



LIMPOPO

PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

**DEPARTMENT OF
ECONOMIC DEVELOPMENT, ENVIRONMENT & TOURISM**

SECURITY POLICY

2020

TABLE OF CONTENTS

No	Contents	Pages
1.	Acronyms	3
2.	Definitions	3
3.	Introduction	7
4.	Background	7
5.	Purpose and objectives	7
6.	Authority of the policy	8
7.	Scope of application	8
8.	Principles	8
9.	Legal framework	9
10.	Policy pronouncements	10
11.	Roles and responsibilities	16
12.	Default	18
13.	Inception date	18
14.	Review	19
15.	Enquiries	19
16.	Approval	19

Security policy

1. ACRONYMS

BCP : Business Continuity Plan

GITO : Government Information Technology Office

HOD : Head of Department

ICT : Information Computer Technology

IT : Information Technology

LEDET : Limpopo Economic Development, Environment and Tourism

SIS : Security and Investigation Services

SSA : State Security Agency

TSCM : Technical Surveillance Counter Measures

2. Definitions

2.1 **'assets'** mean material and immaterial property of the Department. Immaterial assets include but are not limited to information in all forms, stored on any media, networks or systems. Material assets include but not limited to tangible property;

2.2 **'business continuity planning'** refers to a process that ensures that the Department continues operating even after a major disruption or disaster;

2.3 **'candidate'** means an applicant for a post, a contract employee or a person acting on

Security policy

behalf of a contract appointee or independent contractor who has to undergo the vetting process;

2.4 '**certification**' means the issuing of a certificate which confirms that a comprehensive evaluation of the technical and non-technical security features of an Information and communication technology systems (hereinafter referred to as an "ICT" system) and its related safeguards have been undertaken and that it was established that its design and implementation meet a specific required set of security requirements;

2.5 '**critical service**' means a service identified by the Department as critical through Threat and Risk Assessment process and the compromise of such service can endanger the effective functioning of the Department;

2.6 '**cyber-attack**' means unauthorized access to electronic systems;

2.7 '**documents**' mean the following:

- Any note or writing, whether produced by hand or by printing, typewritten or any other similar process, in either tangible or electronic format;
- Any copy, plan, picture, sketch, photographic or other representation of any place or article; and
- any disc, tape, card, perforated roll or other device in or on which sound or any signal has been recorded for reproduction;

2.8 '**employee**' means any male or female person appointed within the Department of Economic Development, Environment and Tourism in terms of the Public Service Act 103 of 1994, as amended;

2.9 '**information security**' includes, but is not limited to:

- Safekeeping of documents;
- Physical security measures for the protection of information;
- Information and communication technology security;

Security policy

- Personnel security;
- Business continuity planning;
- Contingency planning;
- Security screening;
- Technical surveillance counter measures;
- Dealing with information security breaches;
- Security investigations; and
- Administration and organisation of the security function in the Department

2.10 '**need to know principle**' means a principle which determines who must have access to classified information in execution of their duties;

2.11 '**peripherals devices**' mean a device which can be attached to and used with a computer, though not an integral part of it e.g. a USB;

2.12 '**state security structures**' mean the institutions which are meant to secure the state such as State Security Agency, South African Police Service, and South African Defense Force;

2.13 '**reliability check**' means an investigation into the criminal record, credit record and past performance of an individual, private entity or organ of state to determine reliability;

2.14 '**risk**' means the likelihood of a threat materialising through exploitation of security measures;

2.15 '**screening 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;

2.16 '**security breach**' means the negligent or intentional transgression of or failure to

Security policy

comply with security measures;

- 2.17 **'security clearance'** means a certificate issued to a candidate after the successful completion of a security screening investigation, specifying the level of classified information to which the candidate may have access subject to the "Need to know principle";
- 2.18 **'screening investigation'** means a process conducted by the screening investigator to specify the level of classified information which the candidate may have access to, subject to the "Need to know principle";
- 2.19 **'site access clearance'** means clearance required for access to site's installations critical to the State's interest;
- 2.20 **'technical surveillance counter measures'** mean the process involved in the detection, localisation, identification and neutralisation of electronic counter-measures of an individual, an organ of state, facility or vehicle;
- 2.21 **'technical or electronic surveillance'** means the interception or monitoring of sensitive or proprietary information or activities;
- 2.22 **'threat'** means any potential event or act, deliberate or accidental, that could cause injury to persons, compromises the integrity of information or could cause the loss or damage of assets;
- 2.23 **'Threat and Risk Assessment'** within the context of security risk management, means 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; and
- 2.24 **'vulnerability'** means a deficiency related to security that could permit a threat to

materialise.

