



SECURITY POLICY


Version control

Version : 01

Publishing Date : February 2022

Review Date : No sooner than 18 months and no later than three (3) years after the publishing date

Responsible Manager: Senior Manager for Corporate Services

Recommended :  9-2-2022
Mr. E Crouch Date

Approved by the Head of Department:


14.03.2022
7 Mr. MP Dichaba Date

Contents

Policy Aim	3
Legislative Framework.....	3
Policy Scope	3
Policy Statement.....	4
Roles and Responsibilities.....	5
Review and Distribution.....	26

1. Policy Aim

The aim of this policy is:

- 1.1.** To ensure that the Department fully accepts its responsibilities to, as far as practically possible, ensure a safe and secure environment for its employees, clients, contractors and visitors¹, as well as to safeguard all public assets and information entrusted to it.
- 1.2.** To ensure sound Security Management practises and good governance by providing a sustainable, efficient and professional advisory service in respect of Security Management, policies, systems, guidelines and measures aimed at protecting people, property, information and other valuable assets of the Department.
- 1.3.** To lay down a set of security rules by which all employees of the Department of Transport, Safety and Liaison and all its stakeholders must abide by and guide people's conduct while providing a base-line to procure, implement and evaluate security systems.
- 1.4.** To provide a framework for the following security related matters:
 - Physical Security, i.e., physical measures aimed at the protection of people, property and information.
 - Personnel Security, i.e., measures aimed at ensuring that any person who gains access to classified information has the necessary authority and security clearance² to do so.
 - Document Security, i.e., measures aimed at protecting classified and sensitive documents.
 - Communication Security, i.e., measures aimed at protecting classified and sensitive information that needs to be communicated.
 - Information Technology Security, i.e., measures aimed at ensuring the confidentiality and integrity of data, as well as the availability of data and systems.

2. Legislative and Policy Framework

- Constitution Act, 1996 (Act 108 of 1996)
- Minimum Information Security Standards
- Control of Access to Public premises and Vehicles Act, 1985 (Act 53 of 1985)

¹ Members of the public

² An official document that indicates the degree of security competence of a person

- Criminal Procedure Act, 1977 (Act 51 of 1977)
- Extension of Security of Tenure Act, 1997 (Act 62 of 1997)
- Fire-arms Control Act, 2000 (Act 60 of 2000)
- Hazardous Substances Act, 1973 (Act 15 of 1973)
- Intimidation Act, 1982 (Act 72 of 1982)
- National Building Regulations and Building Standards Act, 1977 (Act 103 of 1977)
- National Archives and Record Service of South Africa Act, 1996 (Act 43 of 1996)
(Previous short title “National Archives of South Africa” substituted by s. 19 of Act 36 of 2001)
- National Strategic Intelligence Act, 1994 (Act 39 of 1994)
- Occupational Health and Safety Act, 1993 (Act 85 of 1993)
- [Private Security Industry Regulation Act, 2001 \(Act 56 of 2001\)](#)
- Promotion of Access to Information Act, 2000 (Act 2 of 2000)
- Protected Disclosures Act, 2000 (Act 26 of 2000)
- Protection of Information Act, 1982 (Act 84 of 1982)
- Public Service Act Proclamation 103 of 1994
- Public Service Regulation: 2016, 13 (c)
- Public Service Regulations of 2001, which replaced the 1999 Regulations
- Security Officers Act, 1987 (Act 92 of 1987)
- Trespass Act, 1969 (Act 6 of 1969)

3. Policy Scope

This policy is applicable to all facilities or administrative areas, owned or controlled by the Department, employees in the Department as well as members of the public, clients, service providers and consultants.

4. Policy Statement

It is the policy of the Northern Cape Department of Transport, Safety and Liaison that:

4.1. Security Appraisals are conducted

4.1.1. The Head of Department may request the SAPS, via the Security Manager to conduct physical security appraisals in the Department, or specific components thereof to determine compliance with Minimum Physical Security Standard (MPSS), security policies and measures.

4.2. Security Audits³

4.2.1. The Head of Department may request via the Security Manager, to conduct information security⁴ audits at their departments, or specific components thereof, to determine compliance with security policies and the state preparedness.

4.3. Access Control

4.3.1. Access control⁵ is dealt with in terms of the provisions of the Control of Access to Public Premises and Vehicles Act, 1985 (Act 53 of 1985). This Act empowers Head of Department to, among others, take such steps as they consider necessary to safeguard public premises⁶ and protect people thereon against dangerous objects and this includes the public display of notices at all public entrances to departmental premises.

4.3.2. Head of Department may in writing determine different levels or degrees of access control to different premises (or parts thereof) under his/her control, including restricted⁷ access by employees to their offices after normal office hours.

