agriculture &
rural development
Department:
Agriculture and Rural Development
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

Organisation	Department of Agriculture And Rural Development		
Policy	Security Management Policy	Section: Security Services	Department: DARD
Revision	Annually	Effective Date	Once approved
Preparer	Security Services	Signature	
Approver	HOD	Signature	

Table of Contents

1. PREAMBLE

1.1 The Department of Agriculture and Rural Development (DARD) recognises the importance of an effective security policy to protect and safeguard its employees, assets, information, integrity and reputation from potential threats. In accordance with all security legislation and prescripts governing the directives on Departmental Security Management, this policy strives to provide baseline measures for the implementation of the minimum physical and information security requirements, and to provide consistent protection in this regard.

1.2 The Sub-Directorate: Security Services' commitment is guided by the basic core values, code of conduct and ethics which enhance and contribute to professionalism, respect for employees and stakeholders and a permanent concern for health, safety and the holistic protection of the DARD environment. This Security Policy is based on and guided by the Minimum Information Security Standards, Minimum Physical Security Standards and other relevant legislations and prescripts and is in no way intended to replace any of the above mentioned legislation, prescripts, guidelines or directives

2. STATEMENT OF PURPOSE

2.1 The Department of Agriculture and Rural Development depends on its personnel, information and assets to deliver services that ensure the health, 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.

2.2 Threats that can cause harm to the Department, in the country and abroad, includes but are not limited to the following: Act of terror, sabotage, espionage, unauthorized access to building and premises, theft, armed robbery, fraud and corruption, vandalism, fire, natural disaster and accidental damage. The threat of

cyber-attack and malicious activity through the internet is prevalent and can cause severe harm to electronic 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.

2.3 The Security Policy prescribes the application of security measures to reduce the risk of harm that can be caused to the department if the above mentioned threats should materialize. It has been designed to protect employees, preserve the confidentiality, integrity, availability and value of information and assets, and assure the continued delivery of service. 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 compiled with by employees.

2.4 The main objective of this policy therefore is to support the national interest and the Department business objectives by protecting employees, information and assets and assuring the continued delivery of services to South African citizens.

2.5 This policy complements other Departmental policies (e.g. Human Resource Management, Occupational Health and Safety, Information Management, Assets Control, Real Property and Financial Resources.

3. DEFINITION OF TERMS

3.1 The following definitions, words, phrases and terminology have the same and/or similar meaning unless the context indicates otherwise:-

- "Accreditation" means the official authorization by management for the operation of the information and communication technology (ICT) system, and an acceptance by that management of the associated residual risk. Accreditation is based on the certification process as well as other management considerations.
- "Assets" mean material and immaterial property of the department. 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 international 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.

- "Certification" means the issuing of a certificate certifying that a 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.

- "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" has the meaning assigned thereto in the Information Act, 1982 (Act No. 22 of 1982).

- "Document security" means the conscious provision and application of security measures in order to protect classified/sensitive documents.

- "Employees" for the purpose of this policy includes: permanent staff; temporary/casual staff; national and foreign seconded employees; and non-employees, i.e. employed by the Department of Agriculture, Forestry and Fisheries either individually or through its firms, and/or consultants.

- "Information security" means the condition created by the conscious provision and application of a system or document, personnel, physical, computer and communication security measures to protect sensitive information.

- "Key control" means the effective management, control and safekeeping of departmental keys.

- "National Intelligence Structures" has the meaning assigned thereto in the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994).

- "Need-to-know principle" means the furnishing of only that classified information or part thereof that will enable a person/s to carry out his/her/their task.

- "Persons" means applicants or employees.

- "Premises" for the purpose of this security manual, refer to 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 of Agriculture and Rural Development to which a member of the public has a right of access.

- "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 materializing by exploitation of vulnerability.
- "Screening/Vetting institution" means the South African Police Service, the State Security Agency, South African Secret Service or the South African National Defence Force that, in terms of the rationalization agreement, are responsible for the security screening/vetting of persons within their jurisdictions. The SSA also has a legal mandate to employees within the public service.

- "Security breach" means the negligent or intentional transgression of or failure to comply with security measures.

- "Service providers" means close corporations, companies and any other business entities.

- "Technical Surveillance Counter measures" (TSCM) 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 or accidental, which 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 event.

- "Visitors/Contractors" mean non-employees.

- "Vulnerability" means a deficiency related to security that could permit a threat to materialize.
- "Top secret" relates to all information that may be used by malicious/opposing/hostile elements to neutralize the objectives and functions of the department and/or state.

- "Transmission security" means communication security and entails the safeguarding and secure use of systems linked to one another for the sake of communication.

- "Work stations" means security offices, stores, behind counter of cashier in finance, control room, laboratories, registries, kitchens, photocopy room, library, etc.

- "Biometrics" means a way of measuring and using an individual's physical characteristics for verifying his/her identity. This information is stored by DARD about an individual's physical characteristics that can be used to identify that person. Biometric Information can include, but is not limited to: fingerprints; voice patterns; face, hand, and other biological traits that can be used to identify an individual.

