RUSTENBURG LOCAL MUNICIPALITY

INFORMATION & COMMUNICATIONS TECHNOLOGY POLICY

TABLE OF CONTENTS

PREAMBLE

Information and Communications Technology has proved to be of tremendous importance to Information Management and is of considerable business value to the municipality. However due to lack of proper regulations on the use of technology, several risks are involved particularly those that are likely to endanger the integrity of the municipality.

The absence of clear guidelines with regards to the use of information and communication Technology equipment and resources has resulted in maintenance problems, information management problems and lack of control in terms of the activities of users of ICT equipment and resources.

The latter has prompted the RLM to develop policies with clear guidelines in terms of the dos and the don'ts for employees of the municipality who are making use of ICT equipment and resources while executing their duties. It is envisaged that the development of guidelines will also assist to educate users on various ICT issues.

DEFINITIONS

Chain email or letter Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

Council refers to the council of Rustenburg Local Municipality

Email The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.

Employee or Official means a permanent, temporary, part-time or contract employee, intern, in service trainee, learner participating in a learnership but excluding an independent contractor and a student.

Forwarded Email is an Email resent from an internal network to an outside point.

Private Call refers to use of official telephone for personal benefit.

Sensitive information is considered sensitive if it can be damaging to RLM or its customers' reputation or market standing.

Unauthorized Disclosure the intentional or unintentional revealing of restricted information to people, both inside and outside RLM, who do not have a need to know that information.

Unauthorized Person means people who are not employees of council.

Virus warning. Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.

EXPLANATION OF ABBREVIATIONS

AD: Active Directory

CI: Configuration Item

CIO: Chief Information officer

CMDB: Configuration Management Data Base

FTP: File Transfer Protocol

HVAC: Heating Ventilation and Air Conditioning

IMAC: Install, Move, Add, Change

ICT: Information Communications Technology

ICTSC: ICT Steering Committee

ISMS: Information Security Management System

IT: Information Technology

ITIL: Information Technology Infrastructure Library

ISGS: Information Security Governance System

ISIRT: Information Security Incident Response Team

ISO: Information Security officer

LAN: Local Area Network

NDA: Non-Disclosure Agreement

PDA: Personal Digital Assistant

QA: Quality Assurance

RBAC: Role Based Access Control

RFC: Request for change

RLM: Rustenburg Local Municipality

SDLC: System Development Lifecycle

SLA: Service Level Agreement

WAR: work Area Recovery

PURPOSE AND AIM

The ICT Policies document sets out principles and standards which determine acceptable use of the Information Communications Technology equipment of the RLM. It is the intent of these ICT policies to establish guidelines for all employees and Councillors using RLM's ICT equipment and resources.

The main aim of this ICT policies document is to balance the proper use of computing resources against the need for protection of the systems.

These policies also apply to all users, whether on municipal property, connected via remote connection or any networked connection.

SCOPE OF OPERATION

RLM disclaims any responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of those computing facilities or from system malfunction or any other cause.

These policies cover the usage of all RLM's Information Communication and Technology resources, including but not limited to:

- All computer-related equipment, including personal computers, portable computers, Personal Digital Assistants, workstations, terminals, wireless computing devices, databases, networks, telecommunication equipment, servers, shared computers, printers and all networks and hardware to which this equipment is linked.

- All data stored on municipal equipment

- All software including purchased or licensed business software applications and any other software residing on municipal-owned equipment.

- Confidentiality- to ensure that only people who are authorized to have access to information are able to do so.

- Keeping valuable information only in the hands of those people who are intended to see it.

- Integrity – to maintain the value and the state of information, which means that it is protected from unauthorized modification

It is the responsibility of all the Authorities in the council and their operating units to ensure that these policies are clearly understood, communicated and followed.

APPLICATION

This policy is applicable to:

- All RLM councillors, employees, contractors and agents who act on behalf of the RLM or are in its
- employment and are End Users of the RLM internal IT Systems and Infrastructure;
- All Business Units and Departments within the RLM as well as its affiliated entities of which the RLM has management control;
- All System Administrators appointed with administration responsibilities that are directly or indirectly governed by the specification contained in this policy.
- Process Owner;
- Change Manager;
- Change Coordinator;
- Process Coordinators;
- Process Executor: Technicians and Specialists;
- IT Service Delivery Manager; and
- Project Manager
- All RLM representatives, including employees and contractors;
- Any representatives of service providers given access to information owned by or entrusted to RLM, or information systems owned by or managed on behalf of RLM; or
- Any other party governed by RLM's Information Security Management System (ISMS), such as through formal agreement or contractual obligation, and unto which this policy would apply

CHAPTER1: PASSWORD POLICY

1.1 PURPOSE

The internal IT Systems and Infrastructure are important assets to the business and disruption of their operation can have a negative impact on our business and clients. The order of the impact and the likelihood of the event, constitute a so-called IT security risk. These risks can be mitigated or reduced by proactively instituting policies whereby the likelihood of occurrence and the order of impact is reduced to acceptable levels.

The IT Assets have been classified according the main IT architecture components and subcomponents. A list of potential and relevant security threats has been compiled and the likelihood of each determined. The Password mismanagement is a potential security threat. The process as defined in this policy document should be used as the de facto standard.

1.2 POLICY OBJECTIVES

The objectives of the RLM Password Policy are:

(a) Mitigation of risks associated with Password mismanagement;

(b) Enforce password standards; and

(c) Enforce a Password change procedure.

1.3 POLICY STATEMENT

User-id and password

a) Access to all IT Systems and Infrastructure will be controlled by means of a user-id and password;
b) The owner of a user-id and/or password is fully responsible to ensure that no other person can make use of it to access the IT Systems and Infrastructure;
c) All user-id's and passwords shall be treated as Confidential and Organization sensitive information.

d) All vendor supplied default or generic user-id's must be removed, renamed, disabled and/or passwords changed;
e) End User accounts will be de-activated after a maximum of five (5) consecutive unsuccessful attempts to enter a password. This account will stay inactive for 30 minutes, or until a System Administrator has re-activated the account;
f) It is mandatory that screen saver passwords be activated on PC's. Following no activity on a PC for a maximum of ten (10) minutes, the screen saver password must be automatically invoked. For terminals, the system must automatically blank the screen and suspend the session after 10 minutes; wherever possible, applications should automatically invoke a session timeout after 10 minutes of inactivity. Re-establishment of the session must take place only after the End-user has provided the proper password;
g) It is mandatory that all PC's connected to the network be logged out of the network regularly. It is recommended that this be done each day; A forced logout from the network will be implemented to occur once a week at an appropriate time;
h) All enterprise servers and network switching equipment must be password protected and where practically possible, adhere to all requirements stated in this policy.
i) Where applicable all systems shall have the "Remember Password" option disabled e.g. Internet Explorer websites.

1.4 PASSWORD STANDARDS

a) All passwords must have at least eight (8) characters;
b) Passwords should not be a word found in the dictionary or some other part of speech. For example, proper names, places, and slang should not be used;
c) Passwords should not contain other information easily obtained about you. For example, date of birth, license plate number, telephone number, ID number, make of your car, house address, etc.;
d) Passwords should not be all digits nor should the password contain more than two of the same letter consecutively;
e) Where the operating environment allows, passwords must contain a combination of at least three of following four classes:
    - English Lower Case Letters a, b, c, ...z;
    - Westernized Arabic Numerals 0, 1, 2,... 9;

- At least one special characters e.g. punctuation symbols ! ®,#$%A&*0+h-=":'<>?../
- Passwords should be easy for the End User to remember, but not easy for someone else to guess. For example, the phrase "It's always your duty to stay informed!" Might be the basis for a password such as Iayd2si! This password uses a mix of alphanumeric, and punctuation characters. A date could be added, e.g. January 2004 could be represented by 01-04, or even)! -)$ (By making use of the shift key);
- End Users must not construct passwords that are identical or substantially similar to passwords that they had previously used. IT Systems and Infrastructure should be configured so that End Users are not permitted to reuse at least the last 6 passwords.
- User accounts that have system-level privileges granted through memberships or programs such as SQL Administrator or AD Administrator must have a unique password from all other accounts held by that user.

1.5 PASSWORD STORAGE

The display and printing of passwords must be masked, suppressed, or otherwise obscured in such a way that unauthorized parties will not be able to observe or subsequently recover them.

a) Passwords must always be encrypted when transmitted over networks;
b) Passwords that need to be recorded on paper should be housed in a locked, secure environment. Passwords must not be written down and left in a place where unauthorized persons might discover for example: Never put your password on a sticky note on PC or your desk
c) When a user resigned or dismissed, a written letter from HR must be sent to the IT Department to disable the user account immediate so that all important emails and information can be save and sent to a relevant employee, so that the user account can be removed automatically from the server.'

1.6 PASSWORD CHANGES

a) All End Users should change their passwords at least once every thirty (30) days. This forced change should be automated wherever it is supported;

b) Passwords will expire every 30 days. If the password is not reset within 10 working days of expiry, the relevant account will be disabled. End Users will need to use Help Desk to re-enable this account.
c) When a password has been compromised, it should be changed immediately;
d) All password resets require the End Users to identify themselves to the help desk staff using up-to-date unique information in the organization directory.
e) Passwords shall not be disclosed to an end-user via e-mail, instant messaging, or any other form of electronic communication including verbally. It shall only be sent to the mobile number recorded on the Exchange Directory.
f) In the event of a user who does not have access to a mobile telephone, the user should physically identify himself or herself to a supervisor in the Help Desk by means of their ID document, where after the Help Desk Agent will verbally supply the user with a password.
g) A person may only request his or her own password be reset. End Users can register on the electronic password system to reset their own passwords on the Password Self-Service tool where applicable.
h) Reset passwords may not be a word found in the dictionary or some other part of speech for example, proper names, places, and slang. Administrators must use a Random Password Generator to compile the use once password.
i) The initial passwords issued by a System Administrator must be valid only for the concerned End User's first on-line session. The End User must be forced to choose another password before any other work can be done.

1.7 ROLES AND RESPONSIBILITIES

RLM employees, contractors and agents are responsible for the following:

(a) Ensuring their passwords are not compromised in any way;

(b) Their personal details are always up to date on all electronic systems such as ERP and AD, this can be done via a request to the helpdesk; and

(c) Take reasonable care in choosing their passwords.