4.3.3. The level of access control must be determined on the basis of sensitivity of, or threats against a premise, combined with the extent to which restricted areas could be zoned off and properly secured. In this regard it is important that a balance be struck between efficient public service delivery and the need to secure the safety of persons, information and property for which the Government is responsible.

³ That part of security control undertaken to determine the general standard of information security and to make recommendations where shortcomings are identified, evaluate the effectiveness and application of security standards and make recommendations as well as provide expert advice with regard to security problems

⁴ That condition created by the conscious provision and application of a system of document, personnel, physical, computer and communication security measures to protect sensitive information

⁵ The process by which access to a particular area is controlled or restricted to authorised personnel only

⁶ Any building, structure, hall, room, office, land, enclosure or water surface which is the property of or is occupied by or is under the control of the department and to which a member of the public has access

⁷ Relates to matters pertaining to a specific department only e.g., internal memos, budgets, etc.

4.3.4. A complete record of each visitor should be kept, as well as of all staff members who visit the premises after hours⁸.

4.3.5. In those instances where persons are required to identify themselves before access to a premise is authorised, only the following are deemed to be positive identification:

- RSA identity book.
- Valid passport.
- Driver's licence.
- Personal identification by an employee of the Department of Transport, Safety and Liaison to verify identification. Particulars of the vouching employee must also be provided.
- Valid access permit issued by a person who is duly authorised by the Head of Department (employees, consultants and contractors).

4.3.6. All access permits issued must be returned to the issuing authority at the termination of their service. The issuing authority must dispose of such permits appropriately.

4.3.7. All vehicles (private or government owned) may be searched when leaving the building occupied by a department.

4.3.8. Property, equipment, parcels, documents, etc will only be taken out of the buildings with official removal permits signed by an authorised official.

4.3.9. Any person may be searched to ensure that he/she does not poses a physical threat or that he/she is not in possession of unauthorised objects. In the case of a man, the search should be performed by a man, in the case of a woman, the search should be conducted by a woman. If and when a female Security Officer is unavailable, a woman from the staff compliment of the Department of Transport, Safety and Liaison may be requested to conduct the search.

4.3.10. A complete record of each visitor should be kept, as well as of all staff members who visit the premises after hours.

4.3.11. The conditions subject to which the visitor may enter the premises, must be clearly defined.

⁸ After hours refers to the time between 17h00 and 06h00, Saturdays and Sundays and Public holidays

4.4. Escorting

- 4.4.1. All visitors must report at the security reception of the Departmental buildings for security to confirm such visits by means of tasking the receptionist to make enquiries.
- 4.4.2. Visitors must remain at the reception area for collection and returned by host⁹, or will alternatively be escorted to the Offices of the Member of the Executive Council or Head of Department by a Security Guard, upon confirmation from the receptionist.

4.5. Key Controls and Combination Locks

- 4.5.1. Security Manager must ensure effective control of and records of keys, including duplicate keys, to buildings/premises as well as to safes and strong rooms.
- 4.5.2. Key control must be managed in accordance with the Key Control Policy.

4.6. Maintenance services, repairs, and the cleaning of buildings/offices

- 4.6.1. Occupants of offices where classified or sensitive matters are dealt with must **always** be present when artisans, technicians or cleaners are performing their duties.
- 4.6.2. Special care should be taken on such occasions to ensure that they do not gain access to classified matters.

4.7. General Office Security

- 4.7.1. It is the responsibility of every employee to identify and enquire or assist strangers who are roaming about in the building or offices.
- 4.7.2. Under no circumstances must a visitor be left alone in an office where classified information is dealt with.
- 4.7.3. Cleaning services must be performed during working hours for the prevention of security breaches that might take place after hours. If such a service must be performed after hours, an agreement must be made with security for supervision.
- 4.7.4. Offices must be locked at all times when the occupant goes out, even on short periods and electrical appliances must be switched off.
- 4.7.5. Rubberstamps must be locked away when they are not in use.

⁹ An employee of the department who receives or entertains another person or member of the public as a guest

- 4.7.6. Personal items such, as handbags, briefcases, wallets, cell phones, etc. must not be left unattended.
- 4.7.7. Keys must not be left hanging in the door locks/ padlocks/ lockable facilities and padlocks/ locks to lockable facilities must be locked at all times.
- 4.7.8. The set-up of offices must be in such a way that computers do not face the office entrance.
- 4.7.9. Office windows must be closed when the office is unattended and lights must be switched off.

