Rustenburg Local Municipality

GROUP INFORMATION SECURITY POLICY

Version Control

Version	Date	Author(s)	Details
1 0			Group Information Securıty Policy

Approvals:

Authors by.	Mr. Phogole Marome Manager· Information Technology
Edited by:	Ms. Yondela Robojı Director: Corporate Support Servıces
Approved by:	Surname & Initials: ____________________ Designation: ________________________ Date·________________________

THE CONTENTS

1. INTRODUCTION

Group Information Security Policy is a set of rules enacted by the municipality to ensure that all users or networks of the IT structure within the municipal's domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the municipality stretches its authority

The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of the municipality Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for the municipality to recover.

This Group information security policy outlines Rustenburg Local Municipality's approach to information security management It provides the guiding principles and responsibilities necessary to safeguard the security of the municipality's information systems. Supporting ICT policies, codes of practice, procedures and guidelines provide further details RLM is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which the municipality is responsible

RLM is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract in accordance with the requirements of data security standard ISO 27001

Additionally, if RLM's proprietary information were tampered with or made unavailable, it could impair Municipality's ability to do business, which will affect all employees and other key stakeholders

The IT Unit is the guardian of the electronic and computer systems which all employees need to use to do their work, and as such, the IT Unit requires all employees to diligently protect information as appropriate for its sensitivity level

Failure by employees to comply with this policy may subject them to disciplinary measures and could ultimately result in termination of employment.

2. THE PURPOSE

The purpose of this policy are to:

a) Provide a framework for establishing suitable levels of information security for all RLM information systems (including but not limited to all Cloud environments commissioned or run by RLM, computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems

I This explicitly includes any ISO27001-certified Information Security Management Systems the School may run

II The resources required to manage such systems will be made available.

III. Continuous improvement of any MISS will be undertaken in accordance with POPI Act principles

b) Make certain that users are aware of and comply with all current and relevant South Africa legislations
c) Provide the principles by which a safe and secure information systems working environment can be established for staff, councilors and any other authorised users
d) Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle
e) Protect RLM from liability or damage through the misuse of its IT facilities
f) Maintain research data and other confidential information provided by suppliers at a *level of security commensurate with its classification, including upholding any legal and* contractual requirements around information security.
g) Respond to changes in the context of the organisation as appropriate, initiating a cycle of continuous improvement

3. TERMS AND DEFINITIONS

a. **RLM** refer to Rustenburg Local Municipality

b **IT** may refer to both Information Technology as well as the designated Unit

c. **Hardware** will refer to the CPU, printer, mouse, screen, consumer and third party technology (including, and without limitation mobile devices like phones, i-Pads, Tablets and any like devices) and all related equipment or peripherals required or installed by the Rustenburg Local Municipality to operate IT systems.

d. **Software** will refer to in-house developed as well as registered and the Rustenburg Local Municipality approved software packages as authorized and installed by the IT Unit.

e. **Staff members** will refer to any permanent, temporary or contract workers who are performing specific duties for RLM and are making use of computer equipment belonging to Rustenburg Local Municipality or themselves during the performance of those duties.

f **Databases** will encompass any and all Third Party or Proprietary Database Platforms, and any reports, printouts, exports or screen captures obtained from the said systems

g **Applications** refer to all front-end user interface systems, communicating with database management systems in the back-end

h **GDPR** *refer to General Data Protection Regulation of Protection of Personal* Information act as amended

i. **SLA** refers to Service Level Agreement.

4. SCOPE

4.1 This policy is applicable to, and will be communicated to, all staff, councilors, other key stakeholders and third parties who interact with information held by the RLM and the information systems used to store and process it.

This includes, but is not limited to: Cloud systems developed or commissioned by municipality, any systems or data attached to the RLM data or telephone networks, systems managed by the municipality, mobile devices used to connect to municipality networks or hold municipal data, data over which RLM holds the intellectual property rights, data over which RLM is the data controller or data processor, electronic communications sent from the municipality.

