RISK AND SECURITY DEPARTMENT	Doc Nr	
SECURITY MANAGEMENT POLICY	Version	
	Issue Date	30 June 2025
	Next Review Date	30 June 2026

SECURITY MANAGEMENT POLICY

Signatories The signatories hereof, confirm acceptance of the contents, recommendation, and adoption hereof.			
TITLE	**SECURITY MANAGEMENT POLICY**		
APPROVED DATE		**PAGES**	26
EFFECTIVE DATE		**REVIEW DATE**	
ROLE	**DESIGNATION**	**OFFICIAL/MEMBER**	**SIGNATURES**
INITIATED BY	Manager: Risk and Security	LG Davhana	
RECOMMENDED BY	Municipal Manager		
APPROVED BY	Council		
CUSTODIAN OF THE POLICY	Manager: Risk and Security	LG Davhana	

DOCUMENT CONTROL PAGE				
Document title	SECURITY MANAGEMENT POLICY			
Creation date	MAY 2025			
Effective date				
Status	Draft		Final	
Version	0.1			
Author title, name and contact details	Manager: Risk and Security Email: davhanalg@thulamela.gov.za Telephone:			
Owner title, name and contact details	Manager: Risk and Security Email: davhanalg@thulamela.gov.za Telephone:			
Distribution	• Council • Accounting Authority and Committees • Municipal Officials • Relevant Stakeholders			
Classification	Restricted	N/A	Confidential	N/A
Revision	**Version Number**	**Revision Date**	**Revision Details**	**Revised by**
Review History				

INDEX

1. DEFINITIONS AND ACRONYMS

1.1 Statutory and Regulatory

This Procedure applies to the following meanings and interpretations:

#	TERM	DESCRIPTION
1.1	Candidate	Means an applicant, an employee, a contract employee or a person acting on behalf of a contract appointee or independent contractor
1.2	Accreditation	Means the official authorisation by management for the operation of an Information Technology (IT) system, and acceptance by that management of the associated residual risk. Accreditation is based on the certification process as well as other management considerations
1.3	Assets	Means material and immaterial property of an organisation. Assets include but are not limited to information in all forms and stored on any media, networks or systems, or material, real property, financial resources, employee trust, public confidence, public confidence and international reputation
1.4	Availability	Means the condition of being usable on demand to support operations, programmes and services
1.5	Business continuity planning	Includes the development of plans, measures, procedures and arrangements to ensure minimal or no interruption of the availability of critical services and assets
1.6	Certification	Means the issuing of a certificate certifying that a comprehensive evaluation of the system (hereinafter referred to as an "ICT" system) and its related safeguards has been undertaken and that it was established and its design and implementation meets a specific set of security requirements
1.7	COMSEC	Means the organ of the state known as Electronic Communications Security (Pty) Ltd, which was established in terms of section 2 of the Electronic Communication Security Act,2002 (Act 68 of 2002) and, until such time as COMSEC becomes operational, the South African Communication Security Agency
1.8	Critical services	Means a service identified by an institution as a critical service through a Threat and Risk Assessment and the compromise of which will endanger the effective functioning of the institution
1.9	Document	Means any note or writing, whether produced by hand or printing, typewriting or any other similar process, in either tangible or electronic format; Any copy, plan, picture, sketch or photographic or other representation of any place or article; Any disc, tape, card, perforated roll or

