education
Department:
Education
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

Garona Building, Mmabatho
First Floor, East Wing,
Private Bag X2044,
Mmabatho 2735
Tel.: (018) 388-3429/33
e-mail: sgedu@nwpg.gov.za

OFFICE OF THE SUPERINTENDENT-GENERAL

SECURITY POLICY

APPROVED BY : SESHIBE MW.

POSITION : ACTING SG

SIGNATURE: MW.

DATE OF APPROVAL: 01-07-2024

CLASSIFICATION: N/A

REVISION NO. & DATE 01/07/2025

COPY:

MW.

POLICY

1. STATEMENT OF PURPOSE

1.1. The NW DoE depends on its personnel, information and assets to deliver services that ensure the safety, security and economic well being of South African citizens. It must therefore manage these resources with due diligence and take appropriate measures to protect them.

1.2. Security policy should impact a defence against threats that can cause harm to the NW DoE, in South Africa and abroad, include 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 cyber attack and malicious activity through the internet is prevalent and can cause severe harm to electronic, digital services and critical infrastructure. Threats to the national interest, such as transnational criminal activity, foreign intelligence activities and terrorism, continue to evolve as the result of changes in the international environment and technology.

1.3. The Security Policy of the NW DoE prescribes the application of security measures to reduce the risk and harm that can be caused to the institution if the above threats should materialise.

1.4. It has been designed to protect employees, preserve the confidentiality, integrity, availability and value of the information and assets, and assure the continued delivery of services. Since the Department relies extensively on information and communication technology (ICT) to provide its services, this policy emphasizes the need for acceptable use of ICT equipment as well as ICT protection measures to be complied with by employees.

1.5. The main objective of this policy therefore is to support the national interest and the North West Department of Education's objectives by protecting employees, information and assets, and assuring the continued delivery of services for South African Citizens.

1.6. This policy complements other government policies (e.g. sexual harassment, occupational health and safety, official languages, information management, asset control, real property and financial resources).

2. SCOPE

2.1. This policy applies to the following individuals and entities:-

- All employees of the NW DoE.
- All contractors and consultants delivering services to the NW DoE, including their employees who may interact with the Department;
- Temporary employees
- All information assets of the Department
- All intellectual, movable and fixed property owned or leased by the NW DoE.

2.2. The policy further covers the following seven elements of the security program of the NW DoE.

- Security organization
- Security administration
- Physical security
- Information security
- Personnel security
- Information and Communication Technology (ICT) security
- Business Continuity Planning (BCP)

3. LEGISLATIVE AND REGULATORY REQUIREMENTS

3.1. This policy is informed by and complies with applicable national legislation, national security policies and national security standards.

4. POLICY PROBLEM STATEMENT

4.1. General

- Employees Information and assets of the NW DoE must be protected against identified threats according to baseline security requirements and continuous security risk management.

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

4.2. Compliance

4.2.1. Compliance Requirements

All individuals mentioned in par. 2 above must comply with the baseline requirements of this policy and its associated Security Directives as contained in the Security Plan of the Department. The requirements are based on integrated Security Threat and Risk Assessments (TRA's) to the national interest as well as employees, information and assets of the Department. The necessity of security measures above baseline levels will also be determined by the continuous updating of the Security TRA's to ensure compliance to the security requirements.

4.2.2. Compliance to *Security threat analysis and risk assessment involved:-*

- **Establishing** the scope of the assessment and identifying the information, employees and assets to be protected.
- **Determining** the threats to information, employees and assets of the NW DoE and assessing the probability and impact of threat occurrence.
- **Assessing** the risk based on the adequacy of existing security measures and vulnerabilities.
- **Implementing** any supplementary security measures that will reduce the risk to an acceptable level.

4.2.3. Compliance: Staff accountability and acceptable use of assets

4.2.3.1. The Head of the Department shall ensure that information and assets of the Department are used in accordance with procedures as stipulated in the Security Directives as contained in the Security Plan of the NW DoE.

4.2.3.2. All employees of the NW DoE shall be accountable for the proper utilization and protection of such information and assets. Employees that misuse or abuse both tangible and intangible assets of the Department shall be held accountable therefore, and disciplinary action shall be taken against any such employee.