5. RESPONSIBILITIES

5.1 Director: Corporate Support Services

5 1 1 The Director· Corporate Support Services bears the responsibility of overseeing the development, approval, accountability and implementation of the Group Information Security Policy

5.2 Unit Manager: Information and Communication Technology

a) Shall be responsible for the development of the group information security policies and strategies, regulations, standards, norms, guidelines, best practices and procedures

b) Shall coordinate ICT Security with IT Security specialists.

c) Shall manage all the relationship within all stakeholders that supply information technology products and services, this is done by ensuring that all Business Agreements and SLAs are adhered to

d) Shall monitor and ensure compliance with relevant ICT regulatory framework and policies.

5.3 Information Security Specialist.

a) The Information Technology Security Specialist (ITSS) is primarily responsible for driving and maturing the information security management programme, including the Information Security Governance System (ISGS) within the municipality

b) The Information Technology Security Specialist is required to be approachable and accessible with regards to information security matters Internal and external parties are encouraged to inform the ITSS on information security issues, in order to ensure risks to the municipality can be appropriately identified, classified and managed Constructive suggestions or observations are welcome, and should also be communicated

c) Shall ensure that the IT Unit foresees the implementation of all ICT processes in the municipality

d) Shall ensure that the Group Information Security Policy conforms with Risk Management Plan.

e) Shall provide recommendation remedial actions to be taken to solve all ICT risks faced by the Municipality.

f) Shall identify ICT security risks.

g) Shall ensure that the Information Technology Unit complies with the Risk Management Framework of RLM.

5.4 Third Parties

5 4 1 Shall not be provided with access to the sensitive information unless security clearance is provided to security service

5 4 2 SLAs shall be signed by and between the municipality, third parties and contractors before providing any ICT services to the Municipality.

5.5 Municipal Employees

5 5 1 Shall ascertain and understand the sensitivity of information to which they have access through training, other resources or by consultation with their managers or the IT Service Desk

5 5 2 Shall not in any way divulge, copy, release, sell, loan, alter or destroy any information except as authorized by the appropriate manager within the scope of their professional activities

5 5 3 Shall adhere to the Municipality's requirements for any computers used to transact Rustenburg Local Municipality business regardless of the sensitivity level of the information held on that system.

5 5 4 Shall protect the confidentiality, integrity and availability of Rustenburg Local Municipality's information as appropriate for the information's sensitivity levels, wherever the information is located, e.g. held on physical documents, stored on computer media, communicated over voice or data networks and exchanged in conversation, etc.

5 5 5 Shall safeguard any physical key, ID card or computer/network account that allows them to access Rustenburg Local Municipality's information. This includes creating difficult-to-guess computer passwords

5 5.6 Shall destroy or render unusable any confidential or highly confidential information contained in any physical document (e g , memos, reports, microfilm) or any electronic, magnetic or optical storage medium (e g , USB key, CD, hard disk, magnetic tape) before it is discarded.

5 5 7 Shall report to their supervisors any activities that they suspect may compromise sensitive information

5 5 8 Their obligation to protect sensitive information continues after they leave Rustenburg Local Municipality premises or employment.

5.5.9 While many South African laws create exceptions allowing for the disclosure of confidential information in order to comply with investigative subpoenas, court orders and other compulsory requests from law enforcement agencies, upon receipt of such compulsory requests users should contact the Office of the Municipal Manager before taking any action

5 5 10 If a staff member is performing work in an office that handles information subject to specific security regulations, the staff member will be required to acknowledge that she or he has read, understood and agreed to comply with the terms of this policy

5.6 Managers and Supervisors

5 6 1 In addition to complying with the requirements listed above for all employees and contractors, managers and supervisors must

5.6.2 Ensure that departmental procedures support the objectives of confidentiality, integrity and availability defined by the IT Unit and designees, and that those procedures are followed

5.6.3 Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic

5 6.4 Ensure that each staff member understands his or her information security-related responsibilities.

5.7 Information Technology Unit

5 7.1 In addition to complying with the policy requirements defined for all employees, contractors, managers and supervisors, those who manage computing and network environments that are used to capture, store, process and/or transmit Rustenburg Local Municipality proprietary information, are responsible for ensuring that the requirements for confidentiality, integrity and availability are being satisfied within their environments

This includes the following.

5 7 1 1 Understanding the sensitivity level of the information that will be captured by, stored within, processed by, and/or transmitted through their technologies

5 7.1.2 Developing, implementing, operating and maintaining a secure technology environment that includes·

5 7 1 3 A comprehensive Password policy.