#	TERM	DESCRIPTION
		other device in or on which sound or any signal has been recorded for reproduction
1.10	National intelligence structures	Means the National Intelligence Structures as defined in the section 1 of the National Intelligence Strategic Intelligence Act, Act 39 of 1994
1.11	Reliability check	Means an investigation into the criminal record, credit record and past performance of an individual or private organ of the state to determine his, her or its reliability
1.12	Risk	Means the likelihood of a threat materialising by exploitation of a vulnerability
1.13	Screen investigator	Means a staff member of a National Intelligence Structure designated by the head of the relevant National Intelligence Structure to conduct security clearance investigations
1.14	Security breach	Means negligent or intentional transgression of or failure to comply with security measures
1.15	Technical Surveillance Countermeasures (TSCM)	Means the process involved in the detection, localisation, identification and neutralisation of the technical surveillance of an individual, an organ of state, facility or vehicle
1.16	Technical/ electronic surveillance	Mean interception or monitoring of sensitive or proprietary information or activities (also referred to as "bugging")
1.17	Threats	Means any potential event or act, deliberate or accidental, that could cause injury to persons, compromise the integrity of information or could cause the loss or damage to assets
1.18	Threat Risk Assessment (TRA)	Means, within the context of security risk management, the process through which it is determined when to avoid, reduce and accept risk, as well as how to diminish the potential impact of a threatening event
1.19	Vulnerability	Means a deficiency related to security that could permit a threat to materialise

1.2 ACRONYMS

#	TERM	DESCRIPTION
1.2.1	ICT	Information and Communication Technology
1.2.2	BCP	Business Continuity Management Planning
1.2.3	TRA	Threat and Risk Assessment
1.2.4	CRO	Chief Risk Officer

#	TERM	DESCRIPTION
1.2.5	NIA	National Intelligence Agency
1.2.6	PMT	Political Management Team
1.2.7	SSA	Security Services Agency
1.2.8	TSCM	Technical Surveillance Counter Measures
1.2.9	Municipality	Thulamela Local Municipality

2. POLICY STATEMENT

2.1 Security is an essential part of every organization; therefore, the municipality is committed to an effective, efficient and comprehensive security management program that ensures safety of the organization, as result its personnel and assets and cannot be overlooked. A security management policy is the primary way in which management's expectations for security management are translated into specific and measurable goals and objectives.

2.2 On the contrary, if municipality does not have security policy that defines and communicate those aims and objectives, then municipality will not operate at its efficiency, therefore this will compromise the existence of municipality.

2.3 The municipality must be protected against identified threats according to baseline security requirements and continuous security risk management.

2.4 Information and assets of the municipality must be protected according to baseline security requirements and continuous security risk management.

2.5 Continued delivery of services of the municipality must be assured through baseline security requirements, including business continuity planning, and continuous security risk management.

3. PREAMBLE

3.1 The Municipality depends on its personnel, information, and assets to deliver services that ensure the health, safety, security and economic wellbeing of its residents. It must therefore manage these resources with due diligence and take appropriate measures to protect them.

3.2 Threats that can cause harm to the municipality, that can be found in South Africa and abroad, includes acts of terror and sabotage, espionage, unauthorised access to buildings and premises, theft, armed robbery, fraud and corruption, vandalism, fire, natural disasters, technical failures and accidental damage. The threat of cyberattack and malicious activity through the Internet is prevalent and can cause severe harm to electronic services and critical infrastructure. Threats to national interest, such as transnational criminal activity, foreign intelligence activities and terrorism, continue to evolve as the result of changes in the international environment.

4. PURPOSE

4.1 This policy prescribes the application of security measures to reduce the risk of harm that can be caused to the institution if the above threats should materialise. It has been designed to protect employees, preserve the confidentiality, integrity, availability and value of information and assets, and assure the continued delivery of services.

4.2 Since the municipality relies extensively on information and communication technology (ICT) to provide its services, this policy emphasises the need for acceptable use of ICT equipment as well as ICT protection measures to be complied with by all employees.

5. OBJECTIVES

5.1 The main objective of this policy therefore is to support the regional interest and the municipality's business objectives by protecting employees, information and assets and assuring the continued delivery of services.

5.2 To ensure that confidentiality, integrity of the municipality assets and sensitive information is maintained and protected/safeguarded from unauthorised access, disclosure and theft.