4.8. Private Firearms

- 4.8.1. The carrying of firearm in public place should be in accordance to Section 84 (1) and (2) of the Firearms Control Act 60 of 2000. In accordance with Section 85(1) of the Act the Minister may prescribe conditions which the Registrar may impose on the holder of a permit issued in terms of section 86. (2) The conditions which the Registrar imposes must be specified in the permit.
- 4.8.2. Notwithstanding any other provision in this policy, no person in possession of a private firearm and/or ammunition of any kind is permitted to enter Departmental premises. In such an instance, the private firearm should be handed in at reception and locked away in the gun safe provided at reception.
- 4.8.3. Proper procedures for the safe storage of firearms, including receipt and handing back procedures as well as key control must be formulated.
- 4.8.4. In terms of a Police Officer/Traffic Official on duty and carrying a private firearm, a declaration should be signed at reception by the "Officer on Duty" (Police/Traffic Officer) indicating that he/she is on official duty and is therefore compelled by law to carry a weapon. The responsibility of such weapons is the sole responsibility of the "Officers on Duty" carrying the weapons and not that of the Security Officers.
- 4.8.5. The Department will ensure that proper signage be affixed at the entrances of all premises to the effect of above paragraph.
- 4.8.6. An official residence is deemed to be a private dwelling for the purpose of this policy. Any official living in such official residence assumes full responsibility for the safekeeping and use of his/her private fire-arm(s) in terms of the relevant regulating

laws. However, in respect of official hostel-like residences, Head of Department must ensure that measures are put into place to ensure that the proper safekeeping of private firearms.

4.9. Official Firearms

4.9.1. Refer to the Firearms Policy for the Traffic Component of the Department of Transport, Safety and Liaison for the issuing of ammunition, weapons, storage of weapons, etc.

4.10. Searching

4.10.1. In terms of section 2(2) of the Access to Public Premises and Vehicles Act, 1985 the Head of Department may require that an authorised officer upon entry to public premises search any person and/or vehicle for dangerous objects. Random searches may be conducted at departmental offices after hours or at any stage.

4.11. Procurement of Private Security Services

4.11.1. Private security services, be it longer term or emergency, will be procured in terms of current statutory and other applicable prescripts.

4.11.2. To protect the Government's legal and operational interests, the Department would, as a general guideline from a security point of view, when outsourcing security services to service providers it must be verified by the departmental security manager that the service provider complies with the following conditions:

- Registration with the Security Regulating Authority in terms of the applicable legislation.
- Registration with the relevant authority in terms of the applicable trade legislation (e.g. Companies Act).
- Registration with the relevant authorities in terms of the Compensation for Occupational Injuries and Diseases Act, 1993 (Act 130 of 1993) and the Unemployment Insurance Fund.
- Registration in terms of the relevant tax legislation (income tax and value added tax).
- Accepted full responsibility in terms of section 37(2) of the Occupational Health and Safety Act, 1993 (Act 85 of 1993).

- Is in good stead with Security Regulating Authority, South African Revenue Services and other authorities indicated above.
- Subject to security clearance issued by State Security Agency () of the service provider as well as staff members.
- Has a work force that is:
 - Duly registered with the Security Regulating Authority and properly trained in terms of the Authority's requirements; and
 - Administered and managed in terms of the relevant labour laws, including the Employment Equity Act, 1998 (Act 55 of 1998), Labour Relations Act, 1995 (Act 66 of 1995) and Basic Conditions of Employment Act.
- Has the operational capacity to properly control and support all operational staff, including adequate control room facilities, communications infrastructure, transport and contingency capacity. Where required by the particular service rendered, this operational capacity must be available on a 24-hour basis.
- Is in financial good stead to reasonably cover any liabilities incurred due to the unlawful acts, omissions and/or negligence or staff in rendering services to the department, with the understanding that public liability insurance commensurate with the potential risks to which the service provider are exposed to, will suffice.

4.11.3. All service providers who bids for security services should be informed beforehand of the risk assessment and general conditions (paragraph above) as well as the procurement provisions applicable, preferably as part of the prescribed Bidder documentation to be supplied to potential bidders.

4.12. Vetting of Personnel

- 4.12.1. Head of Department assume overall responsibility to ensure that his/her personnel are vetted in terms of the relevant provisions of the MISS and this policy, including determining the various levels of security for the various personnel or categories of his/her department.
- 4.12.2. Chapter 5 of the MISS provides the following general principles/guidelines that apply in respect of security vetting:

- Security vetting is the systematic process of investigation followed in determining a member of staff's security competence¹⁰.
- The degree of security clearance given to a member of staff security is determined by the content of and/or access to classified information entailed by the post already occupied/to be occupied.
- Aspects such as gender, religion, race and political affiliation do not serve as criteria in the consideration of a security clearance, but actions and aspects adversely affecting the member of staff's vulnerability to blackmail or bribery or subversion and his loyalty to the State or institution does. This also includes compromising behaviour.
- A clearance issued is merely an indication of how the member of staff can be utilised, and does not confer any rights on such a person.
- An applicant should make a declaration of secrecy¹¹ on an official form to any government post before he/she is appointed or during the appointing process.
- Political office bearers may not be vetted.
- A security clearance gives access to classified information in accordance with the level of security clearance, subject to the need-to-know principle.

