the expression of personal or Municipal opinions on the Internet and specifically on news groups.

10.3 **Architecture and Infrastructure**

The Municipality connections to the Internet shall conform to the prevailing Technology Architecture of the Municipality.

IT, representing the Municipality, shall enter into an agreement with an accredited external Internet Service Provider (ISP), or multiple Internet Service Providers if it is in the Municipality's best interest, for access to the Internet. These agreements shall be the only official Municipality approved Internet connection. No other Municipality Department may negotiate its own separate Internet access.

Only IT are allowed to negotiate Web-hosting services. All Municipality's Internet pages will be hosted at a central Web-hosting server supporting the necessary system redundancy, security, and service level agreements.

10.4 **Adherence**

All the Municipality's information and services on the Internet must adhere to the strategy, standards and procedures as described in this policy namely; Internet Design, implementation and presentation standards; Hardware/software standards for Internet access; Request for Internet/Intranet access procedure; Legal guidelines and standards; Internet outsourcing standards; Internet Information Protection security standards; Charge-out procedures; Inter/Intranet Infrastructure Collaborative Web strategy; and Internet/Intranet/Extranet strategies.

Failure to comply with the Municipality's Internet/Intranet/Extranet Policy or any of its directives and standards will result in disciplinary action being taken .

The Municipality reserves the right to cancel/remove any user's Internet access rights and/or application if this can be shown to be in the best interests of the Municipality.

The Municipality reserves the right to "block" access to any category or individual Internet site that can be shown as not to be in the best or business interests of the Municipality.

All material on the Municipality's Internet site must not violate, plagiarise or infringe upon the right of any third party, including copyright, trademark or proprietary rights.

10.5 **Security**

Internet users should at all times adhere to the current Internet security practices within the Municipality when sending confidential or mission critical information across the Internet.

The Municipality reserves the right to monitor any employees Internet/Intranet communications and usage. All messages created, sent, or retrieved over the Municipality's E-Mail/Internet are the property of the Municipality and will be considered company information. Employees should not assume electronic communications are totally private and should transmit highly confidential data in other ways. However, to protect employee's privacy, no one will be allowed to access the system to read other mail without prior approval from the Municipality's ITSC. This will provide some assurance that there won't be rampant review of E-Mail.

The provision of security is important and all services and information provided on the Internet will comply with the latest Municipality Internet security standard regarding: authentication, non-repudiation (of origin and receipt) and data integrity and data privacy. The IT Department must approve all Municipality Internet application security issues prior to implementation.

10.6 **Outsourcing**

Approval of Internet content development outsourcing will depend on the following:

KOUGA Municipality Direct approval for:

Alignment with the Municipality's Internet strategy;

Constituent relationship and support functions in compliance with the Municipality Internet Customer Care policies;

Compliance to the Municipality Internet standards and procedures.

Ensure compliance to the Municipality's Application Standards for Internet development and Internet web server hosting.

KOUGA Municipality Technical Support approval for:

Type of service to be outsourced and its future integration with the Municipality's Internet technical infrastructure;

Ensure compliance with the Municipality's Internet Information Protection and Security standards.

KOUGA Municipality Technical Strategy and Architecture approval for:

Ensuring compliance with the Municipality's Technical Hardware and Software strategy and architecture.

The transferring of ownership and responsibility of the Municipality Internet information and/or services will not be allowed when outsourcing Internet development. All Municipality Internet information will reside within the Municipality premises to ensure efficient management and control of it. Fragmentation and duplication of the Municipality's information and/or services at external outsourced vendors will not be allowed.

11. Violations and Penalties

Any employee who abuses the privilege of Municipality facilitated access to E-Mail or the Internet will be subject to disciplinary action, which may result in dismissal. If necessary, the Municipality reserves the right to advise appropriate legal officers of any illegal violations.