5.3 To identify, assess and mitigate security risks that minimize potential impact to the municipality.

5.4 To ensure compliance with relevant security regulations, laws and industry standards.

6. SCOPE

This policy applies to the following individuals and entities:

6.1 All employees of the municipality;

6.2 All contractors and consultants delivering service to the municipality including their employees who may interact with the municipality;

6.3 Temporary employees of the municipality;

6.4 All information assets of the municipality.

6.5 All intellectual properties of the municipality;

6.6 All fixed property that is owned or leased by the municipality; and

6.7 All moveable property that is owned or leased by the municipality.

6.8 The policy further covers the following seven elements of the security program:

6.8.1. Security organisation

6.8.2. Security administration

6.8.3. Information security

6.8.4. Physical security

6.8.5. Personnel security

6.8.6. Information and Communication Technology (ICT) security

6.8.7. Business Continuity Management Planning (BCP)

7. COMPLIANCE REQUIREMENTS

7.1 All individuals mentioned in par. 6 above must comply with the baseline requirements of this policy and its associated Security Directives as contained in the Security Plan of the municipality. These requirements shall be based on the integrated security Threat and Risk Assessments (TRA's) of SDM as per the national interest as well as employees, information, and assets of the municipality. The necessity of security measures above baseline levels will also be determined by the continual updating of the security TRA's.

7.2 Security threat and risk assessments involve:

7.2.1 Establishing the scope of the assessment and identifying the information, employees and assets to be protected;

7.2.2 determining the threats to information, employees and assets of the municipality and assessing the probability and impact of the threat occurrence;

7.2.3 assessing the risk based on the adequacy of the existing security measures and vulnerabilities;

7.2.4 implementing any supplementary security measures that will reduce the risk to an acceptable level.

7.3 Staff accountability and acceptable use of assets:

7.3.1 The Municipal Manager of the municipality shall ensure that information and assets of the municipality are used in accordance with procedures as stipulated in the Security Directives as contained in the Security Plan of the municipality.

7.3.2 All employees of the municipality shall be accountable for the proper utilisation and protection of such information and assets. Employees that misuse or abuse assets of the municipality shall be held accountable therefore and disciplinary action shall be taken against any such employee.

8. SPECIFIC BASELINE REQUIREMENTS

8.1 Security organisation

8.1.1 Municipal Manager has appointed a Chief Risk Officer (CRO) to establish and direct a security program that ensures coordination of all policy functions and implementation of policy requirements.

8.1.2 Given the importance of this role, a CRO with sufficient experience and training who is strategically positioned within Thulamela local municipality to provide institution –wide strategic advice and guidance to council has been appointed.

8.1.3 The Municipal Manager will ensure that the CRO has an effective support structure (security component) to fulfil the functions referred to in para 8.1.2 below.

8.1.4 Individuals that will be appointed in the support structure of the CRO will all be risk management professionals with sufficient security experience and training to effectively cope with their respective job functions.

8.2 Security administration

8.2.1 The functions referred to in para. 8.1 above include:

8.2.1.1 General security administration (departmental directives and procedures, training and awareness, security risk management, security audits, sharing of information and assets);

8.2.1.2 setting of access limitations;

8.2.1.3 administration of security screening;

8.2.1.4 implementing physical security;

8.2.1.5 ensuring the protection of employees;

8.2.1.6 ensuring the protection of information;

8.2.1.7 ensuring ICT security;

8.2.1.8 ensuring security in emergency and increased threat situations;

8.2.1.9 facilitating business continuity planning;

8.2.1.10 ensuring security in contracting; and

8.2.1.11 facilitating security breach reporting and investigations.

8.3 Security incident /breaches reporting process

8.3.1 Wherever an employee of the municipality becomes aware of an incident that might constitute a security breach of an unauthorised disclosure of information (whether accidentally or intentionally), he/she shall report that to the CRO of The municipality by utilising the formal reporting procedure prescribed in the Security Breach Directive of the municipality.

8.3.2 The Municipal Manager shall report to the appropriate authority (as indicated in the Security Breach Directive of the municipality all cases or suspected cases of security breaches, for investigation

8.3.3 The CRO shall ensure that all employees are informed about the procedure for reporting security breaches.

8.3.4 Security incident/breaches response process

8.3.5 The CRO shall develop and implement security breach response mechanisms for The municipality to address all security breaches/alleged breaches which are reported.