4.2.3.3 There shall be recognition and reward system for an employee(s) who has demonstrated compliance to Departmental Security Requirements

4.3. Specific baseline requirements

4.3.1. Security organisation

4.3.1.1 The Executing Authority (EA) of the NW DoE has appointed a Security Manager (SM) to establish and direct a security program that ensures co-ordination of all security related policy interventions and the implementation of policy requirements.

4.3.1.2 Given the importance of this role, the SM (with sufficient security experience and training who) is strategically positioned in the Department to provide institution-wide strategic advice and guidance to the EA and Senior Management.

4.3.1.3. The EA and HOD of the North West DoE will ensure that the SM has an effective support structure (security component) to fulfil the functions referred to in par. below.

4.3.1.4 Individuals appointed in the support structure of the SM will all be security professionals with sufficient security experience and training to effectively cope with their respective job functions.

4.3.2. Security administration

4.3.2.1 The functions referred to in par. 4.3.1. above include: -

- general security administration (departmental directives and procedures, training and awareness, security risk management, security audits, sharing of information and assets);
- setting of access limitations;

- administration of security screening;
- implementing physical security;
- ensuring the protection of employees, assets and information;
- ensuring ICT Security;
- ensuring security in emergency and increased threat situations;
- facilitating business continuity planning;
- ensuring security in contracting; and
- facilitating security breach reporting and investigations.

4.3.2.2 Security incident/breaches reporting process

- Whenever an employee of the NW DoE becomes aware of an incident that might constitute a security breach or an unauthorized disclosure of information (whether accidentally or intentionally), he/she shall report that to the SM of the Department by utilising the formal reporting procedure prescribed in the Security Breach Directive of the NW DoE.

- The HOD of the Department shall report to the appropriate authority (as indicated in the Security Breach Directive of the NW DoE all cases or suspected cases of security breaches, for investigation).

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

4.3.2.3 Security incident / breaches response process

- The SM shall develop and implement security breach response mechanisms for the North West DoE in order to address all security breaches / alleged breaches which are reported.

- The SM shall ensure that the EA of the North West DoE is advised of such incidents as soon as possible.

- It shall be the responsibility of DoE in conjunction with the State Security Agency Structure to conduct an investigation on reported information security breaches and provide feedback with recommendations to the North West DoE

- Access privileges to classified information, assets and / or to premises may be suspended by the EA of the North West DoE until administrative, disciplinary and / or criminal processes have been concluded, flowing from investigations into security breaches or alleged security breaches.

- The end result of these investigations, disciplinary action or criminal prosecutions may be taken into consideration by the Executing Authority of the North West DoE in determining whether to restore, or limit, or increase the security access privileges of an individual or whether to revoke or alter the security clearance of the individual.

4.3.3 Information Security

4.3.3.1 Categorization of information and information classification system must be put in place by the SM.

4.3.3.2 The SM must ensure that a comprehensive information classification system is developed and implemented in the North West DoE. All sensitive information produced or processed by the North West DoE must be identified, categorised and classified according to the origin of its source and contents and according to its sensitivity to loss or disclosure.

4.3.3.3 All sensitive information must be categorised into one of the following categories.

- State Secret,
- Trade Secret, and
- Personal information.

And subsequently classified according to its level of sensitivity by using one of the recognised levels of classification: -

- Confidential
- Secret; and
- Top secret.

4.3.3.4 Employees of the North West DoE who generate sensitive information are responsible for determining information classification levels and the classification thereof, subject to management review. This responsibility includes the labelling of classified documents.

4.3.3.5 The classification assigned to documents must be strictly adhered to and the prescribed security measures to protect such documents must be applied at all times.

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

- Intrinsic secrecy approach;
- Need-to-know;
- Level of security clearance.

4.3.4 Physical Security

4.3.4.1 Physical security involves the proper layout and design of facilities of the North West DoE and the use of physical security measures to delay and prevent unauthorised access and the activation of an appropriate response. Physical security also includes the provision of measures to protect employees from bodily harm.

4.3.4.2 Physical security measures must be developed implemented and maintained in order to ensure that the entire Department, its personnel, property and information are secured. These security measures shall be based on the findings of the Threat and Risk Assessment (TRA) to be conducted by the SM.