4.13. Levels of Security Clearance – New Appointees

4.13.1. In those instances where the vetting authority is not able to issue a security clearance before the expiry of the probationary period, the letter of permanent appointment must indicate that the appointment is subject to a positive security clearance as required.

4.13.2. The limitations placed on the issuing of security clearances to immigrants, persons with dual citizenship, and persons who have lived/worked abroad for long periods as set out in Chapter 5, paragraphs 3 and 4 of the MISS must be noted and adhered to.

¹⁰ The persons ability to act in such a manner that he does not cause classified information or material to fall into unauthorised hands endangering the interests of the department

¹¹ An undertaking given by a person who will have, has or has had access to classified information that he/she will treat such information as secret

4.14. Levels of Security Clearance – Serving Officials

- 4.14.1. In the case of serving officials in respect of whom the vetting authority has issued a negative recommendation the Accounting Officer of may be approached. A written request must be submitted to the Accounting Officer of, who will after consideration make a ruling.
- 4.14.2. Should the Accounting Officer not be prepared to grant approval for the issuing of clearance of those serving officials in respect of whom the vetting authority has issued a negative recommendation, such officials should be dealt with appropriately in terms of the relevant provisions of the Public Service Act, 1994, Labour Relations Act, 1995 (Act 66 of 1995) and applicable collective agreements.
- 4.14.3. As far as the transfer of officials are concerned, the Head of the receiving Department must indicate whether the official's existing security clearance is acceptable, or whether a new clearance should be requested.
- 4.14.4. Officials, who refuse to be subjected to security vetting and/or refuse to sign the prescribed declaration of secrecy, must be dealt with in a manner similar to that indicated in paragraph 4.14.2 above.

4.15. Security Clearances – Contractors Supplying Services to the Department

- 4.15.1. Head of Department must determine the security risks involved with the appointment of private contractors, including the need for and level of security clearances required, to conduct a prior vetting of the Company in question.
- 4.15.2. Where specific security requirements have to be met by the contractor, these requirements must be contractually agreed to before commencement of service.

4.16. Period of Validity of Security Clearances

- 4.16.1. Top secret¹²: 5 years
- 4.16.2. Secret¹³: 5 years
- 4.16.3. Confidential¹⁴: 10 years

¹² Relates to all information that may be used by malicious, opposing or hostile elements to neutralise the objectives and functions of the department

¹³ Relates to information that may be used by malicious, opposing or hostile elements to disrupt the objectives and functions of the department

4.16.4. The abovementioned requirement does not preclude re-screening at shorter intervals if so required.

4.17. Records – Security Clearances

4.17.1. The Security manager must keep records of the following:

4.17.1.1. All security clearances issued by the screening authority, including contractors and temporary personnel.

4.17.1.2. All serving officials in respect of whom the screening authority has made a negative recommendation.

4.18. Broad Procedures for Requesting Security Clearances

4.18.1. New appointees: Requests must be submitted to the Security Manager by the departmental Human Resource Division who deals with the appointment and the eNatis office which deals with Municipalities Driving Learner Training Centres (DLTC's).

4.18.2. Serving officials: Security Manager to advise supervisors of lapsed security clearance at least six months before the validity period expires.

4.18.3. Contractors: The responsible Head of component must submit requests to the Security Manager.

4.18.4. The Security Manager will provide the necessary documentation to be completed by the individuals concerned, and arrange for the taking of the required fingerprints.

4.18.5. The completed documentation and fingerprints will be submitted to the screening authority by the Security Manager.

4.18.6. The security clearance recommendation of the vetting authority will then be submitted by the Security Manager to the Head of Department (or his delegate) for final acceptance.

4.19. Document Security

4.19.1. The Department of Transport, Safety and Liaison is in possession of information that is to some extent sensitive in nature and this obviously requires security measures.

¹⁴ Relates to information that may be used by malicious, opposing or hostile elements to harm the objectives and functions of the department

The degree of sensitivity will determine the level of protection needed to safeguard this information. This implies that the information needs to be graded or classified according to the sensitivity thereof. Every classification¹⁵ necessitates certain security measures with respect to the protection of such sensitive information, which such classification is known as the Grading of the document.

4.19.2. Should the author of a document on which there is no embargo, reconsider the classification of such document, he/she must inform all addressees of the new classification.

4.19.3. The receiver of a classified document, who is of the opinion that the document concerned must be reclassified, must obtain oral or written authorisation from the author, the Head of the Component institution or his/her delegates, such authorisation must be indicated on the relevant document when it is reclassified.