8.3.6 The CRO shall ensure that the Municipal Manager is advised of such incidents as soon as possible.

8.3.7 It shall be the responsibility of the National Intelligence Agency (e.g. NIA/SSA or SAPS) to conduct an investigation on reported security breaches and provide feedback with recommendations to the municipality.

8.3.8 Access privileges to classified information, assets and/or to premises may be suspended by the Municipal Manager of the municipality until administrative, disciplinary and /or criminal processes have been concluded, flowing from investigations into security breaches or alleged security breaches.

8.3.9 The end result of the investigations, disciplinary action or criminal prosecutions may be taken into consideration by the Municipal Manager in determining whether to restore, or limit, the security access privileges of an individual or whether to revoke or later the security clearance of the individual.

9 INFORMATION SECURITY

9.1 Categorisation of information and information classification system

9.2 The CRO must ensure that a comprehensive information classification system is developed for and implemented in the municipality. All sensitive information produced or processed by the municipality must be identified, categorised, and classified according to the origin of its source and contents and according to its security sensitivity to loss or disclosure.

10 PHYSICAL SECURITY

10.1 Physical security involves the proper layout and design of facilities of the municipality and the use of physical security measures to delay and prevent unauthorised access to assets of the municipality. It includes measures to detect attempted or actual unauthorised access and the activation of an appropriate response. Physical security also includes the provision of measures to protect employees from bodily harm.

10.2 Physical security measures must be developed, implemented and maintained in order to ensure that the entire institution, its personnel/officials, property and information are secured. Application of physical security measures shall be at the discretion of the security officer for members of the Political Management Team (PMT) i.e. the Mayor, the Speaker and the Whip of Council. These security measures shall be based on the findings of the Threat Risk Assessment (TRA) to be conducted by the CRO.

10.3 The municipality shall ensure that physical security is fully integrated early into the process of planning, selecting, designing, and modifying of its facilities. The municipality shall:

10.3.1 select, design and modify facilities in order to facilitate the effective control of access thereto;

10.3.2 demarcate restricted access areas and have the necessary entry barriers, security systems and equipment to effectively control access thereto;

10.3.3 include the necessary security specifications in planning, request for proposals and tender documentation;

10.3.4 incorporate related costs in funding requirements for the implementation of the above.

10.4 The municipality will also ensure the implementation of appropriate physical measures for the secure storage, transmittal, and disposal of classified and protected information in all the times.

10.5 All employees are required to always comply with access control procedures of The municipality. This includes the producing of ID cards (only if in use) upon entering any

sites of the municipality, the display thereof whilst on the premises and the escorting of official visitors.

11 PERSONNEL SECURITY

SECURITY SCREENING

11.1 All employees, contractors and consultants of the municipality, who require access to classified information and critical assets in order to perform his/her duties or functions, must be subjected to a security screening investigation conducted by the former National Intelligence Agency (NIA) and currently Security Services Agency (SSA) in order to be granted a security clearance at the appropriate level.

11.2 The level of security clearance given to a person will be determined by the content of or access to classified information entailed by the post already occupied or to be occupied in accordance with their respective responsibilities and accountability.

11.3 A security clearance provides access to classified information subject to the need-to-know principle.

11.4 A declaration of secrecy shall be signed by every individual issued with a security clearance to complement the entire security screening process. This will remain valid even after the individual has terminated his/her services with the municipality.

11.5 A security clearance will be valid for a period of ten years in respect of the Confidential level and five years for Secret and Top Secret. This does not preclude re-screening on a more frequent basis as determined by the Council and the Municipal Manager of the municipality, based on information which impact negatively on an individual's security competence.

11.6 Security clearance in respect of all individuals who have terminated their services with the municipality, shall be immediately withdrawn.

12 SECURITY AWARENESS AND TRAINING

12.1 A security training and awareness program must be developed by the Chief Risk Officer and implemented to effectively ensure that all personnel and service providers of the municipality remain security conscious.