3. INTRODUCTION

LEDET depends on its personnel, information and assets to deliver services that ensure the safety, security and economic well-being of its clients. The Department must therefore manage these resources with due diligence and take appropriate measures to protect them.

Threats that can cause harm to LEDET, in South Africa and abroad. It includes acts of terror, sabotage, espionage, unauthorized access to buildings and premises, theft, armed robbery, fraud, corruption, vandalism, fire, natural disasters, technical failures, accidental damage, threat of cyber-attack and malicious damage to infrastructure. Threats against the national interest, such as transnational criminal activity, foreign intelligence activities and terrorism continue to evolve as the result of change in the international environment, hence the importance of applying appropriate security measures aimed at protecting all departmental assets

4. BACKGROUND

The security division in LEDET is structured to complement the efforts of a multi-disciplinary approach by government to prevent and control the risks, crime and security breaches that the Department could be exposed to. It has also been designed to protect employees, preserve confidentiality, integrity, and value of information and assets and to ensure continued delivery of services.

5. PURPOSE AND OBJECTIVES

5.1 The purpose of this policy is to:

Security policy

- 5.1.1 strengthen measures aimed at ensuring effective implementation of information and physical security.
- 5.1.2 regulate the process of security screening and background checks of employees and service providers.
- 5.1.3 apply appropriate security measures aimed at protecting all departmental assets.
- 5.1.4 encourage the classification and categorising of comprehensive security information.

5.2 The objective of the policy is to:

- 5.2.1 support the national interest of South Africa and LEDET business objectives by protecting employees, information, assets and assuring the continued delivery of services to the public.

6. AUTHORITY OF THE POLICY

The policy is issued under the authority of the HOD as the Accounting Officer for LEDET.

7. SCOPE OF APPLICATION

This policy applies to all employees (interns and learners), including all contractors, service providers, consultants and stakeholders.

8. PRINCIPLES

The security policy is aimed at contributing to the development of a safe and secure work environment and is strengthened by the following principles:

- 8.1 Code of conduct
- 8.2 Combatting crime

Security policy

8.3 Accountability

8.4 Ethics

8.5 Integrity

8.6 Confidentiality

9. LEGAL FRAMEWORK

9.1 This policy is informed by the following legal mandates:

9.1.1 Control of Access to Public Premises and Vehicles Act 53 of 1985, as amended.

9.1.2 Criminal Procedure Act 51 of 1977, as amended.

9.1.3 Electronic Communication and Transaction Act 25 of 2002.

9.1.4 Firearms Control Act 60 of 2000, as amended.

9.1.5 Fire Brigade Services Act 99 of 1987, as amended.

9.1.6 General Intelligence Law Amendment Act 66 of 2000.

9.1.7 Intelligence Service Act 65 of 2002 and Intelligence Service Regulations, 2003.

9.1.8 Intelligence Services Control Amendment Act 66 of 2002.

9.1.9 Minimum Information Security Standards Second Edition, March 1998.

9.1.10 Minimum Physical Security Standards, 2009.

9.1.11 National Strategic Intelligence Act 39 of 1994.

9.1.12 Prevention of Interception and Monitoring Act 70 of 2002.

9.1.13 Private Security Industry Regulation Act 56 of 2001.

9.1.14 Protection of Information Act 84 of 1982, as amended.

Security policy

- 9.1.15 Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004.
- 9.1.16 Regulation of Interception of Communications and Provision of Communication- Related Information, Act 70 of 2002.
- 9.1.17 Trespass Act 6 of 1959.
- 9.1.18 White paper on Intelligence, (1995).
- 9.1.19 State Security Agency Guidance Documents: ICT Policy and Standards: Part 1&2.

10. POLICY PRONOUNCEMENTS

The Security Policy covers the following seven elements of the security program of LEDET:

- Security administration
- Information security
- Physical security
- Personnel security
- Information and Communication Technology Security
- Communication Security
- Business Continuity Planning

10.1 Security administration

Security administration includes the following:

- 10.1.1 General security competencies as specified in departmental directives and procedures, training and awareness, security audits and sharing of information and assets.