1.8 SYSTEM ADMINISTRATORS

System Administrators are responsible for the following:

(a) Ensuring passwords are not compromised in any way;

(b) The Random Password Generator is used to reset password at all times; and

(c) No user is to receive any password by any means other than a SMS to the number recorded on the AD.

CHAPTER2: PHYSICAL ENVIRONMENTAL SECURITY POLICY

2.1 OBJECTIVES AND STANDARDS

a) Unless Otherwise specified, Physical security is the responsibility of the site's facilities manager

b) Appropriate physical security mechanisms must be in place at all building parameters. Access to areas where "Confidential" information is processed or stored, or where information systems containing such information are located, must additionally be protected through strict access control mechanism

c) All servers and networking equipment must be located in designated laboratory environments, Computer Equipment Rooms or lockable computer equipment Cabinets situated within access controlled areas.

d) Data Centres and Server Rooms must be protected against environmental threats. This includes having appropriate controls of the following nature in place: -
   - Fire Suppressant
   - Heating, ventilation and air conditioning (HVAC)
   - Power redundancy and backup
   - Video surveillance

e) Information asset owners must ensure that appropriate continuity and disaster recovery measures are in place for information systems, in line with the RLM Business Continuity Policy.

f) All information security policies, standards, processes and procedures apply to Business Continuity Sites (BCS) and Work Area Recovery (WAR) sites in the same way as for production sites.

g) Cabling and telecommunications equipment located both inside and outside building perimeters must be reasonably protected against damage or interception of information

h) Any equipment that is disposed of or to be re-used by external parties must have all information stored on it properly destroyed, in line with the RLM Asset Disposal Policy. Such equipment includes any equipment containing hard disks or solid state storage, including removable storage media, servers, laptops, workstations, PDAs, mobile phones, etc.

i) All documents containing “Confidential” information must be shredded before being disposed of or taken offsite for recycling or destruction.

j) Users are required to practice a clear desk policy, and ensure no sensitive information is left unattended in work areas.

k) The RLM Asset Removal Policy regulates the removal of equipment from buildings.

l) All individuals issued with mobile computing equipment must take reasonable steps towards ensuring the security of such equipment at all times.

CHAPTER3: CHANGE MANAGEMENT POLICY

3.1 OBJECTIVES AND STANDARDS

Change Management refers to the management of Change processes involving the following:

(a) Hardware infrastructure;

(b) Servers;

(c) Desktops;

(d) Laptops;

(e) PDAs;

(f) LAN communication equipment and software (switches, Cabling, network cards);

(g) System software;

(h) All documentation and procedures associated with the running, support and maintenance of live systems;

(i) All process improvements and related documentation;

(j) Changes to programs including bug fixing and patches;

(k) Maintenance of hardware and software; and

(l) IMAC Changes to the ICT environment: Installations, Moves, Adds, Change and Disposal ("IMACD") of any Configuration Item ("CI") to the physical environment, with the Configuration Management Data Base ("CMDB") reflecting the actual physical implementation at any point in time. It is classified as a pre---approved Change and handled as a Request from an approval perspective.

3.2 OUT OF SCOPE

The following items are out of the scope of this policy:

(a) Projects in the "development" phase until such time as they impact the ICT production environment;

(b) Changes to RLM clients' networks and systems where the infrastructure is shared with the client. Where Change control is prescribed by the client for their infrastructure, the RLM support personnel shall at all times adhere to the relevant Client's Change control procedure;

(c) Non---production ICT environments utilised within RLM and

(d) Non---group supported ICT environments.

The ICT infrastructure and applications in RLM are changing on a regular basis to meet changing business needs, effecting improvement or to do maintenance. The process of moving from one defined state to another is defined as "Change". Change Management ensures that uniform methods are in place and are used to manage the transition.

The goal of the ICT Change Management Policy is to ensure that standardised methods and procedures are used for efficient and prompt handling of all Changes, in order to minimise the impact of Change upon service quality and consequently to improve the day---to---day operations of our organisation.

Each requested Change should be investigated in terms of risks and potential business impact to enable the ICT Steering Committee to make appropriate approvals. It is particularly important that our Change Management processes have high visibility and open channels of communication in order to promote smooth transitions when Changes take place.

3.3 POLICY OBJECTIVES

The objectives of this policy are to:

a) Ensure that standardised methods and procedures are used for efficient and prompt handling of all ICT Changes;

b) Ensure proper governance and control over all ICT Changes within the scope of Change Management;

c) Assist in assessing risk and business continuity, Change impact, resource requirements and Change approval. This considered approach is essential to maintaining a proper balance between the need for Change against the impact of the Change;

d) Providing a formal method for updating and ensuring the integrity of the CMDB;

e) Accelerate delivery by using best practice techniques during the lifecycle of the Change process;

f) Provide a vehicle for evaluating the performance of implemented Changes;

g) Use applied standards to ensure quality, both in relation to the solution and the program processes used to create that solution;

h) Contribute to measure total solution quality, as well as the processes to ensure the achievement of the desired level of quality; and

Deliver business benefits such as cost reduction or service stability by preventing re---work or service outages.

3.4 POLICY STATEMENT

3.4.1 Change Management process

All the ICT Changes within the scope of this policy document need to follow the ITIL approved process as described in the approved Practice Manual. The process needs to include as a minimum the following process steps:

a) When identified, Changes in scope potentially affecting the ICT production environment are formally defined;

b) The defined Change is logged as a Request for Change in Remedy;

c) The Request for Change is approved for investigation by the Business Owner client;

d) Obtain approval from the ICTSC after consideration of the risk, impact, duration and cost of the Change;

e) Simulate the Change according to plan in the development/QA/laboratory environment;

f) Do full technical and user acceptance testing in the development/QA/laboratory environment;

g) Compile ICTSC documentation pack;

h) Obtain approval of ICTSC to transition Change into production environment;

i) The Change is planned and scheduled as a project;

j) Communicate Change to all affected personnel (client, internal, other vendors);

k) Implement the Change in the ICT production environment as per the pre---approved plan schedule;

l) Obtain signoff of successful operation of changed environment from the Change Owner; alternatively rollback to the previous state;

m) Handover operational support of changed environment to responsible support groups and communicate the success of the Change to the user community;

n) Effect all Changes to the CMDB, billing, responsibility matrix, SLA measurements and reporting; and

o) Close Change request, including project closure.

Controlling the Change Management process during the process of implementing a Change, several minimum "control points" shall be included in the plan to ensure the Change is successful in terms of minimal risk and disruption to the users of the ICT production environment. The minimum control points are listed below.

- Control Point 1: All Changes shall be logged in Remedy;

- Control point 2: After investigating the Change, the risk and impact shall be evaluated against the potential risk and impact of not doing the Change. Only if is business benefit to be gained, as measured against acceptable risk, should the Change proceed. The Project Manager is responsible to obtain sign--- off from all key stakeholders before the process can continue;

- Control point 3: Once the Change has been simulated in the development and QA environments, it shall be thoroughly tested by the key stakeholders. The Project Manager is responsible to obtain sign---off from all key stakeholders before the process can continue;

- Control point 4: Once the Change has been properly planned and tested, it is passed on to the ICTSC for evaluation and final scheduling;

- Control point 5: After implementation in the production environment, the Change is fully retested by the key stakeholders. On successful completion of this testing, the Change will be allowed to remain en--- force; and

- Control point 6: The CMDB is updated and reflects all Changes.

Change categories All Changes are categorised as either a Normal Change, an Emergency Change of a Standard Change. The principles applicable to the different types of Changes are as follows:

Normal Changes Planned Changes with enough lead time to be approved by a ICTSC and which follows the Change Management process.

3.4.2 Emergency Changes

The following principles apply to an Emergency Change:

a) All Emergency Change Requests shall be linked to a logged incident in Remedy;

b) An Emergency Change is only completed once it went through the same process of a Scheduled Change to ensure that the CMDB reflects the state of the entire environment after implementation and that the history of CI Changes can be traced; and

c) Emergency Changes shall be approved by at least two ICTSC members (as mentioned in 7.5b) telephonically, before the implementation of the Change. Communication of such approved Emergency change will be sent to the Service Desk, Command Centre and Change coordinator before implementation of the change. The Emergency change shall be logged formally on the system after implementation and a formal review of the Emergency change may be requested at the next ICTSC.

3.4.3 Standard Changes

Once---off approval is required for Standard Changes. Standard Changes are handled according to the Request Fulfilment Process of the Service Desk. A formal record is maintained in Remedy of all Changes classified as "Standard Changes".

Change Management Windows

The following time slots are available in the business context to implement Changes:

a) Change and Maintenance Window

The second and third weekend of the month between 19:00 on Friday evenings to 05:00 on Monday mornings.

b) Change Freeze Times

First and last weekend of the month

c) Lead Times

Changes has to be submitted to the ICTSC at latest, with all required documentation, before the Tuesday at 12:00 prior to the Change window selected for the implementation of the Change. All testing and risk assessments should be completed, documented and included when the requests are submitted to the ICTSC. Change Implementer and/or requester have to be present at the ICTSC session to obtain approval; non---attendance will result in a rejection of the Change as a default rule.

3.4.4 ICT Steering Committee

a) The ICT Steering Committee (ICTSC) is mandated to approve Changes and to govern the Change Management Process in the assessment and prioritisation of Changes.

b) The Information Management ICTSC members are as follows:

1. Chairperson appointed by the CIO;
2. Applications Manager;
3. Infrastructure Manager;
4. Service Delivery Manager; and
5. ICTSC Secretary.

c) Other members of the Change Control Board are as follows:

1. Change Manager;
2. Change Coordinator;
3. Change Requestors submitting Change Requests;
4. ICTSC Administrator;
5. Business Unit ICTSC Representatives; and
6. Process owner representative, when applicable.

d) The Change Approval Board is chaired by the Information Management Representative appointed by the CIO.

e) When major problems arise, there may not be sufficient time available to convene the full ICTSC, and it is therefore necessary to identify a smaller organisation with the authority to make emergency decisions. This body is known as the ICTSC Emergency Committee. The ICTSC Emergency Committee consist of the ICTSC Chairperson, relevant

Process owner and both the IT Applications and Infrastructure Managers

.

3.5 ROLES AND RESPONSIBILITIES

3.5.1 Process Owner

The Process Owner is responsible for the following:

a) The design, implementation, monitoring and improvement of the process;

b) Providing all the necessary mechanisms to enable process execution. This includes support structures, documentation, forums, reporting structure and governance; and

c) Has the authority to authorise system Changes effecting the business process or business rules.