4.19.4. When a document is classified, the classification assigned to it must be indicated clearly on the document in the following way:

- The classification of loose and not permanently bound documents and bound volumes (books, publications, pamphlets) and other documents that are securely and permanently bound is typed/printed or stamped together at the top and the bottom (preferably in the middle) of every page (including the cover).
- Security classifications should be indicated on copies, photographs, sketches, etc. by means of rubber stamps. The exact position of the mark may vary, depending on the nature of the document, so that the stamp does not obscure essential details. An effort must, however, be made to mark the document as clearly as possible, so that the mark will immediately attract attention.
- Tracings or blueprints should be marked in such a way that the security classification is visible on all copies. Where this is not possible, rubber stamps should be used to mark all the copies.
- Tape recordings and documents on which no marks can be made and where it is physically impossible to place clear classification marks on a document itself, the document should be placed in a suitable box, envelope or other container and, if

¹⁵ The grading of a document in accordance with its sensitivity or in compliance with security requirements

necessary, sealed, and the nature and classification of the contents clearly marked on the outside of the container.

- For files, a clear distinguishing mark, the significance of which is known to those who deal with the file concerned should be placed on both the front and the back cover of Secret or Top-Secret files.
- Unclassified sensitive document(s) received from any institution for the use or storage within the Department of Transport, Safety and Liaison must be classified accordingly by the first receiver and be treated subsequently according to the classification marked.
- Where necessary, the author of such document as explained must be consulted for more information before the document is graded.

4.20. Access to Classified Information

4.20.1. The general rules and prescriptions as to who may have access to or inspect classified matters are as follows:

- Persons who have appropriate security clearance or who are by the way of exception authorised thereto by the Head Department or his/her delegate, with due regard being paid to the need-to-know principle.

4.21. Handling of Classified Documents

4.21.1. All classified documents must be stored in accordance with MISS instructions whilst not in use.

4.21.2. The particulars of classified postal material must be entered in a register. The registers for the Secret and Top-Secret documents must be classified accordingly. The registers must comply with the provisions as contained in the MISS Chapter 4.

4.22. Bulk Conveyance of Classified Documents

4.22.1. When classified documents have to be conveyed in bulk by road, rail or air, the appropriate precautions must be taken for the protection thereof.

4.23. Diplomatic Bags

- 4.23.1. Should it become necessary for the Department to ship classified documents by use of diplomatic bags, it must be co-ordinated by the relevant Component with the Department of Foreign Affairs. (See MISS Chapter 4)
- 4.23.2. The Head of the Department must ensure that the directives of the Department of Foreign Affairs are complied with, until the completion of such shipment.
- 4.23.3. Notwithstanding the directives of the Department of Foreign Affairs, the directives of this policy shall apply to sensitive documents as contemplated on Chapter 4.

4.24. Storage of Classified Documents

- 4.24.1. Classified documents that are not in immediate use must be locked away in a safe storage place according to classification level
- Confidential: Reinforced filing cabinet
 - Secret: Strong room or reinforced filing cabinet
 - Top Secret: Strong room, safe or walk-in safe
- 4.24.2. The keys to any building, part of a building, room, strong room, safe, cabinet, or any other place where classified material is kept must be locked away after which utmost care and effective key control must be instituted. The keeping of the necessary key registers and the safe custody of duplicate keys and control over such keys must be strictly adhered to. The Security Manager must be consulted for assistance in this regard.
- 4.24.3. The keys to safes and strong rooms must be kept in safe custody in accordance with the key control policy.
- 4.24.4. If a strong room or safe is fitted with a combination lock, the combination must, apart from being reset when it is purchased, be changed at least once every three months, or on the following occasions:
- When it is suspected that it has been compromised¹⁶ or tampered with.
 - On resumption of duty by the responsible officer after a continuous period of absence, whether on vacation leave or for official reasons, if the combination had necessarily to

¹⁶ Unauthorised disclosure or exposure or loss of sensitive information or exposure of sensitive operations, people or place whether by design or through negligence

be made known to some other person for use during the period concerned. The inspection of the contents of such safe or strong-room must be done in the presence of any such person who had been in control of such container, be a safe or strong-room.

- When a new user takes over.

4.24.5. Combinations may be comprised if:

- Unauthorised persons noting the combination through observation when the lock is opened.
- Failure to set the combination in accordance with the manufacturer's specifications.
- Failure to change the combination after a reasonable period, or writing of the combination on the piece of paper, which could easily be misplaced.