The following general guidelines may be used for the purposes of disciplinary action against employees who breach this policy:

Offence / Category	**1st Offence**	**2nd Offence**	**3rd Offence**	**4th Offence**
Loading illegal software or offensive, disruptive, insulting or immoral material, such as pornographic material, onto a Municipality owned computer.	Final Written Warning/ Dismissal	Dismissal		
Sending external messages without the Municipality's standard	Written Warning	Final Written Warning	Dismissal	

disclaimer attached.				
Accessing pornographic, offensive, immoral, insulting, disruptive or discriminatory material.	Final Written Warning/ Dismissal	Dismissal		
Changing the configuration of any Internet server, Server or PC without proper authorization.	Written Warning	Final Written Warning	Dismissal	
Using Municipality Internet resources for personal gain.	As per the Municipality's disciplinary code on conducting unauthorized private business.			
Excessive browsing on the internet where it is clear that the sites visited are not work related or in any way linked to the services provided by the Municipality.	Written Warning	Final Written Warning	Dismissal	
Browsing on the internet where such browsing leads to deterioration in the employee's performance and quality of work.	Written Warning	Final Written Warning	Dismissal	
Disclosure of Security ID's and passwords to any other person, including non-staff members.	Final Written Warning	Dismissal		

Willfully downloading and/or opening of virus-infected files.	Final Written Warning	Dismissal		
Transmitting of copyrighted materials without authority of the copyright holder.	Final Written Warning / Dismissal	Dismissal		
Disseminating pornographic, offensive, immoral, insulting, disruptive or discriminatory material.	Final Written Warning / Dismissal	Dismissal		
Transmitting or forwarding of chain letters via the E-Mail system (including power point slides, Flash files or any other similar formats)	Written Warning	Final Written Warning	Dismissal	
Accessing information available on Internet servers for which you are not authorized.	Final Written Warning	Dismissal		
Sending external messages containing personal opinions and/or statements which may be deemed to be the Municipality's opinion.	Final Written Warning	Dismissal		

12. Electronic Mail Security

12.1 Municipal Property

As a productivity enhancement tool, the Municipality encourages the legitimate organizational use of electronic communications. Electronic communications systems, and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of the Municipality.

12.2 Authorized Usage

The Municipality electronic communications systems generally must be used only for Municipal related activities. Incidental personal use is permissible so long as:

(a) It does not consume more than a trivial amount of resources,

(b) Does not interfere with worker productivity, and

(c) Does not pre-empt any Municipal business activity.

Users are forbidden from using the Municipality electronic communication systems for charitable endeavours, private business activities, or amusement/entertainment purposes.

Employees are reminded that the use of Municipal resources, including electronic communications, should never create either the appearance or the reality of inappropriate use. Access to private E-Mail accounts is prohibited as it is a source of security risk. Private internet banking is permissible where individuals have already been granted access to the internet in terms of work requirements, providing the above rules are applied.

12.3 Default Privileges

Employee privileges on electronic communication systems must be assigned such that only those capabilities necessary to perform a job are granted. This approach is widely known as the concept of “least privilege”. Broadcast facilities (such as an “everyone” or “send to all” E-Mail) must be used only after the permission of a Department Manager has been obtained and should be distributed by the IT Network Administrator.

12.4 User Separation

Personal user-Id's and associated passwords must be used to identify and authenticate different users and to isolate the communications of different users. Fax machines that do not have separate mailboxes for different recipients need not support such user separation.

12.4.1 User Accountability

Regardless of the circumstances, the Policies that apply to id's and passwords in the Municipality should also be applied to access of E-Mail. Ignoring these exposes the authorized user to responsibility for actions the other party takes with the password. If users need to share computer resident data, they should utilize message forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms.

12.5 User Identity

Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with electronic messages or postings must reflect the actual originator of the messages or postings.

12.6 No Default Protection

Employees are reminded that the Municipality Electronic Communications Systems are not encrypted by default. If sensitive information must be sent by electronic communication systems, encryption or similar technologies to protect the data must be employed. Assistance can be obtained from the Information Technology Department.

12.7 Respecting Privacy Rights

Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. The Municipality is committed to respecting the rights of its employees, including their reasonable expectation of privacy. The Municipality also is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

12.8 **No guaranteed message privacy**

The Municipality can however not guarantee that electronic communications will be private. Employees should be aware that electronic communications, depending on the technology, can be forwarded, intercepted, printed, and stored by others. Furthermore, electronic communications can be accessed by others in accordance with this policy.