3.5.2 Change Manager

The Change Manager is responsible for the following:

a) Orderly and effective co---ordination of ICT related Changes to the production environment;

b) Appoints other staff members to effect the Change, as he/she sees fit;

c) Communicates the result of the Change in production to the Change Approval Board;

d) Contributes to the Post Implementation Review session on major implementation; and

e) Total owner of the Change Management process.

3.5.3 Change Coordinator

The Change Coordinator is responsible for the following:

a) Coordinating and planning of the Change;

b) Determines if the Change can be added to a Change that was already prepared earlier. If this is the case, the Change should be linked to the existing Change in order to optimise efficiency;

c) Checks the request to ensure that it does not conflict with internal standards or policies. If this is the case, the Request for Change is rejected and the requester is informed of the internal standard or policy that the Request for Change conflicts with;

d) Reviews the risk and impact analysis in business language by gathering information from the related specialist(s);

e) If a new service infrastructure is to be built or if an existing service infrastructure is likely to be modified, requests the relevant approver to create a new service infrastructure design, or modify the existing service infrastructure design;

f) Checks the implementation plan and timing of the Change to minimise the risk, user impact and conflict with other Changes;

g) Obtain necessary approvals;

h) If the Change is rejected for another reason, notify the requester that the Change cannot be implemented;

i) If the Change is an infrastructure Change, assign the preparation task to the specialist in order to ensure operational readiness;

j) Opens a task for updating the CMDB;

k) Closes the Change in Remedy;

l) Drives the efficiency and effectiveness of the process, procedures and work instructions;

m) Schedules the ICTSC meeting;

n) Provides the ICTSC members with the Forward Schedule of Change before the ICTSC meeting;

o) Communicate cut---off date and time to all Change requestors;

p) Ensure that all approvers are in possession of all related documentation required to approve that Change; and

q) Maintain Change records and ensure effective communication.

r) Telephonically communicate insufficient Business representation of affected stakeholders on major changes during ICTSC meetings to Business Unit Executives

3.5.4 Change Requestor

The Change Requestor initiates the Change process by submitting a Request for Change (RFC) and providing assistance to the Change Coordinator as required.

3.5.5 ICTSC

The ICTSC is responsible for the following:

a) Has over-all responsibility for all Changes;

b) Approves final sign---off of the Change before interacting with Release Management to put the Change into production;

c) Takes notice of successful and unsuccessful approved Changes;

d) Is jointly with line Management responsible for deciding on the merits of the Change; and

e) Review implemented Changes and initiate improvement initiatives.

3.5.6 Business Approvers

The Business Approvers are responsible for the following:

a) Confirming the Change for completeness;

b) Confirming the schedule; and

c) Approve or decline the Change.

3.5.7 Process Executor

The Process Executor is responsible for the following:

a) Performs technical or business tasks as allocated by the Change Coordinator or Project Manager.

3.5.8 IT Service Delivery Manager

The IT Service Delivery Manager is responsible for the following:

a) Coordinate all Service Providers to deliver IT services in alignment with contracts and service levels;

b) Ensures availability, continuity, security and access to IT services are maintained; and

c) Measure IT service delivery and facilitate payment for IT services.

3.5.9 Change Owner

The Change Owner is responsible for the following:

a) Assess the scope, risk and impact of request for Changes;

b) Develop and present assessment results to the ICTSC;

c) Appoint Change Coordinator or Project Manager; and

d) Monitor progress and success of Change implementation.

3.6.1 Project Manager

A Project Manager is appointed by the ICTSC in the case where large Changes are to be implemented. The Project Manager is responsible for the following:

a) Plan, organise and control the execution of approved Changes; and

b) Manage the scope, resources, risk, issues and financial requirements in an integrated manner.

3.6.2 ICTSC Administrator

The ICTSC Administrator is responsible for the following:

a) Scheduling of the ICTSC meetings;

b) Receives and administers the Change Request, Change approvals, Change Rejections as well as relevant documentation;

c) Maintaining the records on Remedy on all Changes; and

d) Notifying all ICTSC members on relevant ICTSC meeting issues.

3.6.3 ICTSC Secretary

The ICTSC Secretary is responsible for the following:

a) Documenting meeting proceedings and decisions; and

b) Distributing the minutes of meetings.

CHAPTER4: IT SECURITY POLICY

4.1 OBJECTIVES

The objectives of the Information Security Policy are to: -

a) Clearly define the overarching information security principles and practices to be adhered to;
b) Ensure all relevant parties have access to a well described source of information security control requirements; and
c) Provide a measure of compliance to the minimum expected controls.

The policy statements contained within this document apply to: -

Information is a cornerstone of RLM's business, of which the confidentiality, integrity and availability supports the organization's activity and livelihood. The threats to RLM's information assets increase day by day, and require diligence towards ensuring the organization does not fall prey to the wide array of threats faced. As a public entity RLM has the duty of care in protecting information of its citizens.

Information may be exposed in many ways including through unauthorized or malicious access to fileservers and other servers, desktops, laptops, removable storage devices such as USB memory sticks, printed materials, emails, instant messaging chats, information stored on social networking sites and other internet locations, conversations in public places and many more.

Information that is important to RLM includes: intellectual property, any customer, partner or vendor information, internal financial information, information related to business strategy, mergers and acquisitions, human resource related information, proposals, correspondence containing personal, contractual or sensitive business information, and any information that may be of value to RLM or to an external party. This information is important to RLM for various reasons, and allows it to: -

- Maintain a trust relationship with its customers, partners and suppliers;
- Successful deliver services in a responsible and well governed manner;
- Better facilitate the strategic objective of becoming a world-class city

- Maintain and expand on the reputation of the RLM brand.
  Inappropriate information security controls are likely to detrimentally affect RLM's business, and may lead to: -

- Financial loss;
- Loss of reputation;
- Loss of productivity;
- Loss of privacy;
- Contravention of laws and regulations; and
- Legal liability.
  It is therefore RLM's duty as an organization to ensure its information assets are adequately protected, as it has a direct impact on RLM's business activity and livelihood.

  An Information Security Management System (ISMS) comprises of a set of information security policies, practice- and configuration standards, processes, procedures and supporting activities, such as awareness creation and training. It communicates the organization's expectations on how information security should be managed, and provides a mechanism according to which compliance and performance in this area can be measured.

  This document represents RLM's Information Security Policy, which forms the root of the policy tree in the larger Information Security Management System (ISMS), and governs all other information security policies that reside below it.

4.2 MISSION STATEMENT

RLM's Council intends to act responsibly and appropriately by ensuring a practical information security management strategy is defined, a compliance programmed is developed, implemented and maintained to appropriately manage risks to RLM's business, conform to generally accepted good practice and achieve compliance to all applicable regulatory and legislative requirements.

The information security management programmed must ensure RLM's information is available as and when the business requires it, its integrity is preserved and it is accessible only to those for whose consumption it is intended.

4.3 GOVERNANCE SYSTEM

The Information Security Governance System (ISGS) in place within RLM consists of the following: -

a) Information Security Management System (ISMS), representing a system that describes and dictates how information security should be managed within the organization, through relevant information security strategy, policies, standards, processes, procedures, and training and awareness, in order to ensure risks to information assets are properly managed;
b) Information Security Architecture (ISA), constituting a set of principles, design methods and guidelines, and structured and strategic target architecture designs to guide the selection and deployment of information security technology solutions in a way that would address business requirements in an optimized and secure fashion; and
c) Security Operations, referring to the way information security roles are organized with the organization and how their associated responsibilities are executed. The defined and assigned responsibilities must translate into tactical and day-to-day secure operation of the business.

In order for appropriate facilitation and execution of governance objectives, clear definition and contracting of roles and responsibilities, as pertaining to Information Security Governance, is required. This is in order to best ensure key performance areas are well understood, agreed and performance measured.

4.4 INFORMATION SECURITY ORGANISATION AND RESPONSIBILITIES

Information Security Officer

The Information Security Officer (ISO) is primarily responsible for driving and maturing the information security management programmed, including the Information Security Governance System (ISGS) within the organization.

Although ultimate accountability for the security of information resides with the Information Security Officer, the Council has granted authority to the ISO to act on its behalf in matters relating to information security. The ISO will communicate and report on relevant information security management aspects directly to the Executive Committee.

The Information Security Officer is required to be approachable and accessible with regards to information security matters. Internal and external parties are encouraged to inform the ISO of information security issues, in order to ensure risks to the organization can be appropriately identified, classified and managed. Constructive suggestions or observations are welcome, and should also be communicated.

Information Security Steering Committee

The RLM Security Council (ISC) shall be established, at the behest of the RLM Council, and act as a collaborative forum through which business stakeholders maintain visibility of, gain insight into, provide leadership towards, monitor and manage information security risk.

4.5 GOVERNING PRINCIPLES

a) The RLM Council is accountable for information security and delegates the authority to the Executive to define a security strategy and implementation.
b) The organization's management is obligated to actively seek and promote good information security governance.
c) Information security is everyone's responsibility.
d) Lower level governance documentation, including information security policies, standards, processes and procedures shall not contravene the principles and practices contained in the Information Security Policy, except where the requirements of the RLM ISMS Deviation Policy has been adhered to.
e) Governing principles and practices in the Information Security Policy will apply where more specific lower level governing documentation does not exist.
f) RLM strives to promote a security conscious culture. The organization and all its representatives must conform to information security best practice and constantly strive to raise the level of information security awareness, not only internal to the organization, but also when dealing with RLM

customers, partners or third parties. All staff with management or supervisory roles is required to actively encourage information security conscientious behavior amongst their staff.

g) Ignorance of information security policies, standards, processes or procedures is no excuse. The Information Security Officer should be consulted where any doubt exists.

h) The information security function is intended to underpin and support the business, through an appropriate risk management approach, and not inhibit it. RLM must strive to appropriately manage the risks to the organization by obtaining a balance between information security and business effectiveness and efficiency.

i) RLM expects anyone with access to its information systems or data, including employees, contractors, partners and service providers, to apply the appropriate levels of information security diligence.

j) RLM protects its information assets in order to ensure it meets its organizational, social, legislative and regulatory obligations.

k) RLM employees and representatives must respect the information and information assets of others and apply the same diligence as with RLM's own.

l) RLM promotes the classification of information and requires anyone handling information that has been classified, to do so in an appropriate manner and in line with its classification.

m) Information assets must be protected in a proactive fashion, instead of a reactive. Reactive information asset protection is ineffective and costly to RLM's business.

n) Access to information assets or systems must comply with the least privilege principle: deny by default, unless expressly required. Access levels must be in line with and based on the information's classification level.

o) Duties should be segregated to ensure that no one person is allowed to create, execute, approve and monitor processes or transactions of value.

p) Information systems must limit components, software and applications to the minimum required to support business function. Streamlined systems are less complex, easier to maintain, more stable, more reliable and more secure.

q) Suspect activity and security incidents must be disclosed to the Information Security Incident Response Team (ISIRT).