5.7.1.4 Product implementation and configuration standards.

5 7 1 5 Procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies Rustenburg Local Municipality's security requirements

5.7 1 6 An effective strategy that adheres to IT industry-accepted "best practices" for the technology for protecting information against generic threats and computer hackers

5 7 1 7 Ensuring that staff members understand the sensitivity levels of the data being handled and the appropriate measures used to secure it.

6. POLICY FRAMEWORK

In the interests of simplicity, all the Information technology policies and procedures relevant and applicable to Rustenburg Local Municipality have been condensed into a smaller set of documents to be reviewed and understood by all employees

6.1 IT Network End user IT Policies and Procedures

This document is applicable to all RLM employees It provides guidelines and procedures for completing any computer related tasks whilst in the employ of Rustenburg Local Municipality

The Document includes the following IT policies – applicable to all users on the IT systems

a. Firewall Policy
b Patch Management Policy

c Corporate Governance of Information Communication Technology Policy Framework
d. Disaster Recovery Plan Policy
e Backups Policy

6.2 Ownership and Classification of Information

6 2 1 Information generated, stored, displayed and transported utilising municipal resources belong to the Municipality and shall not be altered or disclosed without specific authorisation.

6 2 2 Information resources generated within the Municipality have a different degree of importance to the organisation. Information resources range from critical information that if destroyed or misused could have a direct impact on service delivery, to information that has no sensitivity

6 2 3 The different information resources of the Municipality must therefore be treated with appropriate care and be protected adequately to guard against misuse, destruction, inappropriate or wrongful access, *disclosure and changes. To this end, the Municipality uses a* classification scheme that classifies its information resources into four categories, namely Highly confidential, Restricted, Internally Confidential and Public.

6.2.4 This policy stipulates the criteria for the different information categories and it provides guidelines on how the user community as owners of these information resources shall treat them to ensure the right level of protection

6 2 5 It is the information users' responsibility to ensure that the information is treated appropriately based on their assessment of its categorisation.

6 2 6 It is the information users' responsibility to ensure that if information has changed in its classification e g. the information is no longer as sensitive, is subsequently reclassified and treated accordingly

6 2 7 Details of the information classification scheme are depicted in the table1 below

Information Category	Municipality Impact (of information being in the wrong hands)	Typical Information	User Responsibility & Treatment of Information
Highly Confidential	▪ Impacts on the image of the Municipality. ▪ Could result in substantial financial loss or litigation ▪ Could render the Municipality vulnerable to abuse.	▪ HR information ▪ Pre-adjudication tender information ▪ In-committee Council documentation. ▪ Audit reports that are highly confidential and contain sensitive information	▪ Only communicate within authorised group both internally & externally ▪ Only access, manipulate or change as per assigned rights and authorities ▪ Employ mechanisms and processes to ensure that information is accessed, changed, communicated or shared only as intended. ▪ Adhere to any other policy or job contract regulating access, change and communication of this type of information. ▪ Communicate any irregularities in the treatment of this type of information to the department head
Restricted	▪ Impacts on the image of the Municipality ▪ Could result in substantial financial loss or litigation ▪ Could render the Municipality vulnerable to abuse	▪ HR Information ▪ Sensitive financial information ▪ Audit reports that are restricted and contain sensitive information. ▪ Management Committee (MANCO) documentation. ▪ Contracts.	▪ Only communicate within authorised group both internally & externally ▪ Only access, manipulate or change as per assigned rights and authority ▪ Employ mechanisms and processes to ensure that information is accessed, changed and communicated only as intended ▪ Ensure protection mechanisms & processes are effective and efficient

Information Category	Municipality Impact (of information being in the wrong hands)	Typical Information	User Responsibility & Treatment of Information
			▪ Adhere to any other policy or job contract regulating access, change and communication of this type of information. ▪ Communicate any irregularities in the treatment of this type of information to the directorate head
Internally Confidential	▪ Cause embarrassment to the Municipality. ▪ Lesser Municipality impact.	▪ HR records ▪ Certain policies and procedures ▪ Confidential Audit findings	▪ Take sufficient care to access, change, communicate or share this type of information only as was intended. ▪ Communicate significant irregularities in the treatment of this type of information to your directorate head
Public	▪ Lesser Municipality impact	▪ Any information that is classified as public in terms of the Promotion of Access to Information Act (PAIA), municipal policies and standards.	▪ Take sufficient care to access, change, communicate or share information in this category only as was intended ▪ Communicate significant irregularities in the treatment of this type of information to your directorate

Table 1: Information Classification Scheme

6.3 Information Disclosure

6 3 1 During their service with the Municipality, employees retain proprietary information and knowledge

6.3.2 Present and former employees must guard against disclosing or using this information to the prejudice of the Municipality's interests.