12.9 **Regular message monitoring**

It is the policy of the Municipality NOT to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that the Municipality will and may from time to time examine the content of electronic communications.

12.10 **Statistical Data**

Consistent with generally accepted practice, the Municipality collects statistical data about electronic communications. Using such information, technical support personnel can monitor the use of electronic communications to ensure the ongoing availability and reliability of these systems.

12.11 **Incidental Disclosure**

It may be necessary for technical support personnel to review the content of an individual employee's communications during the course of problem resolution. Technical support personnel may not review the content of an individual employee's communications out of personal curiosity or at the request of individuals who have not gone through proper approval channels.

12.12 **Contents of messages**

Workers must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, competitors, or others. Such remarks -- even when made in jest -- may create legal problems such as trade libel and defamation of character. Special caution is warranted because back-up and archival copies of electronic mail may actually be more permanent and more readily accessed than traditional paper communications.

12.13 **Message Forwarding**

Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. Sensitive information must not be forwarded to any party outside the Municipality without the prior approval of a Department Manager. Blanket forwarding of messages to parties outside the Municipality is prohibited unless the prior permission of a Department Manager has been obtained and should then be distributed by the IT Network Administrator.

12.14 **Handling information about Security**

Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to the IT Department. Users are prohibited from utilizing the Municipality's systems to forward such information to other users, whether the other users are internal or external to the Municipality.

12.15 **Public Representations**

No media advertisement, Internet home page, electronic bulletin board posting, electronic mail message, voice mail message, or any other public representation about the Municipality may be issued unless it has first gone through the appropriate approval channels. Permission must be granted by the appropriate Department Manager, and should then be issued by the IT Network Administrator.

12.6 **User back-up**

If an electronic mail message contains information relevant to the completion of a transaction, contains potentially important reference information, or has value as evidence of a Municipality Management decision, it should be retained for future reference. Most electronic mail messages will not fall into these categories, and accordingly can be erased after receipt. Users must regularly move important information from electronic mail message files to word processing documents, databases, and other files. Electronic mail systems are not intended for the archival storage of important information. Important stored electronic mail messages can be periodically expunged by systems administrators, mistakenly erased by users, and otherwise lost when system problems occur.

12.17 **Archival Storage**

All official Municipality electronic mail messages, including those containing a formal management approval, authorization, delegation, or handing over of responsibility, or similar transaction, must be archived.

12.18 **Purging electronic messages**

Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. After a certain period -- generally six months -- electronic messages stored on multi-user systems will be automatically deleted by systems administration staff. Not only will this increase scarce storage space, it will also simplify records management and related activities.

12.19 **Harassing or offensive materials**

The Municipality computer and communications systems are not intended to be used for, and must not be used for the exercise of the workers' right to free speech. Sexual, ethnic, and racial harassment --including unwanted telephone calls, electronic mail, and internal mail -- is strictly prohibited and is cause for disciplinary action. Workers are encouraged to respond directly to the originator of offensive electronic mail messages, telephone calls, and/or other communications.

If the originator does not promptly stop sending offensive messages, workers must report the communications to their Manager and the Human Resources Department. The Municipality retains the right to remove from its information systems any material it views as offensive or potentially illegal.

12.20 **Access to Internet e-mail**

Internet based electronic mail may only be accessed via the internet E-Mail servers provided by the Municipality when the target computer is linked to the Municipality Network. Users are not allowed to e.g. dial out to service providers in order to access E-Mail. Downloading of private E-Mail from external mail accounts (e.g. Hotmail, Yahoo, MSN, etc) is prohibited.

12.21 **Virus scan of e-mail**

All inbound and outbound electronic mail must be scanned for viruses before delivery. The scanning should include attachments zipped or otherwise. The exception would be encrypted E-Mail. Specific policies relating to encrypted mail apply in this case.

13. **Standard E-mail disclaimer**

The disclaimer is presented at footer of the E-Mail and is normally created as a default text that is automatically applied when a new E-Mail is created. This is normally set up as a stationery element in the E-Mail client configuration. It is the responsibility of the IT Department to ensure that the disclaimer is automatically configured on the user's computer or E-Mail client.