4.6 GOVERNING PRACTICES

a) The Information Security Officer annually reviews the security scenario and presents a security strategy addressing security risks to the IGSC and the RLM Executive.

b) All applicable information security policies, -standards and processes are published to the RLM DMS. It includes the most current approved version of this, the Information Security Policy.

c) As a business, RLM will provide information security training to employees or contractors that require it, in order to ensure they are equipped and empowered to make better decisions regarding information security. Even though the organization will take pro-active steps to ensure employees and contractors receive reasonable levels of awareness training, the responsibility to request further information security training where perceived as lacking, resides with the employee or contractors. Training should be requested from the RLM Information Security Officer (ISO) where deemed necessary or where a shortfall has been identified.

d) RLM architects, designs, engineers, deploys and operates technology solutions in a secure fashion. RLM expects its providers, who manage systems or data on RLM's behalf to adhere to the same practice.

e) RLM will respond promptly to information security risks once identified. RLM will implement effective measures to mitigate the immediate threat, but also take relevant measures towards proactively preventing such events from occurring in future.

f) RLM measures the effectiveness and efficiency of its Information Security Governance System (ISGS).

4.7 INFORMATION SECURITY POLICY STATEMENTS

Legislation, regulation and governance

1. Stipulations contained in Information Security Management System (ISMS)-related documentation must at all times comply with the following legislative, regulatory or good governance requirements: -
   a. King Code of Governance for South Africa 2009, or otherwise known as King III.

2. RLM will furthermore adopt various industry standards, and requires alignment within the context of its Information Security Management System (ISMS) to the following:
    a. ISO27001: Information security management systems – Requirements;
    b. ISO27002: Code of practice for information security management;
    c. COBIT (Control Objectives for Information and related Technology); and
    d. ITIL (IT Infrastructure Library), mostly from an integration perspective.

ISMS documentation development, maintenance and deviation

1. The development of new and maintenance of existing Information Security Management System-related documentation, including information security policies, standards and processes, must be performed in accordance with the RLM ISMS Document Development and Maintenance Process. This process has been established to ensure: -
    a. The requirement for governance of a given area is acknowledged and receives buy-in from the relevant stakeholders;
    b. Information security policy, standard and process development and maintenance takes place in a structured and transparent fashion; and
    c. Stakeholders remain informed and progress can be evaluated to allow appropriate management of information security risk.
2. Information security policies, standards and processes must be reviewed in accordance with the scheduled review date defined as part of the RLM ISMS Document Development and Maintenance Process.
3. The Information Security Officer (ISO) is responsible for ensuring all Information Security Management System-related documentation, including information security policies, standards and processes, is distributed to the relevant stakeholders and correctly published to the RLM DMS.
4. The RLM ISMS Deviation Policy governs the principles and practices to be adhered to when deviating from any of the requirements of the Information Security Management System (ISMS)-related documentation, including all

information security policies, -standards and -processes. Non-compliance or deviation must follow the standard RLM ISMS Deviation Process.

Asset Management

1. Information and information assets must have ownership assigned.
2. Information- and information asset owners are responsible for ensuring assets under their control are sufficiently protected and secured. Asset owners must ensure they are familiar and comply with the Information Security Management System (ISMS) at all times. The Information Security Officer is required to, through guidance and collaboration, assist asset owners in achieving this objective.
3. It is the responsibility of information asset owners (business or technical) to ensure an appropriate and current inventory of assets is available at all times, including asset locality, allocation and license number.
4. All information in use by the organization must have an owner assigned, regardless of the form in which it exists, including electronic, paper-based or otherwise.
5. The business owner, and not the technical owner (custodian), is the owner of information. As dictated by the RLM Information Classification Policy (discussed below), the Chief Information Officer (CIO) will be the default owner of information where information ownership is not expressly defined.
6. Information processing facilities or -systems must have business- and technical ownership assigned. The business owner is commonly the role that owns the business function and governance thereof. Technical ownership (custodianship) will typically be assigned to the individual or that is overall responsible for the technical upkeep and administration of the system or facility.
7. Where information processing facility or -system ownership is not expressly defined, the following will apply:
    a. Business ownership will default to the Chief Information Officer (CIO).
    b. Technical ownership will default to the Chief Information Officer (CIO).
8. The use of information and information assets are strictly regulated and must adhere to the RLM Acceptable Usage Policies, as listed in section 11.6 (Human resource security).

9. All equipment and hardware must have appropriate identifiers or asset tags attached.

Information Classification

1. RLM implements an Information Classification System, described in the RLM Information Classification Policy, aimed towards protecting the information assets that is most important to it. An effective and uniformly implemented information classification regime is the cornerstone of many critical areas of governance including access control, network segmentation and personnel clearance, to name but a few.
2. All of the stipulations as contained in the RLM Information Classification Policy must be adhered to at all times.
3. Within the context of the RLM Information Classification Policy, information should be described in terms of information classes, such as “customer records”, “human resource information” or “transaction records”. Information classes may be defined coarsely initially, and specified more granularly where required or necessitated by business use or ownership requirements.
4. Every defined information class must be described in an Information Class Policy document. Information Class Policy documents are described in detail in the RLM Information Classification Policy and contains (at a high level), but is not restricted to: -
    a. The unique name of the information class;
    b. A description of the information class, assigned an unambiguous meaning within the organization;
    c. An information category, which can be “Public”, “Internal Use Only”, or “Confidential”. All information within the “Confidential” or “Internal Use Only” categories can collectively be described as sensitive information. Whenever the term sensitive information is used in the context of the Information Security Management System (ISMS), these categories are implied;
    d. An Information Class Owner. The information owner is responsible for ensuring the accuracy and appropriateness of the specific Information Class Policy as a whole;

e. Access management requirements, including an access list of business roles that should have access to the information defined by the information class;
f. Clearance requirements, indicating the vetting requirements prior to individuals being allowed access to information;
g. Permissible actions, dictating in which security zones information can be stored or processed, or transmitted to/from.
h. Labeling standards, indicating how information should be marked, depending on the format it is contained in; and
i. Retention and disposal requirements.

5. The requirements contained in the Information Class Policy must be adhered to at all times. Any deviations must be raised with the information owner, as defined in the Information Class Policy, or the Information Security Officer.

Human resource security

1. The following parties must always ensure they adhere to the relevant information security policies, standards and processes of the organization:

   a. RLM employees and contractors;
   b. Service providers with access to RLM's information or with access to RLM's assets or assets managed on its behalf; and
   c. Third parties entrusted with RLM's information or with access to RLM's assets or assets managed on its behalf.

2. As of the effective date of this policy all employees and contractors must sign:
   a. An employment contract or contractor agreement, respectively, which must require adherence to all the requirements of the RLM Information Security Management System (ISMS), and collectively includes: information security policies, standards, processes and procedures.
3. All RLM representatives (including employees and contractors), service provider representatives and third party representatives granted access to RLM's information systems, including end-user technologies, or information systems managed on behalf of RLM, must at a minimum sign the RLM Acceptable Usage Policy.

4. Any person(s) requiring access to sensitive RLM information must be cleared before access is deemed authorized. The following clearance rules apply: -
    a. Access to “Public” information does not require any clearance, as it is not regarded as sensitive.
    b. Clearance to access “Internal Use Only” information requires: -
        i. A background check; and
        i. A credit check.
    c. Clearance to access “Confidential” information always requires the clearance requirements for “Internal Use Only” information (as stated above) to have been satisfied at a minimum. Over and above the aforementioned, the Information Class Policy, as defined by the information owner, stipulates any possible additional clearance requirements for classes assigned into the “Confidential” information classification category.
5. Clearance requirements must be adhered to regardless of the relationship RLM has with an individual(s). It must be ensured that all contractual agreements (employment, contractor, service provider, partner etc.) make provision for clearance requirements relevant to the information that will be accessed.
6. Access to information or provisioning of employees, contractors or third parties on information systems may only be granted once the relevant commercials are in place and clearance procedures have been followed.
7. Upon termination of employment or contract, all copies of information and assets in the possession of the employee or contractor must be returned to RLM. All rights and access granted to the employee or contractor within their employment or contract term must immediately be revoked upon termination thereof or final formally agreed day of service.
8. Negligence or malicious behavior will, in the case of employees, result in the RLM Disciplinary Process being invoked. Contractors or service provider representatives will immediately be escorted offsite and remediation sought in line with any contractual agreement or binding usage policy. Legal action may be instituted where deemed necessary.

Physical and environment security

1. Unless otherwise specified, physical security is the responsibility of the site's Facilities Manager.
2. Appropriate physical security mechanisms must be in place at all building perimeters. Access to areas where "Confidential" information is processed or stored, or where information systems containing such information are located, must additionally be protected through strict access control mechanisms.
3. All servers and networking equipment must be located in designated laboratory environments, Computer Equipment Rooms (CERs) or lockable computer equipment Cabinets situated within access controlled areas.
4. Data Centers and Servers Rooms must be protected against environmental threats. This includes having appropriate controls of the following nature in place: -
    a. Fire suppressant;
    b. Heating, ventilation and air conditioning (HVAC);
    c. Power redundancy and backup; and
    d. Video surveillance.
5. Information asset owners must ensure that appropriate continuity and disaster recovery measures are in place for information systems, in line with the RLM Business Continuity Policy.
6. All information security policies, standards, processes and procedures apply to Business Continuity Sites (BCS) and Work Area Recovery (WAR) sites in the same way as for production sites.
7. Cabling and telecommunications equipment located both inside and outside building perimeters must be reasonably protected against damage or interception of information.
8. Any equipment that is disposed of or to be re-used by external parties must have all information stored on it properly destroyed, in line with the RLM Asset Disposal Policy. Such equipment includes any equipment containing hard disks or solid state storage, including removable storage media, servers, laptops, workstations, PDAs, mobile phones, etc.
9. All documents containing "Confidential" information must be shredded before being disposed of or taken offsite for recycling or destruction.