12.2 All employees shall be subjected to the security awareness and training programs and must certify that the contents of the program(s) have been understood and will be complied with. The program must cover/covers training regarding specific security responsibilities and sensitise employees and relevant contractors and consultants about the security policy and security measures of the municipality and the need to protect sensitive information against disclosure, loss, or destruction.

12.3 Periodic security awareness presentations, briefings and workshops will be conducted as well as posters and pamphlets frequently distributed to enhance the training and awareness campaign program. Attendance of the above programs is compulsory for all employees identified and notified to attend the events.

12.4 Regular surveys and walkthrough inspections shall be conducted by the Chief Risk Officer and members of the security component to monitor the effectiveness of the security training and awareness program.

13 INFORMATION AND COMMUNICATION TECHNOLOGY

IT SECURITY

13.1 A secure network shall be established for the municipality to ensure that information systems are secured against rapidly evolving threats that have the potential to impact on their confidentiality, integrity, availability, intended use and value.

13.2 To prevent the compromise of the IT systems, the municipality shall implement baseline security controls and any additional control identified through the security TRA. These controls, and the security roles and responsibilities of all personnel, shall be clearly defined, documented, and communicated to all employees.

13.3 To ensure policy compliance, the IT Manager of the municipality shall:

13.3.1 Certify that all systems are secure after procurement, accredit IT systems prior to operation and comply with minimum security standards and directives;

13.3.2 Conduct periodic security evaluations of systems, including assessments of configuration changes conducted on routine basis;

13.3.3 Periodically request assistance, review, and audits from the former National Intelligence Agency (NIA), and the current SSA to get an independent assessment.

13.4 Server rooms and other related security zones where IT equipment are kept shall be secured with adequate physical security measures and strict access controls shall be enforced and monitored.

13.5 Access to the resources and the network of the municipality shall be strictly controlled to prevent unauthorised access. Access to all computing and information systems and peripherals of the municipality shall be restricted unless explicitly authorised.

13.6 Systems hardware, operating and application software, the network and communication systems of the municipality shall all be adequately configured and safeguarded against both physical attack and unauthorised network intrusion.

13.7 All employees shall make use of IT systems of the municipality in an acceptable manner and for business purposes only. All employees shall comply with the IT Security Directives in this regard at all times.

13.8 The selection of passwords, their use and management as primary means to control access to systems is to strictly adhere to best practice guidelines as reflected in the IT Security Directives. In particular, passwords shall not be shared with any other person for any reason.

13.9 To ensure the ongoing availability of critical services, the municipality shall develop IT Continuity plans as part of its overall Business Continuity Planning (BCP) and recovery activities.

Internet Access

13.10 The IT Manager of the municipality, having the overall responsibility for setting up internet access for the municipality, shall ensure that the network of the municipality is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall. Human Resources management shall ensure that all personnel with internet access (including e-mail) are aware of, and will comply with, an acceptable code of conduct in their usage of the Internet.

13.11 The IT Manager of the municipality shall be responsible for controlling user access to the Internet, as well as for ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security breaches and incidents.

13.12 Incoming e-mail must be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible computer viruses or other malicious code.

USE OF LAPTOP COMPUTERS

13.13 Usage of laptop computers by employees of the municipality is restricted to business purposes only, and users shall be aware of, and accept the terms and conditions of use, especially the responsibility for the security of information held on such devices.

13.14 The information stored on a laptop computer of the municipality shall be suitably always protected, in line with the protection measures prescribed in the IT Security Directive.

13.15 Employees shall also be responsible for always implementing the appropriate security measures for the physical protection of laptop computers, in line with the protection measures prescribed in the IT Security Directive.

COMMUNICATION SECURITY

13.16 The application of appropriate security measures shall be instituted to always protect all sensitive and confidential communication of the municipality in all its forms.

13.17 All sensitive electronic communications by employees, contractors or employees of the municipality must be encrypted in accordance with COMSEC standards and the Communication Security Directive of the municipality. Encryption devices shall only be purchased from COMSEC and will not be purchased from commercial suppliers.

13.18 Access to communication security equipment of the municipality and the handling of information transmitted and/or received by such equipment, shall be restricted to authorised personnel only (personnel with Top Secret) Clearance who successfully completed the COMSEC Course.