4.3.4.3 The North West DoE shall ensure that physical security is fully integrated early in the process of planning, selecting, designing and modifying of its facilities. The North West Department of Education shall;

- Select, design and modify facilities in order to facilities the effective control of access thereto,
- Demarcate restricted access areas and have the necessary entry barriers, security systems and equipment to effectively control access thereto,
- Include the necessary security specifications in planning, request for proposals and tender documentation;
- Incorporate related costs in funding requirements for the implementation of the above.

4.3.4.4 The North West DoE will also ensure the implementation of appropriate physical security measures for the security storage, transmittal and disposal of classified and protected information in all forms.

4.3.4.5 All employees are required to comply with access control procedures of the North West DoE at all times. This includes the producing of ID Cards upon entering any sites of the North West DoE, the display thereof whilst on the premises and the escorting of official visitors.

4.3.5 Personnel Security

4.3.5.1 Security Screening

- All employees, contractors and consultants of the North West DoE, who requires access to classified information and critical assets in order to perform duties or functions, must be subjected to a security screening investigation conducted by the State Security Agency (SSA) in order to be granted a security clearance at the appropriate level.

- 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.

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

- 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 North West DoE.

- A security clearance will be valid for a period of five years for Secret and Top Secret. This does not preclude re-screening on a more frequent basis as determined by the EA of the North West Department of Education, based on information which impact negatively on individual's security competence.

- Security clearances in respect of all individuals who have terminated their services with the North West DoE shall be immediately withdrawn.

4.3.5.2 Polygraph examination

- A polygraph examination shall be utilized to provide support to the security screening process. All employees subjected to a Top Secret security clearance will also be subjected to a polygraph examination. The polygraph shall only be used to determine the reliability of the information gathered during the security screening investigation and does not imply any suspicion or risk on the part of the applicant.

- In the event of any negative information being obtained with regard to the applicant during the security screening investigation (all levels), the applicant shall be given an opportunity to prove

his/her honesty and/or innocence by making use of the polygraph examination. Refusal by the applicant to undergo the examination does not necessarily signify that a security clearance will not be granted.

4.3.5.3 Transferability of security clearances

- A security clearance issued in respect of an official from other government institutions shall not be automatically transferable to the North West DoE.

4.3.5.4 Security Awareness and Training

- A security training and awareness program must be developed by the SM and implemented to effectively ensure that all personnel and service providers of the Department remain security conscious.

- All employees shall be subjected to the security awareness and training programs and must certify that the content of the program has been understood and will be complied with. The program covers training with regard to specific security responsibilities and sensitizes employees and relevant contractors and consultants about the security policy and security measures of the North West DoE the need to protect sensitive information against disclosure, loss or destruction.

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

- Regular surveys and walkthrough inspections shall be conducted by the SM and members of the security component to monitor the effectiveness of the security training and awareness program.

4.3.6 Information and Communication Technology (ICT) Security

4.3.6.1 IT Security

- A secure network shall be established for the NW DoE in order 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.

- To prevent the compromise of IT systems, the NW DoE 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.

- To ensure policy compliance, the IT Manager of the NW DoE shall: -

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

    - Conduct periodic security evaluations of systems, including assessments of configuration changes conducted on a routine basis.

    - Periodically request assistance, review and audits from the State Security Agency (SSA) in order to get an independent assessment.

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

- Access to the resources on the network of the NW DoE shall be strictly controlled to prevent unauthorised access. Access to all computing and information systems and peripherals of the Department shall be restricted unless explicitly authorized.

- System hardware, operating and application software, the network and communication systems of the NW DoE shall all be adequately configured and safeguarded against both physical attack and unauthorised network intrusion.

- All employees shall make us of IT systems of the NW DoE in an acceptable manner and for business purposes only. All employees shall comply with the IT Security Directives in this regard at all times.

- The selection of passwords, their use and management as a 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.

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

- The ICT manager shall limit the use of privately owned laptops/computers unless approved with certification of permission.

4.3.6.2 Internet access

- The IT Manager of the NW DoE, having the overall responsibility for setting up Internet access for the Department, shall ensure that the network of the NW DoE 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.

- The IT Manager of the NW DoE 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 reaches and incidents.

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

4.3.6.3 Use of Laptop computers.

- Usage of laptop computers by employees of the NW DoE 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.