10. Users are required to practice a clear desk policy, and ensure no sensitive information is left unattended in work areas.
11. The RLM Asset Removal Policy regulates the removal of equipment from buildings.
12. All individuals issued with mobile computing equipment must take reasonable steps towards ensuring the security of such equipment at all times.

Operational procedures and responsibilities

1. Change control requirements, as defined in the RLM Change Management Policy, should be strictly implemented for all production systems, but especially for systems containing sensitive information or systems that support key business activity.
2. Environments used for system development and testing must be segregated. At a minimum, production facilities must be separated from development and testing.
3. Production data may not be used within development and testing environments.
4. All code implementations to production must go through an appropriate release management process. A designated Release Manager role, separate from general developer roles, should be used to deploy code releases into production.

System planning and acceptance

1. Appropriate capacity planning must be performed for information systems.
2. Information security controls must be implemented and tested as part of systems acceptance testing.

Information backup

1. The availability of information is critical to the organization. It must be ensured that any information of value is sufficiently backed up and can be suitably recovered.
2. The stipulations contained in the RLM Business Continuity Policy must be adhered to at all times.

Network security

1. Network infrastructure must be securely implemented, operated and managed at all times.
2. Network Administrators are responsible for ensuring network infrastructure is securely designed, deployed and maintained, by adhering to all the requirements of the RLM ISMS, including the RLM Component Security Policy, and security configurations standard situated below it.
3. Network segregation is a key design principle that must be implemented between networks that have different trust levels. Segregation includes appropriate segmentation of networks and implementation of network filtering, such as implemented through firewall access rules, between network segments of different trust levels.
4. The following security zones, which include both the network and physical environment, have been defined within the RLM context: -
    a. Network Management (extreme trust to be maintained);
    b. Enterprise network (medium trust to be maintained);
    c. DMZ (high trust to be maintained); and
    d. Internet (no trust).
5. The requirements of the RLM Network Filtering Security Practice Standard must always be adhered to. Appropriate network filtering (firewall, network traffic filter) access rules must be implemented, in line with this standard, to ensure only valid and absolutely required traffic is allowed to traverse the network segment boundaries of the security zones defined above.
6. Systems that have access to and are used to manage network infrastructure must be appropriately secured, and should be segmented on a network level. The Network Management security zone is designated to this purpose.
7. Network infrastructure must be securely implemented to ensure information transmitted via site-to-site links over public networks, or networks over which RLM does not have control, (be that operational or contractual) is safeguarded. This includes ensuring appropriate authentication and encryption of traffic. This requirement also applies to remote users connecting to the corporate network.

8. Client contractual requirements may demand additional controls over and above the aforementioned (clause 7). These controls must be consistently and uniformly enforced in order for RLM's obligations to be sufficiently met.
9. Wireless network infrastructure should only be implemented if there is a definite business need. Where implemented, wireless networks must adhere to current best practice and enterprise-class configuration. Authentication mechanisms such as pre-shared keys (PSK) may therefore **NOT** be used. The appropriateness of the security of wireless networks must be assessed in line with the stipulations of the RLM Vulnerability and Patch Management Policy.
10. Changes to network infrastructure must adhere to the requirements of RLM Change Management Policy, and the RLM Network Filtering Security Practice Standard where network filtering access rules are involved.
11. Network infrastructure should appropriately log activity, including security events. Logging must be performed in line with the requirements contained in **Monitoring**.

Access control

1. Access to information systems and information, especially where classified as "Confidential", must be strictly controlled.
2. Information systems, applications and network protocols must require appropriate authentication. Authentication levels should be in line with the value of the information system. High value systems, such as those storing or processing "Confidential" information, should preferably implement two-factor authentication.
3. Unique user identifiers (logins or accounts) must always be used when granting access.
4. System- and application owners (custodians) are responsible for ensuring the operating system; system components or applications under their control always adhere to the RLM Password Security Practice Standard (previously referred to as the Password Policy).
5. Default and built-in system- or application administrative account passwords must be appropriately secured at all times. Knowledge of such passwords must be limited to the system- or application owner, or highly trusted individuals to which such authority has been expressly delegated.

The RLM Password Security Practice Standard governs the management of such passwords.

6. Information system users are responsible for: -
   a. Understanding and adhering to RLM Password Security Practice Standard;
   b. Keeping their passwords confidential at all times;
   c. Not allowing any other person to utilize their logon sessions in an unattended fashion, or allowing their password to become known to any other party, including IT personnel; and
   d. Informing the relevant system or application owner(s) immediately, should their password be disclosed, compromised or suspected of having been compromised in any way.
7. Information systems must implement Role-Based Access Control (RBAC) measures that are aligned with business roles.
8. Rights assignment must adhere to the least privilege principle. Access must therefore be denied, except if expressly required. Rights must only be granted to the role(s) that have a valid business purpose to access the information or information system in question.
9. The rights assigned must always be in line with the access list defined in the Information Class Policy for that particular class of information (described in section 11.5 – Information Classification), especially where the information is classified as “Confidential”. Where information has not been expressly classified, the “Internal Use Only” classification would apply.
10. Administrative access to systems may only be allowed to expressly authorized personnel.
11. Standard user access profiles should be defined for common job functions.
12. Access rights must be adjusted or removed within one business day, should business roles change or access no longer be required.
13. Access levels must be reviewed on a regular basis in order to ensure it reflects current access requirements. This especially includes review of privileged roles or role- s, which have a high level of privilege, such as system administrator roles.
14. Personnel, both internal and on the part of service providers, responsible for granting and revoking access to information systems, must ensure they are familiar with user provisioning and de-provisioning processes and procedures.

15. Access to information systems may not be granted without the appropriate provisioning processes and procedures having been followed.
16. Individuals may not be granted access to the Enterprise and Network Management security zones, and systems or applications residing within it, without: -
    a. An authorization form having been completed and approved.
17. System and application owners must ensure they have registered with Human Resources in order to be included in relevant RLM Joiners and Leavers Process flows.
18. Unattended user equipment and access sessions must be secured. This includes enforcing the locking of user sessions when unattended for more than 10 minutes.

System and component security

1. All hosts, including network devices, servers, workstations and mobile computers, such as laptops, must be deployed and maintained in a secure fashion. This includes adhering to the requirements of the RLM Component Security Policy at all times.
2. All vulnerabilities or security issues with a critical or high severity rating must be remediated within thirty (30) days of release of patch or update by the operating system-, system component- and application vendor.
3. All hosts must be configured and maintained in a secure manner, and security vulnerabilities must be remediated in line with any additional requirements of the RLM Vulnerability and Patch Management Policy.
4. Systems must be protected against malicious and unauthorized code, as required by the RLM Component Security Policy. This includes diligence on the part of the users of these systems, and the implementation, operation and management of appropriate measures, technological and otherwise, to prevent malicious and unauthorized code from executing on systems.
5. Only authorized software may be installed on RLM's systems or systems managed on its behalf.
6. Appropriate Release Management must be in place to ensure only authorized and licensed software is deployed onto systems.
7. Business information stored on workstations, laptops and servers must be appropriately backed up to designated network locations.

8. Foreign hosts may not be introduced onto RLM's network without prior authorization, and are required to have security controls in place that are in line with or exceed that of acceptable internal RLM systems.
9. The use of information systems is strictly regulated and must adhere to the Acceptable Usage Policies defined in section 11.4 (Asset Management).

Information systems acquisition, development and maintenance

1. Business processes involving development of new, acquisition of off-the-shelf or enhancements to existing information systems, must ensure the requirement for security controls are clearly defined, implemented and tested. Security must be a consideration from the planning phase and must never be treated as an afterthought.
2. Security controls must adhere to the minimum RLM requirements, but should additionally be in line with the business value of the system. Adoption of purchased products or development of internal information systems or processing facilities must adhere to the requirements of the RLM Risk Assessment and Management Policy.
3. The RLM ISMS Deviation Process must be followed where inappropriate controls are encountered on internally developed or purchased products, especially where it cannot be remediated or becomes infeasible to remediate.
4. Security must be embedded within the Systems Development Lifecycle (SDLC).
5. All application security policies and practice standards must be adhered to within the development and maintenance lifecycles.
6. Systems and applications must ensure users and automated processes are properly authenticated. Suitable authorization to data and functions must be enforced throughout.
7. Applications must ensure appropriate input validation is performed. Input validation includes both validation according to business rules and validation for security purposes.
8. Internal system processes must ensure the integrity and confidentiality of data is preserved. It must also be ensured that appropriate controls are in place to guarantee message integrity and confidentiality when communicating with other information systems.

9. Appropriate validation of system output must be performed, including validation according to business rules and from a security perspective.
10. Information leakage in applications must be guarded against.
11. Enterprise-class frameworks should be used when developing applications. Best practice development and application architecture techniques should be implemented. This includes using secure data access layers when applications access data in data repositories.
    a. where Internet-facing, undergo the relevant testing and assessment, in line with the requirements of the RLM Vulnerability and Patch Management Policy; and
    b. Non-conformance to security standards must be for the cost of the provider.
12. Deployment of information systems and enhancements must follow the RLM Change Management Process and code releases must be suitably managed.

Cryptography and key management

1. Only acceptably secure cryptographic algorithms or operations should be implemented on information systems, in line with the requirements of the RLM Cryptographic Algorithm and Key Management Policy.
2. Secure key management practices, as stipulated in the RLM Cryptographic Algorithm and Key Management Policy, should be followed throughout the key lifecycle, including during key generation, key exchange, key backup and key recovery.
3. Key management practices must be strictly adhered to, especially during the interchange of keys with external parties.

Third party services

1. Diligence must be applied in the take-on of third party- or service provider services.
2. The RLM Service Provider Security Management Policy must at all times be adhered to before granting external parties direct access to RLM “Internal Use Only” or “Confidential” information assets or assets managed on behalf of RLM. This includes information, information systems and -processing facilities.

Client security management

1. Diligence must be applied in the management of client systems and information.
2. Unless expressly agreed otherwise, all client systems must be managed in line with the policies and standards as required by the RLM Information Security Management System (ISMS).
3. All client information must be treated as “Confidential” and may only be disclosed to RLM personnel or approved external parties with an express need to know.