TECHNICAL SURVEILLANCE MEASURES (TSCM)

13.19 All offices, meeting, conference, and boardroom venues of the municipality where sensitive and classified matters are discussed on a regular basis shall be identified and shall be subjected to proper and effective physical security and access control measures. Periodic electronic Technical Surveillance Counter Measures (sweeping) will be conducted to ensure that these areas are kept sterile and secure.

13.20 The Chief Risk Officer of the municipality shall ensure that areas that are utilised for discussions of sensitive nature as well as offices or rooms that house electronic communication equipment, are physically secured in accordance with the standards laid down by the former NIA, and the current SSA in order to support sterility the environment after a TSCM examination, before any request or a TSCM examination is submitted.

13.21 No unauthorised electronic device shall be allowed in any boardrooms and conference facilities where sensitive information of the municipality is discussed. Authorisation of such must first be obtained from the Chief Risk Officer.

BUSINESS CONTINUITY PLANNING (BCP)

13.22 The Chief Risk Officer of the municipality must establish a Business Continuity Plan (BCP) to provide for the continued availability of critical services, information, and assets if a threat materialises and to provide for appropriate steps and procedures to respond to an emergency to ensure the safety of employees, contractors, and visitors.

13.23 The BCP shall be periodically tested to ensure that the management and employees of the municipality understand how it is to be executed.

13.24 All employees of the municipality shall be made aware and trained on the content of the BCP to ensure understanding of their own respective roles in terms thereof.

13.25 The Business Continuity plan shall be kept up to date and re-tested periodically by the IT Manager.

14 IMPLEMENTATION: ROLES AND RESONSIBLITIES

14.1 HEAD OF INSTITUTION

14.1.1 The Municipal Manager of the municipality bears the overall responsibility for implementing and enforcing the security program of the municipality.

14.1.2 Towards the execution of this responsibility, the Municipal Manager shall:

14.1.2.1 Establish the post of a Chief Risk Officer and appoint a well-trained and competent official in the post;

14.1.2.2 Establish a security committee for the institution and ensure the participation of all senior management members of all the core business functions of the municipality in the activities of the committee;

14.1.2.3 Approve and ensure compliance with this policy and its associated Security Directives by all it is applicable to.

14.2 CHIEF RISK OFFICER

14.2.1 The delegated security responsibility lies with the Chief Risk Officer of the municipality who will be responsible for the execution of the entire security function and program within the municipality (coordination, planning, implementing, controlling, etc). Towards execution of his/her responsibilities, the Chief Risk Officer shall, amongst others:

14.2.1.1 chair the security committee of the municipality;

14.2.1.2 draft the internal Security plan (containing the specific and detailed Security Directives) of the municipality in conjunction with the security committee;

14.2.1.3 review the Security Policy and Security Plan at regular intervals;

14.2.1.4 conduct a security TRA of the municipality with the assistance of the security committee;

14.2.1.5 advise management on the security implications of management decisions;

14.2.1.6 implement a security awareness program;

14.2.1.7 conduct internal compliance audits inspections at the municipality at regular intervals;

14.2.1.8 establish a good working relationship with both NIA and SAPS and liaise with these institutions on a regular basis.

14.2.1.9 Manages the safeguarding of all accesses and keys at the municipality.

14.2.2 The Chief Risk Officer of the municipality must manage the implementation process of this policy and its associated Security Directives (contained in the Security Plan) by means of an action plan (also to be included in the Security Plan of the municipality.

14.3 SECURITY COMMITTEE

14.3.1 The Security Committee referred to in par. 14.1.1 above shall consist of senior managers of the municipality representing all the main business units of the municipality.

14.3.2 Participation in the activities of the Security Committee by the appointed representatives of business units of the municipality shall be compulsory.

14.3.3 The Security Committee of the municipality shall be responsible for, amongst others:

14.3.3.1 assisting the Chief Risk Officer in the execution of all security related responsibilities at the municipality, including completing tasks such as drafting/reviewing of the Security Policy and Plan, conducting of security audits, drafting of a Business Continuity Plan (BCP) and assisting with security awareness and training.