Security policy

10.1.2. Implementing physical security and ensuring physical access limitations to ICT systems such as server rooms.

10.1.3 Ensuring the protection of employees, classified information and assets.

10.1.4 Management of security screening processes of service delivery contracts with LEDET and facilitating reports on security breaches.

10.1.5 Management of security emergencies and threats.

10.2 Information security

10.2.1 All sensitive information produced or processed by the Department must be identified, categorised and classified according to the origin of its source and the contents according to the merits of sensitivity in order to prevent loss, compromise or disclosure.

10.2.2 All sensitive information must be categorized into one of the following groupings:

- State Secret:
- Trade Secret; and
- Personal information.

10.2.3 Sensitive information must be classified according to its level of sensitivity by using one of the following recognised levels of classification:

- Confidential;
- Secret; and
- Top Secret.

10.2.4 The classification assigned to documents must be strictly adhered to.

Security policy

10.2.5 Access to classified information will be determined by the following principles:

- 'Need-to-know'; and
- Level of security clearance.

10.3 Physical Security

10.3.1 Physical security involves the proper layout and design of facilities of LEDET and the use of physical security measures to prevent unauthorized access to assets by certain officials.

10.3.2 It includes measures to detect attempted or actual unauthorised access and the activation of an appropriate response, including the provision of measures to protect employees from bodily harm.

10.3.3 Physical security measures must be implemented and maintained in order to ensure that LEDET, its employees, property and information are secured.

10.4 Personnel Security

10.4.1 All employees, contractors, consultants and stakeholders who require access to classified information and assets in order to perform their duties or functions must be subjected to a security screening investigation conducted by the SSA in order to be granted a security clearance at the applicable level;

10.4.2 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.

10.4.3 A security clearance provides access to classified information subject to the

Security policy

“need-to-know principle”.

10.4.4 The oath of secrecy shall be signed by all employees of LEDET.

10.4.5 Every employee issued with a security clearance to complement the entire security screening process shall sign a declaration of secrecy. This declaration will remain valid even after the employee has terminated his or her services with LEDET.

10.4.6 A security clearance will be valid for a period specified on the certificate. This does not prevent re-screening on more frequent basis as determined by the HOD or based on information which could impact negatively on an employee's security competence.

10.4.7 SSA shall timeously be informed of all employees who have terminated their services with LEDET.

10.5 Information and Communication Technology Security

10.5.1 ICT Security

10.5.1.1 Server rooms and other related security zones where IT equipments are kept shall be secured with adequate physical security measures and strict access control shall be enforced and monitored.

10.5.1.2 Employees shall be responsible for implementing the appropriate security measures in safeguarding all IT equipments under their control such as laptops, computers and peripherals devices as outlined in the ICT Security policy of the Department.

10.6 Business Continuity Planning

- 10.6.1 The contingency plan must be focussed on saving lives, safeguarding property and information as well as ensuring that activities can continue with as little disruption as possible in an event of an emergency or a disaster.
- 10.6.2 This can only be achieved through well-organised action in which all the available resources are used in a co-ordinated and effective way to put preventative and control measures into operation.
- 10.6.3 The departmental Security Committee shall be responsible for managing the drafting, authorising, implementing and timely reviewing of the BCP.
- 10.6.4 All employees of LEDET shall be made aware of the content of the BCP to ensure understanding of each employee's respective role thereof.

10.7 Exceptions

- 10.7.1 Deviations from this policy and its associated security directives will only be permitted in the following circumstances:
- a) When security must be breached in order to save or protect lives; and
 - b) During unavoidable emergency circumstances e.g. natural disasters.

10.8 Other Considerations

- 10.81 The following shall be taken into consideration when implementing this policy:
- a) Occupational Health and Safety issues at LEDET
 - b) Disaster management at LEDET
 - c) Persons with disabilities 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.

Security policy

10.9 Reporting of security breaches

The Director: SIS has the following responsibilities in ensuring that security breaches are handled appropriately:

- 10.9.1 Any security breach shall be reported to the Director: SIS.
- 10.9.2 The Director: SIS shall ensure that all security breaches are investigated.
- 10.9.3 The Director: SIS shall ensure that the HOD is advised of all noteworthy incidents within 24 (twenty-four) hours.
- 10.9.4 The Director: SIS, in collaboration with the State Security Structures (where required), will conduct investigations into all security breaches and provide reports on such investigations to the HOD.
- 10.9.5 The HOD may suspend access privileges to classified information, assets and/or premises, depending on the seriousness of the security breach or alleged security breach under investigation until the administrative, disciplinary and criminal processes are concluded.