Exchange of information

1. External parties may pose a risk to RLM through a lack of appropriate information security management on their part.
2. Third parties must be made aware of their responsibilities, and agree to the safe and secure handling of such information before it is interchanged. This accounts for the ultimate recipient of the information and any providers that may be facilitating the interchange.
3. An appropriate Confidentiality Agreement, also referred to as a Non-Disclosure Agreement (NDA), must be signed before “Internal Use Only” or “Confidential” information is exchanged or access is granted to RLM information assets. The upkeep of these legal agreements is the responsibility of the RLM Legal Department, from which current versions are available.
4. Clearance requirements, as described in section 11.6 (Human resource security), must be satisfied before information is interchanged with third parties.
5. When exchanging information with third parties it must be ensured that “Confidential” information is appropriately secured and protected, by adhering to the following requirements:
    a. Where the Information Class Policy for the information in question does not expressly allow disclosure to the external party, approval must be obtained from the information owner prior to disclosure;

b. Information must not be exchanged using unencrypted means of communication, such as through unencrypted email or other clear-text networking protocols; and

c. Senders and recipients of information must take care in the interchange process, such as taking precaution when having telephonic conversations, not leaving facsimiles unattended or leaving hardcopy documents in a generally accessible area.

6. Information that is exchanged using portable storage media must be securely deleted from such media once the exchange has been completed.

Electronic commerce

1. When conducting electronic commerce or transacting online or through mechanisms such as email, it must be ensured that both parties can appropriately identify each other, and that the transaction's confidentiality and integrity remains intact.
2. Where transactions are required to be binding, appropriate measures should be in place to ensure non-repudiation, such as using digital signatures or compliance with the RLM Procurement Policy.

Media handling

1. All media should be appropriately protected from unwanted disclosure of information.
2. It must be ensured that appropriate measures are implemented to keep the information stored on media, including backup tapes, CDs, DVDs, USB memory sticks, fixed or removable hard drives etc., secure at all times.
3. Measures include ensuring media is sufficiently protected from physical theft.
4. Measures must be taken to ensure "Confidential" information stored on media is sufficiently protected in case of compromise. Acceptable measures include the use of encryption technology, and acceptable key management procedures in line with section 11.15 (Cryptography and key management).

5. In cases where physical theft of electronic storage media do occur, the information on the media must have been appropriately secured (encrypted) and remain protected.
6. Media disposal must occur in a safe, dependable and secure fashion, specifically where “Confidential” information is involved. Media disposal must be in line with the requirements of the RLM Asset Disposal Policy.

Monitoring

1. Information systems and applications should generate appropriate audit logs.
2. Audit logs should capture relevant transactional information and user-, system- and application activity.
3. The requirements of the RLM Security Event Log Management and Analysis Policy must be adhered to at all times, including ensuring: -
    a. Appropriate audit log configuration and settings are applied;
    b. Systems are time synchronized, and audit logs contain timestamps;
    c. Audit logs are secured against modification and only accessible to authorized identities;
    d. Audit logs for key systems must be reviewed on a regular and appropriate basis, or relevant automated analysis performed and alerts generated. Security incidents must be escalated in a timely manner, in line with section 11.24 (Information security incident response).
    e. Audit logs on key systems must be securely backed up on a regular basis; and
    f. Audit logs must be retained in line with the log retention requirements as stipulated in the Information Class Policy / Policies that may apply to the system in question.

Vulnerability management

1. An appropriate Vulnerability and Patch Management Programmed must be maintained at all times.
2. The stipulations contained in the RLM Vulnerability and Patch Management Policy must be adhered to at all times.

3. Information system- and application owners must give their support for, make the necessary resources available and ensure they cooperate with the Vulnerability and Patch Management (VPMG), in order to ensure it is capable of meeting its objectives.

Risk assessment

1. Information security risk assessments must be performed on an annual basis, in line with the RLM Risk Assessment and Management Policy.
2. The RLM Security Council (GSC) chairperson, as stipulated by the GSC Terms of Reference, is responsible for ensuring any risks, including those identified during the course of the formal information security risk assessment exercise, are: -
    a. Appropriately managed, through application of remedial actions; or
    b. Accepted through invocation of the RLM ISMS Deviation Process.

Information security incident response

1. The RLM Information Security Incident Response Policy must be adhered to at all times, when responding to information security incidents.
2. All actual or perceived information security incidents must be reported to the Information Security Incident Response Team (ISIRT) Manager, a role held by the Information Security Officer. Where not available, the ISIRT Contact List, published to the RLM DMS and also generally distributed, should be consulted for other relevant Information Security Incident Response Team contacts.

3. Information asset owners must provide their full cooperation to the Information Security Incident Response Team, or any representatives thereof, and ensure relevant personnel are mobilized to deal with the incident in an appropriate and swift manner.

    RLM representatives, and service provider representatives that are contractually bound, must provide their full cooperation to the Information Security Incident Response Team, or any representatives thereof, at all times.

CHAPTER5: TELEPHONE USAGE POLICY

5.1 OBJECTIVES AND STANDARDS

The purpose of this policy is to:

1. Regulate what is permissible when using council resources
2. To ensure the effective and efficient use of municipal telephones
3. To ensure that employees pay the cost of using municipal telephones for private use.
4. To minimize lost time due to employees devoting council time in pursuit of personal interests.
5. To prevent the use of municipal telephones by unauthorized persons
6. To minimize telephone costs for the municipality
7. To outline expected recourse for misuse of telephones

The main objective is to regulate the usage of the Municipality's telephones to ensure that telephones are available and are used for the conduct of official municipal business, in the direct support of assigned duties and responsibilities of users and the delivery municipal services.

It shall be the responsibility of the council to provide all directorates with a satisfactory and reliable telephone service.

5.2 TIMEFRAMES

- This policy shall be reviewed or re-confirmed as in every 12 months.
- This policy becomes effective from the date of approval by council
- The policy shall remain in force until it is appropriately replaced with another policy

5.3 PRINCIPLES

This policy is underpinned by the principles of:
-Honesty
- Fairness
- Accountability
- Collective responsibility
- Equity
- Transparency

5.4 ROLES AND RESPONSIBILITIES

ICT STEERING COMMITTEE
The ICT steering committee through the IT Security Officer shall be the implementing authority of this policy and shall facilitate its annual revision.

MUNICIPAL EMPLOYEES
All Municipal employees are expected to familiarize themselves with the provisions of this policy and to comply with these provisions.

COUNCIL
Only the council may approve this policy and any amendment.

5.5 TELEPHONE USAGE CONTROL MEASURES

5.5.1 CALL RESTRICTIONS

- Each official (pin code) shall be restricted to make calls to a specific amount per month and shall be automatically deactivated upon reaching the limit.

- Officials shall only be entitled to make international calls with the specific approval of the Director/Unit manager.

5.5.2 PIN CODES

- The official in whose name the pin code is issued is responsible and liable for the usage of pin code.

- Management may change pin codes frequently to mitigate fraud risks

- Each qualifying municipal official shall be allocated a secret telephone access pin code signed for and known to the employee who will be responsible for its protection at all times

- The owner of the pin code is still liable for any cost arising out of calls by someone who fraudulently obtained it.

5.5.3 PRIVATE CALLS

-The Municipality recognizes that there may be some occasions normally due to circumstances or an emergency where it is necessary for members of staff to make private calls.

- The telephone system is an organizational resource and use of the telephone can and may be monitored and an itemized listing of telephone numbers for a period will be produced.

- The making/receiving of private telephone calls should be kept to a minimum and be of short duration.

- Private telephone calls should be timed whenever possible to ensure minimum disruption both to the work of individual and to the workload of colleagues.

5.5.4 TELEPHONE ACCOUNTS

-The IT unit shall issue out monthly telephone statements of account for each official

-Each staff member shall after declaring the private calls sign the statement as an authorization that the cost of their private calls be deducted from their salaries
-The Human Resources department shall make payroll deductions from employees' salaries in respect of private calls made.

- Telephone statements shall be delivered to the managers, who will inspect such statements before distributing them to the respective employees.

CHAPTER6: INTERNET USAGE POLICY

6.1 USAGE THREATS

Internet connectivity presents the RLM with new risks that must be addressed to safeguard the facility's vital information assets. These risks include:

6.1.1 Inappropriate Use of Resources

Access to the Internet by personnel that is inconsistent with business needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet. Additionally, the RLM may face loss of reputation and possible legal action through other types of misuse.

6.1.2 Misleading or False Information

All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

6.2 INTERNET SERVICES

Access to the Internet will be provided to users to support business activities and only on an as needed basis to perform their jobs and professional roles.

6.2.1 User Services

6.2.2 Internet Services Allowed

Internet access is to be used for business purposes only. Capabilities for the following standard Internet services will be provided to users as needed:

• E-mail -- Send/receive E-mail messages to/from the Internet (with or without document attachments).

• Navigation -- WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser tool. Full access to the Internet; limited access from the Internet to dedicated RLM public web servers only.

• File Transfer Protocol (FTP) -- Send data/files and receive in-bound data/files, as necessary for business purposes.

• Telnet -- Standard Internet protocol for terminal emulation. User Strong Authentication required for Internet initiated contacts into the RLM. Management reserves the right to add or delete services as business needs change or conditions warrant. All other services will be considered unauthorized access to/from the Internet and will not be allowed.

6.2.3 Request & Approval Procedures

Internet access will be provided to users to support business activities and only as needed to perform their jobs.

6.2.4 Request for Internet Access

As part of the Internet access request process, the employee is required to read both this Internet usage Policy and the associated Internet/Intranet Security Policy. The

user must then sign the statements (located on the last page of each document) that he/she understands and agrees to comply with the policies. Users not complying with these policies could be subject to disciplinary action up to and including termination.

Policy awareness and acknowledgment, by signing the acknowledgment form, is required before access will be granted.

6.2.5 Approval

Internet access is requested by the user or user's manager submitting an IT Access Request form to the IT department along with an attached copy of a signed Internet usage Coverage Acknowledgment Form.

6.2.6 Removal of privileges

Internet access will be discontinued upon termination of employee, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be re-evaluated by management annually. In response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users.

6.3 USAGE POLICIES

6.3.1 Resource Usage

Access to the Internet will be approved and provided only if reasonable business needs are identified. Internet services will be granted based on an employee's current job responsibilities. If an employee moves to another business unit or changes job functions, a new Internet access request must be submitted within 5 days. User Internet access requirements will be reviewed periodically by RLM departments to ensure that continuing needs exist.

6.3.2 Allowed Usage

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the IT Department.

Acceptable use of the Internet for performing job functions might include:

• Communication between employees and non-employees for business purposes;

• IT technical support downloading software upgrades and patches;

• Review of possible vendor web sites for product information;

• Reference regulatory or technical information.