14.4 Line Management

14.4.1 All managers of the municipality departments must ensure that their subordinates comply with this policy and the Security Directives as always contained in the Security Plan of the municipality.

14.4.2 Managers must ensure that appropriate measures are implemented, and steps are taken immediately to rectify any non-compliance issues that may come to their attention. This includes the taking of disciplinary action against employees if warranted.

14.5 Employees, Consultants, Contractors, and other Service Providers

14.5.1 Every employee, consultant, contractor, and other service providers of the municipality shall know what their security responsibilities are, accept it as part of their normal job function, and not only cooperate but contribute to improving and maintaining security at the municipality at all times.

15 ENFORCEMENT

15.1 All employees of the municipality are required to fully comply with this policy and its associated Security Directives as contained in the Security Plan.

15.2 Prescripts to ensure compliance to this policy and the Security Directives by all consultants, contractors or service providers of the municipality shall be included in the contracts signed with such individuals/institutions/companies. The consequences of any transgression/deviation or non-compliance shall be clearly stipulated in said contracts and shall be strictly enforced. Such consequences may include the payment of prescribed penalties or termination of the contract, depending on the nature of any non-compliance.

16 EXCEPTIONS

16.1 Deviations from this policy and its associated Security Directives will only be permitted in the following circumstances:

16.1.1 When security must be breached in order to save or protected the lives of people;

16.1.2 During unavoidable emergency circumstances e.g. natural disasters;

16.1.3 On written permission of the Municipal Manager of the municipality (reasons for allowing non-compliance to one or more aspects of the policy and directives shall be clearly stated in such permission; no blanket non-compliance shall be allowed under any circumstances).

17 OTHER CONSIDERATIONS

The following shall be taken into consideration when implementing this policy:

17.1 Occupational Health and Safety issues in the municipality;

17.2 Disaster management at the municipality;

17.3 Persons with disability shall not be inconvenienced by physical security measures and must be catered for in such a manner that they have access without compromising security or the integrity of this policy.

17.4 Environmental issues as prescribed and regulated in relevant legislation (e.g. when implementing physical security measures that may impact on the environment).

18 LEGISLATIVE AND REGULATORY FRAMEWORK

This policy is informed by and complies with applicable national legislation; national security policies and national security standards documents in this regard are as follows:

18.1 Constitution Act of South Africa, 1996 (Act 108 of 1996)

18.2 Protection of Information Act, 1982 (Act no 84 of 19820

18.3 Promotion of Access to Information Act, 2000 (Act no 2 of 2000)

18.4 Copyright Act, 1978 (Act no 98 of 1978)

18.5 National Archives of South Africa Act, 1996 (Act no 43 of 1996) and regulations

18.6 Public Service Act ,1994 (Act no 103 of 1994) and regulations

18.7 Occupational Health and Safety Act, 1993 (Act no 85 of 1993)

18.8 Criminal Procedure Act,1977 (Act 51 of 1977), as amended

18.9 Private Security Industry Regulations Act,2001(Act 56 of 2001)

18.10 Control of Access to Public Premises and Vehicles Act, 1985 (Act 53 of 1985)

18.11 National Key Points Act, 1980 (Acct 102 of 1980)

18.12 Trespass Act,1959 (Act 6 of 1959)

18.13 Electronic Communication and Transaction Act,2002 (Act 25 of 2002)

18.14 Electronic Communication Security (PTY) Ltd Act,2002 (Act 68 of 2002)

18.15 State Information Technology Agency Act,1998 (Act 88 of 1998)

18.16 Regulation of Interception of Communications and Provision of Communication Related Information Act,2002 (Act 70 of 2002)