4.24.6. Precautions must therefore be taken by the authorised user to ensure that no other person is present when the new combination is set or the lock is opened. When a combination is reset, the following rules should be adhered to with:

- The figures making up a specific combination should not be used more than once in succession, even if they are in a different order.
- Avoid the use of numbers with some personal significance, e.g. age, date of birth, telephone numbers, street addresses and numbers of safes, etc. Also avoid the figures zero (0), five (5), ten (10) and multiples of the last two. High and low numbers should preferably be used alternately (e.g. 68-13-57-11).
- Only the user may set a combination lock.

4.24.7. Knowledge of a combination should be restricted to the minimum number of persons desirable on the grounds of operational requirements, e.g., in the case of a communal safe.

4.24.8. After the combination has been reset, the new combination must be handed to the key custodian or other person designated for the purpose, in a sealed envelope for safe custody, so that he can complete the combination lock register.

4.24.9. As far as safe and strong room keys and the combinations of cryptographic centres are concerned, the requirements contained in the Communication Security Instructions of SACS must be complied with.

4.24.10. Access to any controlled building, part of a building or room where classified information is handled/stored outside normal office hours should be prohibited to all

persons who do not work there. Repairs to and the cleaning of such premises must take place in the presence and under supervision of persons who work there.

- 4.24.11. Persons who have to gain access to a building after hours must be duly authorised by the Head of the Department or his/her delegate. The Security Manager must take appropriate steps to arrange access and record keeping.

4.25. Removal of Classified Documents from Premises

- 4.25.1. The removal of classified documents from office buildings must be prohibited as far as possible.
- 4.25.2. Classified material may not be taken home without the written approval of the Head of the Department or his/her delegate; a list of the documents to be removed must be handed to the person in control of record keeping.
- 4.25.3. Persons may take classified documents home only if they have proper lock-up facilities. If a person has no such facilities, the documents may not be kept at such a person's home for the purpose of work after hours.
- 4.25.4. Classified documents taken out of a building with a view to utilise at meetings or appointments must be removed in a lockable security attaché case.

4.26. Typing of Classified Documents

- 4.26.1. Only persons having the appropriate security clearance may type classified documents. Such typing must be done in a manner that will ensure that the information is not divulged to unauthorised persons.
- 4.26.2. Drafts of classified documents, typewriter ribbons, flash disks and copies and floppy disks must at all times be treated as classified documents.

4.27. Destruction of Classified Documents

- 4.27.1. In terms of the Archives Act, 1996 (Act 43 of 1996), all documents received or created in a government office whilst conducting affairs of such office are subject to the Act, except where they are excluded due to their very nature or the prescriptions of some or other Act of Parliament. It should be a point of departure that all state

documentation is subject to the Archives Act, unless justifiably excluded along the above-mentioned lines.

4.27.2. It should be noted that no document is to be excluded merely because it is classified.

4.27.3. The Head of Department will have to decide, after consultation with their legal advisers as well as the Director: State Archives whether the document(s) concerned is/are of such a nature that there is a legitimate demand for secrecy that goes beyond the degree of safekeeping by the State Archives.

4.27.4. Where destruction has been properly authorized, it should take place by burning or some other approved method, e.g., by means of a shredder (in the latter case – preferably a cross-cut machine), in which case the strips may be no wider than 1,5mm.

4.27.5. The person who has destroyed the documents must provide a certificate of destruction of the documents concerned to the Head of the Department or Security Manager.

4.28. Photocopying of Classified Documents

4.28.1. All mechanical/electronic reproduction appliances should be properly controlled to prevent the unauthorised or uncontrolled copying of classified documents. This apparatus must therefore either be centralised or distributed and be under the direct control of an authorised and appropriately cleared officer.

4.28.2. The relevant component/institution must keep a record of all the reproductions of classified documents at its disposal. The register must contain the following particulars: Date, Person requesting copies/reproduction, Classification, File reference, Heading/nature of documents, Purpose of the copies, Number of copies, Meter reading before and after copying.

4.29. Communication Security – Personal Security

4.29.1. In terms of the Protection of Information Act, 1982 (Act 84 of 1982) all personnel who potentially have access to classified information are required to sign a prescribed declaration of secrecy, which prohibits the unauthorised release of official information.

4.29.2. All personnel appointed in terms of the Public Service Act, 1994 (Proclamation 103 of 1994) must note and adhere to Regulation 20 of the Public Service Regulations, 2016

that deals with the handling of official information and documents: “An employee shall not release official information unless she or he has the necessary authority”.

4.29.3. Due cognisance must also be taken to the provisions of the Promotion of Access to Information Act, 2000 (Act 2 of 2000).

4.29.4. No classified information may be conveyed via telephone, fax, cellular phone or any other communication equipment/aids unless both the sender and receiver use appropriate encryption equipment.

4.29.5. The Security Manager will co-ordinate the acquisition and maintenance of security equipment.

4.29.6. Communication security equipment will be acquired from and maintained by the South African Communication Security Agency (SACSA) as nationally designated sole provider of such equipment.