• Research

6.3.3 Personal Usage

Using RLM computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

All users of the Internet should be aware that the RLM network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The RLM is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property

6.3.4 Prohibited Usage

Information stored in the wallet, or any consequential loss of personal property.

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

The RLM also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libellous materials.

Other activities that are strictly prohibited include, but are not limited to:

• Accessing RLM information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.

• Misusing, disclosing without proper authorization, or altering customer or personnel information.

This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.

• Deliberate pointing or hyper-linking of RLM Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the RLM.

• Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law including without limitations US export control laws and regulations.

• Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.

• Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.

• Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libellous, threatening, harassing material, including but not limited to comments

based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.

• Any form of gambling.

Unless specifically authorized under the provisions of section 4.3, the following activities are also strictly prohibited:

• Unauthorized downloading of any shareware programs or files for use without authorization in advance from the IT Department and the user's manager.

• Any ordering (shopping) of items or services on the Internet.

• Playing of any games.

• Forwarding of chain letters.

• Participation in any on-line contest or promotion.

• Acceptance of promotional gifts.

Bandwidth both within the RLM and in connecting to the Internet is a shared, finite resource.

Users must make reasonable efforts to use this resource in ways that do not negatively affect other employees. Specific departments may set guidelines on bandwidth use and resource allocation, and may ban the downloading of particular file types. If you have any questions about Acceptable Use, contact the IT Department

6.3.5 Software License

The RLM strongly supports strict adherence to software vendors' license agreements. When at work, or when RLM computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to the IT Department for review or to request a ruling from the Legal Department before any copying is done.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

Using RLM computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

All users of the Internet should be aware that the RLM network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The RLM is not responsible for any loss of information, such as information,

such as information stored in the wallet, or any consequential loss of personal property

6.3.6 Review of Public Information

All publicly-writeable directories on Internet-connected computers will be reviewed and cleared each evening. This process is necessary to prevent the anonymous exchange of information inconsistent with RLM business. Examples of unauthorized public information include pirated information, passwords, credit card numbers, and pornography.

6.3.7 Expectation of Privacy

6.3.7.1 Monitoring

Users should consider their Internet activities as periodically monitored and limit their activities accordingly. Management reserves the right to examine E-mail, personal file directories, web access, and other information stored on RLM computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of RLM information systems.

6.3.7.2 E-mail Confidentiality

Users should be aware that clear text E-mail is not a confidential means of communication. The RLM cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once an E-mail is transmitted it may be altered. Deleting an E-mail from an individual workstation will not eliminate it from the various systems across which it has been transmitted.

6.4. Maintaining Corporate Image

6.4.1 Representation

When using RLM resources to access and use the Internet, users must realize they represent the RLM. Whenever employees state an affiliation to the RLM, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the RLM". Questions may be addressed to the IT Department.

6.4.2 RLM Materials

Users must not place RLM material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, public news group, or such service. Any posting of materials must be approved by the employee’s manager and the public relations department and will be placed by an authorized individual.

6.4.3 Creating Web Sites

All individuals and/or business units wishing to establish a WWW home page or site must first develop business, implementation, and maintenance plans. Formal authorization must be obtained through the IT Department. This will maintain publishing and content standards needed to ensure consistency and appropriateness.

In addition, contents of the material made available to the public through the Internet must be formally reviewed and approved before being published. All material should be submitted to the Corporate Communications Directors for initial approval to continue. All RLM pages are owned by and are the ultimate responsibility of, the Corporate Communications Directors.

All RLM web sites must be protected from unwanted intrusion through formal security measures which can be obtained from the IT department.

6.4.4 Periodic Reviews

6.4.5 Usage Compliance Reviews

To ensure compliance with this policy, periodic reviews will be conducted. These reviews will include testing the degree of compliance with usage policies.

6.4.6 Policy Maintenance Reviews

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of usage policies. These reviews may result in the modification, addition, or deletion of usage policies to better suit RLM information needs.

6.5 REFERENCES

6.5.1 Points of Contact

If you need assistance regarding the following topics related to Internet usage, contact the IT Department for additional assistance: **014 590 3159/7**

CHAPTER7: E-MAIL USAGE POLICY

7.1 OBJECTIVE

To prevent tarnishing the public image of RLM When email goes out from RLM the general public will tend to view that message as an official policy statement from the RLM.

7.2 POLICY STATEMENT

- **Prohibited Use**.

  The RLM email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any RLM employee should report the matter to their supervisor immediately. Email sending capacity is limited to 10MB

- **Personal Use**.

  Using a reasonable amount of RLM resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a RLM email account is prohibited. Virus or other malware warnings and mass mailings from RLM shall be approved by RLM VP Operations before sending. These restrictions also apply to the forwarding of mail received by a RLM employee.

- **Monitoring**

  RLM employees shall have no expectation of privacy in anything they store, send or receive on the council's email system. RLM may monitor messages without prior notice. RLM is not obliged to monitor email messages.

- **E-mail Archiving**

  The Exchange Server has a quota based system. For any archiving the user is prompted monthly by Outlook to archive locally to their machine and not on the server but it is recommended that users must archive their e-mails on the backup shared drives.

CHAPTER8: ANTI-VIRUS POLICY

8.1 OBJECTIVES

This policy applies to all RLM computers that run Microsoft or Macintosh operating systems. This includes, but is not limited to, desktop computers, laptop computers and servers.

a) All RLM computers running Microsoft Windows or Macintosh operating systems must have RLM standard, supported anti-virus software installed and scheduled to run at regular intervals.

b) In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free.

c) The RLM IT department/unit is responsible to ensure that anti-virus software is active at regular intervals, and computers are verified as virus-free.

d) Any activities with the intention to create and/or distribute malicious programs into RLM's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Acceptable Use Policy.

8.2 ANTI-VIRUS POLICY

a) The RLM will use a single anti-virus product for anti-virus protection and that product is McAfee anti-virus software.

b) The anti-virus product shall be operated in real time on all servers and client computers. The product shall be configured for real time protection.

c) The anti-virus library definitions is automatically updated once a day.

d) Anti-virus scans shall be done a minimum of once a week on all user controlled workstations and servers. No one should stop anti-virus definition updates and anti-virus scans except for domain administrators.

8.3 EMAIL SERVER POLICY

a) The email server will have additional protection against malware threats since email with malware threats must be prevented from entering the network.

b) When a virus or malware threat is found in an email, such email should be deleted with immediate effect and not to notify either the sender or recipient. The reason for this is that most viruses fake the sender of the email and sending them a notice that they sent a message with a virus may alarm them unnecessarily since it would not likely be true.

It would simply cause an additional help desk call by the notified person and most likely waste system administrator's time needlessly. Notifying the

recipient that someone tried to send them a virus would only alarm them needlessly and result in an increased number of help desk calls.

CHAPTER9: BACKUP POLICY

9.1 PURPOSE

RLM Technical team is responsible for ensuring that all operational data and latest status is recoverable in the event of accident loss or damage.

9.2 FREQUENCY AND TIMING OF BACKUPS

- **Main Site:**
  Full back up of the operational site shall be made every day including:

  All Operational Data
  All Servers Data and Status
  All user files saved on a central user documents on the domain controller server.

- **DR Site:**
  The DR Site is a replica of the main site and there is real-time synchronisation of data and state between the two sites.

  The backup device will be installed at the main site. The backup will be scheduled to run automatically at 3pm daily during the week, i.e: Monday to Friday.

9.3 BACKUP ROSTER

A designated Backup technician will be responsible to manage and monitor the backup schedule and the IT Manager will supervise the overall backup plan.

Tasks:

1. Changing tapes: inserting tape at close of day and removal of tape first thing on every Friday morning, from the backup unit – see attached instructions[3]
2. Storing the backup tapes
3. Checking the backup has been successful
4. Managing a backup failure
5. Maintaining the backup log.

- **Verification of Backup Status**

  The designated member of staff must check the backup status on the system first thing each morning and report any failures to the IT manager before 9am every morning.

- **Backup Log**

  A daily backup log (see Index) is issued to keep a report of backups, their status, which tapes are used and housekeeping of the backup system. These logs and tapes will be stored offsite.

- **House-keeping of the Backup System**

  Regular maintenance of the backup device will be carried out to ensure it is kept in good working order.

  Cleaning tapes will be carried out in accordance with manufacturer's instructions and recommendations. DLT tape drives should be cleaned monthly or more often if the cleaning light is illuminated.

- **Managing Backup Failure**

  In the event of an unsuccessful backup, the staff responsible for checking the backup must immediately:

  1. Note any messages / information on the server monitor
  2. Report the failure to the IT manager
  3. Record the failure in the backup log and any actions taken as a result
  4. Clean the tape drive using the manufacturer's recommended cleaning cartridge
  5. Check the age of the tape used. Destroy tape and replace if near or over its age limit
  6. If the backup fails repeatedly, it may be necessary to perform a manual backup. This takes time, and must be performed when all users are logged out.

- **Storage of Backup Tapes**

  The backup tapes when removed from the server will be stored securely in a locked fire-proof media safe offsite.

  The tapes will be collected on specified days of the week to be taken off-site when removed from the server and stored in a fire-proof media safe. At the same time, the tape deposited [two or three] weeks previously will be collected and returned to the Main Site for reuse the following week.

  At any time there should be:

  - [Two or more, depending on tape rotation] complete backup tapes (both less than four days old) stored on the premises
  - [Two or more, depending on tape rotation] complete backup tapes (both less than fifteen days old) stored off-site at a secure location.

- **Validation of Backup Tapes**

  A backup tape will be validated every 3 months. As part of this process the team will check to ensure data can be fully restored from the tape.

- **Management of Tapes**

  Tapes will be clearly labelled with a [number or day of the week] and used in strict rotation to ensure even wear and immediate identification of any problems with a specific tape.

  An example of a typical backup cycle:

  All data is backed up to tape overnight on Monday/Friday (each week). One tape per site will be used to back-up the entire data **(Full backup),** and another tape will be used for incremental and differential backup and another tape) will be used to do the monthly backup (Full Backup of all data). This is in-line with the ***Grandfather – Father – Son*** backup method.

  Tapes must be replaced at the first sign of deterioration. Tapes are labelled to show age, and date due for replacement, according to the manufacturer's recommendations.

  Old tapes are reformatted or physically disrupted so as to render any data on them unrecoverable. (Need a tape disposal policy)

  Tapes left in the server over the weekend are used three times instead of once a week. This additional wear is taken into account when determining its replacement date.