- The information stored on a laptop computer of the NW DoE shall be suitably protected at all times. In line with the protection measures prescribed in the IT Security Directive.

- Employees shall also be responsible for implementing the appropriate security measures for the physical protection of laptop computers at all times, in line with the protection measures prescribed in the IT Security Directives and information security policy

4.3.6.4 Communication security

- The application of appropriate security measures shall be instituted in order to protect all sensitive and confidential communication of the Department in all its forms and at all times.

- All sensitive electronic communications by employees, contractors or employees of the Department must be electronically encrypted in accordance with the South African Communication Security Agency (SACSA) standards and the Communication Security Directive of the Department

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

4.3.6.5 Technical surveillance counter measures (TSCM)

- All offices, meeting, conference and boardroom venues of the NW DoE 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 by State Security Agency (SSA) to ensure that these areas are kept sterile and secure.

- The SM of the Department shall ensure that areas that are utilize for discussions of a sensitive nature as well as offices or rooms that house electronic communications equipment, are physically secured in accordance with the standards laid down by (SSA) in order to support the sterility of the environment after a TSCM examination, before any request for a TSCM examination is submitted.

- No unauthorised electronic devices shall be allowed in any boardrooms and conference facilities where sensitive information of the NW DoE is discussed. Authorisation must be obtained from the SM.

4.3.7 Business Continuity Planning (BCP)

4.3.7.1 The SM of the NW DoE must establish a Business Continuity Plan (BCP) to provide for the continued availability of critical services, information and asset if a threat materialises and to provide for appropriate steps and procedures to respond to an emergency situation to ensure the safety of employees, contractors, consultants and visitors.

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

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

4.3.7.4 The Business continuity plan shall be kept up to date and re-tested periodically by the SM.

4.3.7.5 Innovative measures shall continually be taken as opportunities in sustaining Business Continuity Plan.

5 SPECIFIC RESPONSIBILITIES

5.3 Head of Department

5.3.1 The EA of the NW DoE bears the overall responsibility for implementing and enforcing the security program of the government. Towards the execution of this responsibility, the EA shall:-

- Establish the post of the SM and appoint a well-trained and competent security official in the post;

- Establish a security committee for the institution and ensure the participation of all senior management members of all the core business functions of the Department in the activities of the committees.
- Approve and ensure compliance with this policy and its associated Security Directives by all it is applicable to.

Security Manager

5.3.2 The delegated security responsibility lies with the SM, who will be responsible for the execution of the entire security function and program within the Provincial Government (coordination, planning, implementing, controlling, etc.). Towards execution of his/her responsibilities, the SM shall, amongst others:-

- Chair the security committee of the NW DoE.
- Draft the internal security policy and security plan (containing the specific and detailed Security Directives of the Department in conjunction with the security committee,
- Review the Security Policy and Security Plan at regularly intervals
- Conduct a security TRA with the assistance of the security committee of the DoE
- Advise management on the security implications of management decisions
- Implement a security awareness program,
- Conduct internal compliance audits and inspections at the at regular intervals;
- Establish a good working relationship with both SSA and SAPS and liaise with these institutions on a regular basis

5.4 Security Committee

5.4.1 The Security Committee referred to in par. 5.1.1. above shall consist of senior managers of the NW DoE representing all the main business units of the Department.

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

5.4.3 The Security committee of the NW DoE shall be responsible for amongst others.

- Assisting the SM in the execution of all security related responsibilities at the NW DoE, including completing tasks such as drafting / reviewing of the Security Policy and plan, conducting of a security TRA, conducting of security audits, drafting of a BCP and assisting with security awareness and training.

5.5 Line Management

5.5.1 All managers of the NW DoE shall ensure that their subordinates comply with this policy and Security Directives as contained in the Security Plan of the Department.

5.5.2 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.

5.6 Employees, consultants, contractors and other Service Providers

5.6.1 Every employee, consultant, contractor and other service providers of the NW DoE 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 Department at all times.

6 AUDIENCE

6.1 This policy is applicable to all members of the management, employees, consultants, contractors and any other service providers of the NW DoE. It is further applicable to all visitors and members of the public visiting premises of or may officially interact with the Department.