18.17 General Intelligence Law Amendment Act ,2000 (Act 66 of 2000)

18.18 Intelligence Service Act,2002 (Act 65 of 2002) and regulations

18.19 National Strategic Intelligence Act,1994 (Act 39 of 1994)

18.20 Intelligence Services Control Act, 1994 (Act 40 of 1994)

18.21 Labour Relations Act, 1995 (Act 66 of 1995)

18.22 Employment Equity Act, 1998 (Act 55 of 1998)

18.23 Occupational and Safety Act,1993, (Act 83 of 19930

18.24 Fire-arms Control Act, 2000 (Act 60 of 2000) and regulations

18.25 Non-Proliferation of Weapons of Mass Destruction Act, 1993 (Act 87 of 1993)

18.26 Protection of Constitutional Democracy Against Terrorism and Related Activities Act, 2004 (Act 33 of 20040

18.27 National Building Regulations and Building Standards Act, 1977 (Act 103 of 1977)

18.28 Protected Disclosure Act,2000 (Act 26 of 2000)

18.29 Intimidation Act, 1982 (Act 72 of 1982)

18.30 Prevention and Combating of Corrupt Activities Act, 2004 (Act 12 of 2004)

18.31 Minimum Information Security Standards (MISS), Second Edition March 1998

18.32 White paper on Intelligence (1995)

18.33 SACSA/090/1(4) Communication Security in the RSA

18.34 NIA Guidance Documents: ICT Policy and Standards: Part 1& 2

18.35 ISO 17799

18.36 National Building Regulations

19 EFFECTIVE AND REVIEW DATE

19.1 This policy shall be reviewed on an annual basis or as and when the needs arise

20 MONITORING AND EVALUATION

20.1 The Chief Risk Officer, with the assistance of the security component and security committee of the municipality must ensure compliance with this policy and its associated Security Directives by means of conducting internal security audits and inspections on a frequent basis.

20.2 The findings of the said audits and inspections shall be reported to the Municipal Manager of the municipality forthwith after completion thereof.

21 DISCIPINARY ACTION

21.1 Non-compliance with this policy and its associated Security Directives shall result in disciplinary action which may include, but not limited to:

21.1.1 Re-training;

21.1.2 Verbal and written warnings;

21.1.3 Termination of contacts in the case of contractors, consultants or any other service provider delivering a service to The municipality.

21.1.4 Dismissal;

21.1.5 Suspension;

21.1.6 Loss of The municipality information and asset resources;

21.1.7 Loss of access to certain privileges.

21.2 Any disciplinary action taken in terms of non-compliance with this policy and its associated directives will be in accordance with the disciplinary code/directive of the municipality.

22 CONCLUSION

22.1 The policy outlines and addresses critical matters raised in the purpose and the objectives. The provisions in the policy contents highlights the need for the municipality to adhere to the key issues narrated which will address challenges encountered and lead to effective and efficient implementation of the policy.

22.2 The Municipality commits to make resources available, monitor and evaluate the effectiveness of the policy, thus encouraging all relevant stakeholders to familiarise themselves with the policy.

22.3 Non-adherence/ compliance/ Breaching of the policy security Management policy will neither be acceptable nor condoned by the municipality.

23 ANNEXURES

23.1 Business Process Map

23.2 Standard Operating Procedure

Private Bag X5066
Thohoyandou
0952
Limpopo Province
Tel: 015 962 7500
Fax: 015 962 4020

THULAMELA MUNICIPALITY

EXTRACT RESOLUTION OF THULAMELA MUNICIPALITY SPECIAL COUNCIL MEETING NO. 07/2025 HELD ON THE 30TH OF JUNE 2025.

RESOLUTION NO. SC 07/06/2025

SUBMISSION OF THE RISK MANAGEMENT RELATED POLICIES FOR 2025/26 FINANCIAL YEAR.

Council resolved:

a) To approve the Risk Management related policies for 2025/26 financial year and,

b) To note risk management related strategies and plans for 2025/26 financial year.

.....
CHAIRPERSON OF COUNCIL
30 JUNE 2025

LIST OF POLICIES

RISK AND SECURITY DEPARTMENT (30June2025-30 June2026)

1. Security management Policy.
2. Anti-Fraud and Corruption Policy.
3. Whistle blowing Policy.
4. Risk management Policy.