- **Software**

  Only the IT technical staff are authorised to load software onto any part of the RLM network. Any other member of staff found to be loading software without authorisation may be subject to disciplinary procedures.

  HR will ensure that all staff is aware of this by [signing policy, induction etc.].

  Original copies of RLM software and licensing agreements will be stored in IT Manager's Office and System Administrator will be responsible for safe keeping of the media.

CHAPTER10: SYSTEMS ACCESS CONTROL POLICY

10.1 OUT OF SCOPE

The RLM external website and other information classified as 'Public'.

Systems outside the IT Unit control

10.2 RESPONSIBILITIES

Members of RLM:

All members of RLM, RLM's associates, agency staff working for RLM may have or require access to RLM data or IT systems, and may be responsible for the systems upon which RLM's data reside.

10.3 SYSTEM OWNERS

Those with responsibility for systems (including designating access) upon which RLM data reside. This includes but is not limited to Finance and Public Safety.

- **Information Technology Department**:

  Responsible for administering access to RLM's Active Directory environment and many of its systems. Responsible for implementing role based access control upon the Municipality's shared access file systems, creating RLM's Active Directory user accounts and passwords, and maintaining RLM's network infrastructure.

- **Information Security Officer**:

  Responsible for writing this policy and establishing access control principles.

- **Information Security Advisory Board**

  Responsible for the advising on and recommending information security policies to the Information Technology Committee, assessing information security risks, identifying and implementing controls to risks.

- **Information Technology Steering Committee**

  Responsible for approving information security policies.

10.4 POLICY

- **Principles**

  RLM will provide all employees and contracted third parties with on-site access to the information they need to carry out their responsibilities in an effective and efficient manner as possible.

- **Generic identities**

Generic or group IDs shall not normally be permitted as means of access to RLM data, but may be granted under exceptional circumstances if sufficient other controls on access are in place.

- **Privileged accounts**

  The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled and not provided by default.

  Authorisation for the use of such accounts shall only be provided explicitly, upon written request from a Departmental manager, and will be documented by the system owner. Technical teams shall guard against issuing privilege rights to entire teams to prevent potential losses of confidentiality and / or integrity.

- **Least privilege and need to know**

  Access rights will be accorded following the principles of least privilege and need to know.

- **Maintaining data security levels**

  Every user should understand the sensitivity of their data and treat them accordingly. Even if technical security mechanisms fail or are absent, every user should still attempt to maintain the security of data commensurate to their sensitivity. The Information Classification Standard enables users to classify data appropriately and gives guidance on how to store it, irrespective of security mechanisms that may or may not be in place.

  Users electing to place information on digital media or removable storage devices or maintaining a separate database are advised by the IT Department only do so where such an action is in accord with the information's security classification. Users are consequently responsible in such situations for ensuring that appropriate access to the data are maintained in accord with the Information Security

  Policy and any other contractual obligations they may have to meet.

  Users are obligated to report instances of non-compliance to the RLM via the IT Helpdesk.

  Instances of non-compliance will be published on IT Unit's risk register and supplied to external auditors upon request.

- **Access Control Authorisation**

- **User accounts**

  Access to RLM IT resources and services will be given through the provision of a unique user account and complex password.

- **Staff User Accounts**

  Staff user accounts can only be requested in writing, and by using the appropriate forms, by departmental managers.

No access to any RLM staff IT resources and services will be provided without prior authentication and authorisation of a user's RLM account.

By default staff are provided with access to P: drive (with access denied to all other users), and an email account. They have access to a standard suite of software applications, the remote desktop and VPN services.

By default staff accounts will upon termination of contract, unless a request for an extension is received from the relevant Departmental Manager.

- **Third parties**

  Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles.

  The accounts will be removed at the end of the contract or when no longer required.

  Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.

- **Passwords**

  Password issuing, strength requirements, changing and control will be managed through formal processes.

  Password issuing will be managed by the IT Helpdesk.

  Password length, complexity and expiration times will be controlled through Windows Active Directory

  Group Policy Objects. The criteria for staff passwords is given at:

  http://100.100.200.15/intranet/documents/Password Policy and on the P: shared drive under ICT Policies.

  Password changing can be performed on RLM workstations, via the IT Helpdesk or the remote desktop.

- **Access to Confidential, Restricted and Internal Use information**

  Access to 'Confidential', 'Restricted' and 'Internal Use' information will be limited to authorised persons whose job responsibilities require it, as determined by law, contractual agreement or the Information Security Policy. The responsibility to implement access restrictions lies with the data and systems owners.

  Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within RLM's Active Directory domains and administered by the IT Unit.

  There are no restrictions on the access to 'Public' information.

- **Policies and guidelines for use of accounts**

  Users are expected to become familiar with and abide by RLM policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.

- **Access for remote users**

  Access for remote users shall be subject to authorization by the IT Unit and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.

- **Access Control Methods**

  Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Policy.

  Access control methods include explicit logon to devices, Windows share and file permissions to files and folders, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, RLM login rights, database access rights, encryption and other methods as necessary.

  Access control applies to all RLM-owned networks, servers, workstations, laptops, mobile devices and services run on behalf of RLM.

  Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within RLM's Active Directory domains.

- **Further Policies, Codes of Practice, Procedures and Guidelines**

  This policy sits beneath RLM's overarching Information Security Policy. Other supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on RLM's intranet. All staff and third parties authorised to access RLM's network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

  The below list of current policies is in no way authoritative and new policies will be published on the RLM's intranet as they become available.

  Associated polices:

  Information Security Policy, Password Policy, Change Management Policy and Physical Environmental Policy.

  Review and Development

  This policy shall be reviewed and updated regularly by the IT Steering Committee and an auditor external to IT Services as appropriate to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

  Additional regulations may be created to cover specific areas.

  IT Steering Committee comprises representatives from all relevant parts of the RLM. It shall oversee the creation of information security and subsidiary policies.

  The Information Security Officer will determine the appropriate levels of security measures applied to all new information systems.

CHAPTER11: IT PROCUREMENT POLICY

11.1 POLICY STATEMENT

This document is primarily intended for municipal staff involved in the procurement of ICT goods and services within all the municipality structures including the IT Unit.

In line with the Municipal Asset Management Policy and Municipal Procurement Policy.

11.2 **Categories of ICT Assets**

11.2.1 **Physical Assets**

a) User Workstations
    1. Desktop Computers
    2. Mobile or Portable Devices
    3. Portable Storage Devices
    4. Monitors
    5. Input Devices
    6. Pointing Devices
b) Printers, Copiers and multifunction machines
c) Scanners and Facsimile
d) Servers
e) Firewalls
f) Routers
g) Switches
h) Telephone equipment

11.2.2 **Logical Assets**

a) Off the shelve software and applications
b) Directorate specific software and applications
c) Core Business software and applications

11.2.3 **Background**

While all business units within the municipality have allocation of funds for ICT products and services for effective resourcing of the respective business units, there are a number of factors that require specific recognition including:

Standardisation of all ICT assets – Physical and Logical Assets

a) Seamless integration with a complex ICT environment
b) Need for informed choice on a range of delivery options
c) Municipality's outlay on ICT assets and services which provide leverage in supporting the municipality achieve its objective.
d) Ensure that ICT resources are managed effectively throughout their lifecycle
e) Ensure a continued utility, functionality, performance and value for money.

11.3 IT Asset Management Process

11.3.1 ICT Asset Acquisition

a) All the business units that require procuring ICT Assets, shall submit to the steering committee before submitting to specifications committee for approval.
b) The ICT Steering Committee shall recommend ICT Assets procurement, and shall do so in accordance with the Municipality's ICT Standard and Specification as set out in the Technology Architecture document.
c) Where there is no standard required and the asset has an impact on the enterprise architecture, then the head of the business unit shall consult with the IT head for recommendation and verification before procurement is instigated.
d) All the relevant ICT asset procurement requisition form shall the verified and approved by a mandated IT personnel before being approved by finance and Supply Chain personnel
e) Upon delivery at the municipal offices the order paper work and delivery notes shall be processed by procuring Unit/Directorate personnel and verified by the IT Unit to ensure that the equipment delivered matches the original order and that all items are in order.
f) All ICT assets shall have an asset tag will be provided then be recorded in the inventory register in accordance with Municipality's Asset Management Policy.

All ICT assets shall be installed in consultation with the IT Unit personnel and a technician will be assigned to that installation, he/she will complete the associated asset sheet and register maintained by the IT Unit.

CHAPTER12: COMPUTER USAGE POLICY

12.1 POLICY STATEMENT

- Users may not tamper with someone else's files or programmes
- No user may gain access, , with or without permission, to another user's password
- No unauthorized hardware may be attached to the computer network
- Activate the password protected screen lock when temporarily leaving the office
- When travelling by car, protect notebooks by locking them in the car boot when you travel.
- If your workstation or RLM confidential information is stolen or lost, you must report the loss to the IT Department and your manager as soon as the loss is discovered.
- No workstation may be moved to a new user or location without informing the IT Department.
- At the end of the workday always logoff/shutdown your workstation.
- Lock up all materials that contain RLM confidential information or take them with you
- Users may not copy or transfer any software provided by the Municipality
- No user may introduce any programme which is designed to damage or hinder the network
- No programmes may be entered onto the network
- Always use the physical locking cable if provided with your workstation
- All computer workstations must be on the domain at all times.
- All computer workstations must be protected with anti-virus software at all times.
- Workstations affected by virus should be removed from the domain immediately.

ENFORCEMENT

Any person who contravenes or fails to comply with the provision of this policy shall be guilty of an offence and shall, upon conviction be liable to-

- A fine or imprisonment for a period not exceeding six months or to such imprisonment without the option of a fine or to both such fines and such imprisonment and,

- In the case of a continuing offence, to an additional fine of an additional period of imprisonment of 10 days or to such additional imprisonment without the option of a fine or to both such additional fine and imprisonment for each day on which such offence is continued and,
- A further amount equal to any costs and expenses found by the court to have incurred by the municipality as a result of such contravention or failure.

IMPLEMENTATION OF THE POLICY

This policy shall be implemented once approved by council as part of the Rustenburg Local Municipality policies

AVAILABILITY OF THE POLICY

This Policy shall be freely available in hardcopy, electronically on the local shared (P:) drive and on the RLM intranet site

SHORT TITLE

This document shall be called Information and Communications Technology security policy of the Rustenburg Local Municipality.