6.3.3 The Municipality reserves the right to take action, including legal action, against present and former employees who disclose or use any proprietary information to the detriment of the Municipality.

6.4 Suppliers

All Municipality's suppliers will abide by RLM's group Information Security Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance.

This includes

a when accessing or processing RLM assets, whether on site or remotely

b. when subcontracting to other suppliers

6.5 PC and Electronic Device Acceptable Usage Policy

This policy governs the usage of any electronic device in use on any premises owned or rented by the Municipality, whilst in the employment of Rustenburg Local Municipality

The *policy provides summary guidelines regarding access to and disclosure of data on* any of the Rustenburg Local Municipality electronic communication systems, and will help users to better determine how to use these systems in light of their and the Municipality's privacy and security concerns

The Policy Document is applicable to all users of the IT systems, within the Rustenburg Local Municipality 's Information technology network operations

6.6 Municipal and Contractor Policies and Procedures

This policy document describes the roles and responsibilities of any member of Rustenburg Local Municipality, IT support team and any contractor who may be appointed to assist with the efficient operation of the IT systems at Rustenburg Local Municipality

The document includes the following IT Policies

a. Backups Policy

b Password Policy

c User Change Management Policy and Procedure

d. Firewall Policy

e. IT Service Desk Management Policy and Procedure

The Policy Document is applicable to all users of the IT systems within the municipality 's area of operations

6.7 Contractor Confidentiality and non-Disclosure Agreement

A standard document specifying the responsibilities of any contractor providing outsourced IT services to Rustenburg Local Municipality

This Policy document is applicable to and must be completed by IT Contractors, temporary staff and visitors into the Server rooms at the various Rustenburg Local Municipality sites.

7. 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.

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

8. GOVERNING PRINCIPLES

a) The RLM Council is accountable for information security and delegates the authority to the Senior Management 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 policy, standards, processes and procedures shall not contravene the principles and practices contained in the Group Information Security Policy, except where the requirements of the other RLM Policies has been adhered to

e) Governing principles and practices in the Group 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 adopting a reactive approach 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.

9. Policy Review and Maintenance

The Policy shall be reviewed and updated after 24 months after council approval, or as a needed arises, to ensure that the policy remains aligned with changes to relevant laws, policies, contractual obligations and best practice

Annexure A: Privacy Waiver, Monitoring and Interception of Electronic Communications Notice and Acknowledgement of Understanding.

PRIVACY WAIVER

Users are given access to ICT resources (computers, software, printers, email, internet access, other ICT devices etc.) to assist them in the performance of their job functions Users should have no expectation of privacy in anything they create, store, send or receive using the Municipality's information and communications technologies equipment The computer network is the property of the Municipality and is used to conduct municipal business. Users expressly waive any right of privacy in anything they create, store, send or receive using the municipal computer equipment, software or email and Internet system and all ICT devices Users consent to allow management to access and review all materials created, stored, sent or received through any Municipality network or internet connection.

MONITORING AND INTERCEPTION OF ELECTRONIC COMMUNICATIONS

The Municipality has the right to monitor and log any and all aspects of its network including, but not limited to, monitoring email sent and received by users, monitoring chat and newsgroups, monitoring file downloads, and internet usage by users

ACKNOWLEDGEMENT OF UNDERSTANDING

I have read and agree to comply with the terms of this policy governing the use of ICT facilities owned, leased, hired or otherwise provided by Rustenburg Local Municipality, ICT facilities connected directly or remotely to Rustenburg Local Municipality's network or ICT facilities, and ICT facilities used on Rustenburg Local Municipality 's premises

I understand that violation of this policy may result in disciplinary action, including possible termination and civil and criminal penalties

---------------------------------- ---------------------------------------

User name Signed

---------------------------------- ---------------------------------------

Employee no *Date*