- *"Unwanted individual"* A person who has been suspended or dismissed, or whose employment or any contract with DARD has been terminated

- "Electronic Security Systems" refers to the use of computer software and electronic devices to carry out a host of security functions to enhance the protection of designated area.

4. ABBREVIATIONS

The abbreviations hereinafter have the following meaning allocated to them:-

HOD	:	Head of Department
COMSEC	:	Electronic Communications Security (Pty) Ltd
DARD	:	Department of Agriculture and Rural Development
ICT	:	Director: Information and Communication Technology.
SM		Deputy Director: Security Manager
GITO	:	Government Information Technology Officers.
SANDF	:	South African National Defense Force.
SAPS	:	South African Police Service.

SASS	:	South African Secret Service.
SMS	:	Senior Management Service.
SSA	:	State Security Agency
IT Manager		Senior Manager for the departmental Information and Technology
ESS	:	Electronic Security Systems
CCTV	:	Closed Circuit Television

5. LEGISLATIVE FRAMEWORK

The following primary and secondary legislation informs and regulates the Security Policy:-

- Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996)
- Control of Access to Public Premises and Vehicles Act, 1985 (Act No. 53 of 1985)
- Copyright Act, 1978 (Act No. 98 of 1978)
- Criminal Procedures Act, 1977 (Act No. 51 of 1977), as amended.
- Electronic Communication and Transaction Act, 2002 (Act No. 25 of 2002)
- Electronic Communication Security (Pty) Ltd Act, 2002 (Act No. 68 of 2002)
- Employment Equity Act, 1998 (Act No. 55 of 1998)
- Firearms Control Act, 2000 (Act No. 60 of 2000)
- Firearms Control Regulations, 2004
- Intimidation Act, 1982 (Act No. 72 of 1982)
- Labour Relations Act, 1995 (Act No. 66 of 1995)
- National Archives and Record Services of South Africa Act, 1996 (Act No. 43 of 1996)
- National Archives and Record Service of South Africa Regulations, 2002
- National Building Regulations and Building Standards Act, 1977 (Act No. 103 of 1977)
- NIA Guidance Documents: ICT Policy and Standards: Part 1 and 2
- National Key Points Act, 1980 (Act No. 102 of 1980)
- National Strategic Intelligence Act, 1994 (Act No. 39 of 1994)
- Non-proliferation of Weapons of Mass Destruction Act, 1993 (Act No. 87 of 1993)

- Occupational Health and Safety Act, 1993 (Act No. 85 of 1993)
- Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 12 of 2004)
- Private Security Industry Regulations Act, 2001 (Act No. 56 of 2001)
- Protected Disclosures Act, 2000 (Act No. 26 of 2000)
- Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)
- Promotion of Administrative Justice Act, 2000 (Act No. 3 of 2000)
- Protection of Constitutional Democracy against Terrorism and Related Activities Act, 2004 (Act No. 33 of 2004)
- Protection of Information Act, 1982 (Act No. 84 of 1982)
- Public Finance Management Act, 1999 (Act No. 1 of 1999)
- Treasury Regulations, 2005
- Public Service Act, 1994
- Public Service Regulations, 2001
- State Information Technology Agency Act, 1998 (Act No. 88 of 1998)
- Trespass Act, 1959 (Act No. 6 of 1959)
- White Paper on Intelligence (1995)
- Minimum Information Security Standards (MISS), 1996
- Minimum Physical Security Standards (MPSS) 2009
- POPIA

6. SCOPE

6.1 This policy applies to the following individuals and entities:

- All employees, interns of Department of Agriculture and Rural Development;
- All contractors and consultants delivering a service to the department, including their employees who may interact with the department;
- Temporary employees of department;
- All information assets of department;
- All intellectual property of department;
- All fixed property that is owned or leased by department;
- All movable property that is owned or leased by department;
- All biological assets of department

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

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

7. POLICY STATEMENT

7.1 General

Employees must be protected against identified threats according to baseline security requirements and continuous security risk management.
Information and assets of department must be protected according to baseline security requirements and continuous security risk management.
Continued service delivery of department must be assured through baseline security requirements, including business continuity planning, and continuous security risk management.

7.2 Compliance requirements

7.2.1 All individuals mentioned in Para.8.1 below must comply with baseline requirements of this policy and its associated Security Directives as contained in the Security Procedure Manual. These requirements are/shall be 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 continual updating of the security TRA's.

7.2.2 Security threat and risk assessments involve:

- 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 department 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.

7.2.3 Staff accountability and acceptable use of assets

7.2.3.1 The HOD shall ensure that information and assets of department are used in accordance with procedures as stipulated in the Security Directives as contained in the Security Procedure Manual.

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

8. POLICY IMPLEMENTATION

8.1 Senior Managers, Managers and Supervisors shall be responsible for implementation of this policy in their respective components. Each employee is obliged to ensure adherence to this policy and applicable prescripts.