The purpose of the disclaimer is to protect the Municipality from litigation arising from the accidental discloser of information to an unintended third party, from damage to a third party's computer system resulting from a computer virus or any other harmful program hidden in or embedded into an E-Mail or attachment to an E-Mail.

The E-Mail footer, in addition to the disclaimer, should contain the organisation from which the E-Mail is being transmitted, the E-Mailer's name and contact information. This is required so that any individual receiving an E-Mail in error can notify the originator and destroy the E-Mail without any copies of the mail being retained.

ANNEXURE A

KOUGA MUNICIPALITY E-MAIL DISCLAIMER

E-Mail sent by the Kouga Municipality is to be treated as confidential, and the information in it may not be used or disclosed except for the purpose for which it has been sent. If you have reason to believe that you are not the intended recipient of this communication, please contact the sender immediately. Please then delete the message and do not disclose its contents to any person. Neither the sender nor Kouga Municipality accepts any liability whatsoever as a result of the further dissemination of this message. Whilst all reasonable steps are taken to avoid corruption of data or information, we do not accept any liability should such corruption occur. No employee or agent is authorized to conclude any binding agreement on behalf of the Kouga Municipality with another party by E-Mail without express written confirmation by the Kouga Municipality.

ANNEXURE B

ACCEPTANCE OF CONDITIONS OF POLICY

I hereby acknowledge that I have read the terms and agreements stated in the Policy. If I do not comply to this Policy I acknowledge that I will be subject to disciplinary action as stated above.

…… **EMPLOYEE NUMBER**

…… **FULL NAME & SURNAME**

……**DEPARTMENT**

……**SECTION**

…… **SIGNATURE**

……**WITNESS SIGNATURE**

Signed at ……on this ……day of……20…….

ANNEXURE C

COMPLIANCE AGREEMENT

AGREEMENT TO COMPLY WITH INFORMATION SECURITY POLICIES

User's Clearly Printed Name: _____

E-Mail Address :_____@kouga.gov.za Employee No: _____

Department: _____ Job Title: _____

User's Telephone Number (Including Extension): _____

User's Office Physical Address:

_____

User's IP Address: _____

I, the user, agree to take all reasonable precautions to assure that the Municipality's internal information, or information which has been entrusted to the Municipality's by third parties (such as customers), will not be disclosed to unauthorized persons.

I understand that I am not authorized to use this 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 agree to return to the Municipality all information to which I have had access as a result of my position with the Municipality on termination of my employment or contract with the Municipality.

I have access to copies of the Municipality's IT Policies, I have read and understand the contents of the Policy, and I understand how it impacts my position in the Municipality.
As a condition of continued employment at the Municipality, I agree to abide by these information security policies. I understand that non-compliance will be cause for disciplinary action up to and including system privilege revocation, dismissal from the Municipality, and perhaps criminal and/or civil penalties.

I agree to choose a difficult-to-guess password as described in the Municipality's Information

Security Password Standards document as discussed in this Policy. I agree not to share this password with any other person, and I agree not to write this password down unless it has been transformed in an unrecognizable way.

I will ensure that only legal and licensed software is installed on the computer and accept that the Municipality cannot be held liable for any violations due to my actions.

I also agree to promptly report all violations or suspected violations of information security policies to the Manager of IT and my direct Manager.

I agree that the terms and conditions of this Compliance Agreement are both reasonable and necessary for the protection of the Municipality's internal information, or information which has been entrusted to the Municipality by third parties.

User Signature:_____ User's Manager: _____

Date:_____ Date:_____

DOCUMENT CONTROL SHEET

KOUGA MUNICIPALITY

IT POLICY

Document Title:	**KOUGA Municipality Information Technology (IT) Policy**			
Department/Section Finance Department /Information Technology(IT)		**Documnt Number**	**Revision** 1	**Issue Date** 2008-09-10
APPROVAL	**Name**	**Job Title/ Role**	**Signature**	**Date**
Approved by				

Originally Compiled by	**:**	**Council**
Directorate	**:**	**Finance**
Department	**:**	**Finance**
Section	**:**	**Information Technology (IT)**
Date	**:**	**<10 September 2008>**
Version number	**:**	**1**
Reviewed by	**:**	**Council**
Date of last review	**:**	**26 June 2012**
Document reference	**:**	