4.29.7. No cellular phones will be allowed in areas where sensitive matters are discussed, i.e., conference rooms.

4.29.8. Offices, conferences rooms and other places where classified matters are discussed should, apart from effective access control, be secured by means of periodic technical/electronic surveillance counter measures (“sweeping”).

4.29.9. The need for and frequency of such measures will be determined by the Head of Department in consultation with the Security Manager. The Head of Department in writing must provide specific authorisation.

4.29.10. All technical/electronic surveillance counter measures will be executed only by the Head of Department or any person/institution designated by the Head of Department in writing.

4.30. Communication Security – Personal Security

4.30.1. Computer Security¹⁷ does not focus only on the per se, but most especially to the information contained in the computer database as well as in the computer apparatus. In the light of the increasing dependence on and the proliferation of computers in

¹⁷ The condition created in a computer environment by the conscious provision and application of security measures which includes information concerning the procedure for procurement and protection of equipment

Government and also of the extent to which classified information is processed by means of computers, security has become essential in this area.

4.30.2. All computer storage media (usually magnetic or optical) are documents in terms of the definition in the Protection of Information Act, 1982 (Act 84 of 1982). These documents, when containing classified information, must be handled according to the document security standards as described in Chapter 4 of MISS.

4.30.3. It is the responsibility of the Head of the Department or his/her delegate to ensure that all personnel concerned with computers receive the necessary security training. In addition, the security awareness of all personnel using computers must receive regular attention.

4.30.4. Against this background the following measures must be implemented:

- Essential backup of computer system and data;
- Physical security measures as prescribed;
- Computer security responsibilities should be clearly established;
- The allocation and use of passwords as prescribed on all sensitive and classified documents, including e-mail.

4.30.5. All breaches of security in the computer environment must be reported as soon as possible.

4.30.6. In cases of uncertainty regarding the implementation or appropriateness of security measures in the computer environment, the Security Manager must be approached to arrange for assistance.

4.31. Contingency Plans

4.31.1. Head of Department must ensure that proper contingency planning¹⁸ is affected for all public premises under his/her control. Contingency planning in this regard refers to prior planning to prevent, combat and/or counteract the effect of an emergency situation where lives, property or information are threatened. This includes compiling, approving, and distributing a formal written plan, and the practice thereof to identify and rectify gaps in and to familiarise employees with the plan.

¹⁸ The prior planning of any action that has the purpose to prevent and or combat or counteract the effects and results of an emergency situation where lives, property or information is threatened.

4.31.2. In compiling contingency plans and measures (such as emergency evacuations, fire prevention and control, first aid and training emergency personnel) cognisance must be taken of the relevant provisions of the MISS and of the statutory requirements contained in, among others, the following laws:

- National and Local Government Disaster management/By-laws relating to Community Fire Safety.
- Hazardous Substances Act, 1973 (Act 15 of 1973)
- National Building Regulations and Building Standards Act, 1977 (Act 103 of 1977).
- Occupational Health and Safety Act, 1993 (Act 85 of 1993)

4.32. Security Breaches

4.32.1. The Security Manager must issue clear instructions and procedures to ensure that all breaches of security are reported.

4.32.2. The Security Manager will investigate security breaches and recommend remedial actions, including preventative measures and possible disciplinary actions where appropriate.

4.32.3. Normal reporting of incidences to the SAPS applies to effect possible criminal investigation.

4.32.4. Incidences of an economic nature must also be reported to the Security Manager who will report serious security breaches to the SSA and request their involvement in follow-up investigations where appropriate. Reporting to the Security Manager is also required to ensure ongoing and up-dated security assessments.

4.33. Monitoring Compliance

4.33.1. Compliance with the implementation of this policy will be monitored by the security audits on a quarterly or adhoc basis. In addition to the security audits that the State Security Agency will initiate on its own accord in pursuance of its statutory mandate the Head of Department may request the State Security Agency to conduct security audits at his/her department, or specific components thereof, to determine compliance with security policies and the state of preparedness.

4.33.2. 22.2 Further compliance of the security policy will be accomplished by after hour's inspections, site inspections, spot checks.

5. Roles and Responsibilities

5.1. *The Head of Department is responsible for:*

5.1.1. Overall responsibility for the provision and maintenance of security at all provincial premises/buildings.

5.2. *Security Manager is responsible for:*

5.2.1. Overall control, co-ordination of all security personnel and matters in the Department.

5.2.2. Establishment of the security committee comprising of representatives of all Senior Managers in the department.

5.2.3. Ensuring that policies, procedures and standards are maintained throughout the department and regional/satellite offices.

5.2.4. Identifying all risks and threats to the security of the institution, as well as vulnerabilities in the institution's capacity to counter these. Base security planning on the risk level.