7 ENFORCEMENT

7.1 The Head of Department for the NW DoE and the appointed SM are accountable for the enforcement of this policy.

7.2 All employees of the Department are required to fully comply with this policy and its associated Security Directives as contained in the Security Plan. Non-compliance with any prescripts shall be addressed in terms of the Disciplinary code/regulations of the Department.

7.3 Prescripts to ensure compliance to this policy and the Security Directives by all consultants, contractors or service providers of the NW DoE 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.

8 EXCEPTIONS

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

- When security must be breached in order to save or protect the lives of people,
- During unavoidable emergency circumstances e.g. natural disasters.
- On written permission of the HOD for the NW DoE (reasons for allowing non-compliance to one or more aspects of the policy and directives shall be clearly in such permission; no blanket non-compliance shall be allowed under any circumstances).

9 OTHER CONSIDERATIONS

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

9.1.1 Occupational Health and Safety issues in the Department.

9.1.2 Disaster management at the NW DoE.

9.1.3 Disabled persons 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

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

10 COMMUNICATING AND ENFORCEMENT OF THE POLICY

10.1 The SM of the Department shall ensure that the content of this policy (or applicable aspects thereof) is communicated to all employees, consultants, contractors, service providers, clients, visitors, members of the public that may officially interact with the Department.

10.2 The SM will further ensure that all security policy and directive prescriptions are enforced and complied with.

10.3 The SM must ensure that a comprehensive security awareness program is developed and implemented with the Department to facilitate the above said communication. Communication of the policy by means of this program shall be conducted as follows:-

- Awareness workshops and briefings to be attended by all employees;
- Distribution of memos and circulars to all employees;
- Access to the policy and applicable directives on the intranet of the NW DoE.

11 REVIEW AND UPDATE PROCESS

11.1 The SM, assisted by the Security Committee of the NW DoE, must ensure that this policy and its associated Security Directives is reviewed and updated on an annual basis. Amendments shall be made to the policy and directives as the need arise.

12 IMPLEMENTION

12.1 The SM of the NW DoE 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 Department)

12.2 Implementation of the policy and its associated Security Directives is the responsibility of each and every individual this policy is applicable too (see par. 2.1. above)

13 MONITORING OF COMPLIANCE

13.1 The SM, with the assistance of the security component and security committee of the NW DoE must ensure compliance with this policy and its associated Security Directives by means of conducting internal security audits and inspections on a frequent basis.

13.2 The findings of said audits and inspections shall be reported to the HOD forthwith after completion thereof.

14 DISCIPLINARY ACTION

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

- Re-training
- Verbal and written warnings
- Termination of contracts in the case of contractors or consultants delivering a service to the NW DoE.
- Dismissal
- Suspension
- Loss of the NW DoE information and asset resources access privileges

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

ANNEXURE A: APPLICABLE LEGISLATION AND OTHER REGULATORY FRAMEWORK DOCUMENTS

Applicable legislation

- Constitution of the Republic of South Africa, 1996 (Act 106 of 1996)
- Protection of Information Act, 1982 (Act No. 84 of 1982)
- Promotion of Access to Information Act 2000 (Act No. 2 of 2000)
- Promotion of Administrative Justice Act, 2000 (Act 3 of 2000)
- Copyright Act, 1978 (Act No. 98 of 1978)
- National Archives of South Africa Act, 1996 (Act No. 43 of 1996) and regulations
- Public Service Act, 1994 (Act No. 103 of 1994) and regulations
- Occupational Health and Safety Act, 1993 (Act No. 85 of 1993)
- Criminal Procedures Act, 1977, (Act 51 of 1977) as amended
- Private Security Industry Regulations Act, 2001 (Act 56 of 2001)
- Control of Access of Public Premise and Vehicles Act, 1985 (Act 53 of 1985)
- National Key Points Act, 1980 (Act 102 of 1980)
- Trespass Act, 1959 (Act 6 of 1959)
- Electronic Communication and Transaction Act, 2002 (Act 25 of 2002)
- Electronic Communication Security (Pty)Ltd Act, 2002 (Act 68 of 2002)
- State Information Technology Agency Act, 1998 (Act 88 of 1998)
- Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act 70 of 2002)
- General Intelligence Law Amendment Act, 2000 (Act 66 of 2000)
- Intelligence Service Act, 2002 (Act 65 of 2002) and regulations
- National Strategic Intelligence Act, 1994 (Act 39 of 1994)
- Intelligence Service Control Act, 1994 (Act 40 of 1994)
- Labour Relations Act, 1995 (Act 66 of 1995)
- Employment Equity Act, 1998 (Act 55 of 1998)
- Occupational Health and Safety Act, 1993 (Act 83 of 1993)
- Fire-Arms Control Act, 2000 (Act 60 of 2000) and regulations
- Non-Proliferation of Weapons of Mass Destruction Act, 1993 (Act 87 of 1993)
- Protection of constitutional Democracy Against Terrorism and Related Activities Act 2004 (Act 33 of 2004)
- National Building Regulations and Building Standards Act, 1977 (Act 103 of 1977)
- Protected Disclosures act, 2000 (Act 26 of 2000)
- Intimidation Act, 1982 (Act 72 of 1982)
- Prevention and Combating of Corrupt Activities Act, 2004 (Act 12 of 2004)
- Public Finance Management Act, 1999 (Act 1 of 1999) and Treasury Regulations.