10.10 Technical Surveillance Counter Measures

- 10.10.1 All offices, meetings, conferences and boardroom venues at LEDET, where sensitive and classified matters are discussed on a regular basis, shall be identified and be subjected to proper and effective physical security and access control measures. Periodic electronic Technical Surveillance Counter Measures (sweeping) will be conducted by SSA to ensure that these areas are secure.
- 10.10.2 The Director: SIS shall ensure that areas that are utilized for discussions of a sensitive nature as well as offices or rooms that house electronic

Security policy

communications equipment, are physically secured in accordance with the standards laid down by SSA, prior to any request as well as after a TSCM examination, in order to support the required security integrity.

10.11 Polygraph examination

10.11.1 A polygraph examination may be utilised to provide support to the security screening process.

10.11.2 All employees subjected to a Top Secret security clearance will be subjected to a polygraph examination done by SSA.

10.12 Transferability of Security Clearances

10.12.1 A security clearance issued in respect of a candidate from other government institutions shall not be automatically transferable to LEDET.

10.12.2 The responsibility for deciding whether the candidate should be re-screened rests with the Director: SIS.

10.13 Security Awareness programs

10.13.1 A security awareness program shall be developed by the Director: SIS and implemented to effectively ensure that all employees, consultants and service providers of LEDET remain security conscious.

10.13.2 All employees shall be subjected to the security awareness program.

11. ROLES AND RESPONSIBILITIES

11.1 HEAD OF DEPARTMENT

Security policy

- 11.1.1 The HOD bears the overall responsibility for implementing and enforcing the security programme of LEDET.
- 11.1.2 The HOD shall establish a Security Committee and ensures the participation of all committee members in the functions and activities of the Committee.

11.2 DIRECTOR: SIS

The Director: SIS has the following responsibilities:

- 11.2.1 Direct the prescribed security program.
- 11.2.2 Review the Security Implementation Plan by conducting annual Threat and Risk Assessments.
- 11.2.3 Advise management on the security implications of management decisions.
- 11.2.4 Establish and maintain a good working relationship with State Security structures and any other relevant stakeholders.
- 11.2.5 Manage the following:
 - a) General security administration;
 - b) Administration of security screening;
 - c) Implementation of physical security measures;
 - d) Protection of employees and classified information;
 - e) Physical security of ICT systems in liaison with the Director: GITO;
 - f) Security emergencies;
 - g) Security breach reporting and investigations;
 - h) Security information classification system within the Department;
 - i) Regular surveys, audits and walkthrough inspections to monitor the effectiveness of the security awareness program;

Security policy

- j) Ensures that security measures are fully integrated in the planning and designing of departmental facilities;
- k) Demarcation of restricted access areas; and
- l) Inclusion of the necessary security specifications during the drafting of tender documentation.

11.3 SECURITY COMMITTEE

The Security Committee shall be responsible for: -

- 11.3.1 Drafting and reviewing of a Business Continuity Plan;
- 11.3.2 Participation in the activities of the Security Committee;
- 11.3.3 Monitoring foreign visits by employees of the Department in terms of the Database and compliance with applicable legal prescripts;
- 11.3.4 Regular reporting to SSA; and any other related matters.

11.4 CONTRACTORS AND CONSULTANTS

Hosts directorates of all contractors and consultants must ensure that such consultants and contractors are sent to SIS for vetting and briefing before commencement of their respective contracts.

12. DEFAULT

An employee who fails to comply with the provisions of this policy shall be dealt with in terms of the Public Service Disciplinary Code and Procedures for the Public Service.

13. INCEPTION DATE

The inception date of this policy is 30 (thirty) days after approval by the Head of Department.

Security policy

14. REVIEW

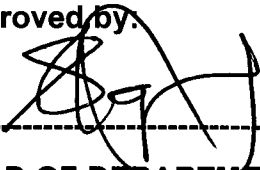
This policy shall be reviewed every 36 (thirty-six) months.

15. ENQUIRIES

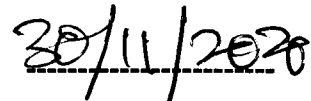
Enquiries regarding the policy shall be directed to the Director: SIS

16. APPROVAL

Approved by:



HEAD OF DEPARTMENT: LEDET



DATE