5.2.5. Advising management about the security implications of management decisions.

5.2.6. Ensuring appropriate security awareness programmes are in place within the Department.

5.2.7. Implementing the security policy in the department and to provide guidance for the implementation thereof.

5.2.8. The general, scientific and systematic gathering and assessing of all information relating to security risks that will impede the continuity of the Department's business operations due to attack/s or catastrophic events and plan according.

5.2.9. Protecting the Department's integrity, stakeholders, processes and assets.

5.2.10. Monitoring the extent of adherence/compliance to the security policy and measures, including the screening of officials with access to sensitive information.

5.2.11. Liaising regularly with employees for advice, assistance and information regarding information security.

- 5.2.12. Reporting all incidents or suspected incidents of security breaches and/or leakages of sensitive information, for investigation and to keep records of all incidents (e.g. leakage, thefts/burglaries, tampering with security systems, etc. in an Incident Register.
- 5.2.13. Liaising with the South African Police Services about all physical security needs, problems, etc. to ensure effective security (e.g., key control, access control and other security equipment/installations).
- 5.2.14. Ensuring the proper administration of vetting applications, including keeping of a record of security clearances issued, ensuring the completeness of vetting applications before forwarding to the vetting institution, a process/procedure to ensure timeous re-vetting.
- 5.2.15. Initiating corrective / disciplinary steps in cases of non-adherence, in line with the policy about misconduct.
- 5.2.16. Evaluating and improving the effectiveness of security measures and procedures from time to time.
- 5.2.17. With the assistance of the IT personnel, or once the OFE System Network is in place, perform Personal Computer and laptop screening from time to time to ensure there is a proper security data base.
- 5.2.18. Performing after hour inspections in offices on the premises belonging to the Department of Transport, Safety and Liaison, accompanied by the Head / Manager / Supervisor of each respective Division within the Department.
- 5.2.19. The Security Manager, after consultation with the designated structures of the State Security Agency (SSA) and the South African Police Service, must at least on a quarterly basis present a threat and risk assessment to Head of Department and Management. This risk assessment must address the Department's vulnerabilities/risks in respect of physical, personnel, document, and communication and information technology security.

5.3. *Security Committee is responsible for:*

- 5.3.1. Identifying categories of information that require protection.
- 5.3.2. Identifying which components in the department handles such information.

- 5.3.3. Identifying who may require access to such information (internal/external).
- 5.3.4. Identifying the physical area where the information is handled or stored.
- 5.3.5. Identifying history of security breaches with regard to information.
- 5.3.6. Consulting with the security manager to identify trends with regard to the compromise of information.
- 5.3.7. Assisting the Security Manager with conducting of Threat and Risk Assessment.
- 5.3.8. Assisting the Security Manager with the drafting and reviewing of the security policy, plan and procedures.
- 5.3.9. Assisting with Security Awareness Programmes.

5.4. *Management/Employees are responsible for:*

- 5.4.1. Co-operating in all anti-loss systems and an awareness of the need for security.
- 5.4.2. Locking away valuable assets and sensitive documents in cabinets when not in use.
- 5.4.3. Securing their workstations/office layout and restricting access/entrance.
- 5.4.4. Disposing of classified/sensitive papers in the prescribed manner (shredding).
- 5.4.5. Not storing or saving sensitive/classified information on laptops.
- 5.4.6. Reporting suspicious visitors to security.
- 5.4.7. Reporting suspected security breaches (e.g., theft).
- 5.4.8. Looking after their keys/access control cards and ensuring that such keys/access control cards do not fall into the wrong hands
- 5.4.9. The safe keeping of laptops/flash disks when not in use.
- 5.4.10. Management must keep photocopiers, printers, fax machines under constant supervision to ensure that no unauthorised transmissions of classified/sensitive documents take place or unauthorised copies are made:
 - All members to complete Control Registers at Copy Machines;
 - All members to complete Fax-in and Fax-out Control Registers when sending or receiving faxes.
- 5.4.11. Senior Managers/Divisional Heads are responsible for the implementation of all security measures within their components, floor/blocks and units. The Senior Managers/Divisional Heads are also representatives to assist with the implementation of

security measures in their components. This applies to all Departmental buildings and offices.

6. Review and Distribution

- 6.1.** The senior manager for Corporate Services is responsible for this policy and for ensuring that it is reviewed and updated.
- 6.2.** This Policy will be reviewed after 18 months but no later than 3 years of the last publication date. If necessary, an updated version will be issued, if not a formal cover letter will be issued to supplement the cover of this Policy (identifying a revised publication date).
- 6.3.** The senior manager for Policy & Planning will distribute updated versions to:
- Member of the Executive Council
 - Head of Department
 - All senior managers who will in turn distribute to their staff as appropriate.