Other regulatory Framework documents

- Minimum Information Security Standards (MISS), Second Edition March 1999
- White Paper on Intelligence (1995)
- SACSA/090/1(4) Communication Security in the RSA
- SSA Guidance Documents: ICT Policy and Standards: Part 1 & 2
- ISO 17799
- National Building Regulations

ANNEXURE B: DEFINITIONS

- "**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.
- "**assets**" means material and immaterial property of an institution. 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 and internal reputation,
- "**availability**" means the condition of being usable on demand to support operations, programmes and services;
- "**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.
- "**candidate**" means an applicant, an employee, a contract employee or a person acting on behalf of a contract appointee or independent contractor
- "**certification**" means the issuing of a certificate certifying that comprehensive evaluation of the technical and non-technical security features of an Information and communication Technology system (hereinafter referred to as an ICT system) and its related safeguards has been undertaken and that it was established that its design and implementation meets a specific set of security requirements.
- "**COSMEC**" means the organ of state known as Electronic Communications Security (Pty) Ltd, which was established in terms of section 2 of the Electronic communications security act, 2002 (Act No. 68 of 2002) and, until such time as COMSEC becomes operational, the South African Communication Security Agency;
- "**critical service**" 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.
- "**document**" means"-
    - Any not or writing, whether produced by hand or by 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 other device in or on which sound of any signal has been recorded for reproduction,
- "**Information security**" includes, but is not limited to:-
    - Document security
    - Physical security measures for the protection of information
    - Information and communication technology security
    - 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 at organs of state.
- "**National Intelligence Structures**" means the National Intelligence Structures as defined in section 1 of the National strategic Intelligence Act, Act 39 of 1994
- "**reliability check**" means an investigation into the criminal record, credit record and past performance of an individual or private organ of state to determine his, her or its reliability
- "**risk**" means the likelihood of a threat materialising by exploitation of a vulnerability.
- "**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.
- "**security breach**" means the negligent or international transgression of or failure to comply with security measures.
- "**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

- "**site access clearance**" means clearance required for access to installations critical to the national interest
- "**Technical Surveillance Countermeasures**" (TSCMO) means the process involved in the detection, localisation, identification and neutralisation of technical surveillance of an individual, an organ of state, facility or vehicle
- "**technical / electronic surveillance**" means the interception or monitoring of sensitive or proprietary information or activities (also referred to as "bugging")
- "**threat**" means any potential event or act, deliberate of accidental, that could cause injury to persons, compromise the integrity of information or could cause the loss or damage of assets,
- "**Threat and 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 even,
- "**vulnerability**" means a deficiency related to security that could permit a threat to materialise

ANNEXURE C: ACRONYMS

- BCP – Business Continuity Plan
- EA – Executing Authority
- HOD – Head of Department
- ICT- Information and Communication Technology
- NW DoE – North West Department of Education
- SACSA – South African Communication Security Agency
- SAPS – South African Police Service
- SM – Security Manager
- SSA – State Security Agency
- TRA – Threat and Risk Assessment
- TSCM – Technical Surveillance Counter Measures