8.2 Employees who are considered to be in transgression of this policy may be subjected to the disciplinary code and procedures applicable in the Public Service.

9. POLICY ENFORCEMENT

9.1 The HOD and the appointed SM are responsible for the enforcement of this policy.

9.2 All employees are required to fully comply with this policy and its associated security directives. Non-compliance with any prescripts shall be addressed in terms of the Disciplinary Code and/or any other relevant.

9.3 SPECIFIC BASELINE REQUIREMENTS

9.3.1 Security Organization

9.3.1.1 The HOD will appoint/ has appointed a Security Manager (SM) to establish and direct a security program that will ensure co-ordination of all policy functions and implementation of policy requirements.

9.3.1.2 Given the importance of this role, a Security Manager with sufficient security experience and training who is strategically positioned within the department so as to provide institution-wide strategic advice and guidance to senior management.

9.3.1.3 The HOD will ensure that the Security Manager has an effective support structure (security component) to fulfill the functions referred to.

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

9.3.2 SECURITY ADMINISTRATION

9.3.2.1 The functions referred in Para. 9.3.1 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;

- Ensuring the protection of information;
- Ensuring ICT security;
- Ensuring security in emergency and increased threat situations;
- Facilitation business continuity planning;
- Ensuring security in contracting; and
- Facilitating security breach reporting and investigations

9.3.2.2 Security incidents/breaches reporting process

9.3.2.2.1 Whenever an employee becomes aware of an incident that might constitute a security breach or an unauthorized disclosure of information (whether accidentally), he/she shall report that to the Security Manager by utilizing the formal reporting procedure prescribed in the Security Procedure Manual.

9.3.2.2.2 The HOD shall report to the appropriate authority (as indicated in the Security Procedure Manual) all cases or suspected cases of security breaches, for investigation.

9.3.2.2.3 The Security Manager shall ensure that all employees are informed about the procedure for reporting security breaches.

9.3.2.3 Security incident/breaches response process

9.3.2.3.1 The Security Manager shall develop and implement security breach response mechanisms for department in order to address all security breaches/alleged breaches which are reported.

9.3.2.3.2 The Security Manager shall ensure that the HOD is advised of such incidents as soon as possible.

9.3.2.3.3 It shall be the responsibility of the National Intelligence Structure (e.g. the SSA or SAPS) to conduct an investigation on reported security breaches and provide feedback with recommendations to the department.

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

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

9.3.3 INFORMATION SECURITY

9.3.3.1 Categorization of information and information classification system

9.3.3.1.1 The Security Manager, together with Records Management must ensure that a comprehensive information classifications system is developed for and implemented in the department. All sensitive information produced or processed by department must be identified, categorized and classified according to the origin of its source and contents and according to its sensitivity to loss or disclosure.

9.3.3.1.2 All sensitive information must be categorized into one of the following categories:

- State Secret;
- Trade Secret; and
- Personal Information

9.3.3.1.3 And subsequently classified according to its level of sensitive by using one of the recognized levels of classification:

- Confidential;
- Secret; and
- Top Secret

9.3.3.1.4 Employees who generate sensitive information are responsible for determining information classification levels and the classification thereof,

subject to management review. This responsibility includes the labeling of classified documents.

9.3.3.1.5 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.

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

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

9.3.4 PHYSICAL SECURITY

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

9.3.4.2 Physical security measures must be developed, implemented and maintained in order to ensure that the entire department, its personnel, assets, 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 Security Manager

9.3.4.3 The department shall ensure that physical security is fully integrated early in the process of planning, selecting, designing and modifying of its facilities. The department shall:

- Select, design and modify facilities in order to facilitate 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

9.3.4.4 The department will also ensure the implementation of appropriate physical security measures for the secure storage, transmittal and disposal of classified and protected information in all forms.

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

9.3.5 PERSONNEL SECURITY

9.3.5.1 Security Vetting

9.3.5.1.1 All employees, contractors and consultants of department, who requires access to classified information and critical assets in order to perform his/her duties or functions, must be subjected to a security vetting investigation conducted by the State Security Agency (SSA) in order to be granted a security clearance at the appropriate level.

9.3.5.1.2 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.

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

9.3.5.1.4 A declaration of secrecy shall be signed by every individual issued with security clearance form to complete the entire security vetting process. This will remain valid even after the individual has terminated his/her services with the department.

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

9.3.5.1.6 Security clearances in respect of all individuals who have terminated their services with department shall be immediately withdrawn.

9.3.5.2 Polygraph Examination

9.3.5.2.1 A polygraph examination shall be utilized to provide support to the security vetting 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.

9.3.5.2.2 In the event of any negative information being obtained with regard to the applicant during the security vetting 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.

9.3.5.3 Transferability of Security Clearance

9.3.5.3.1 A security clearance issued in respect of an official from other government institution shall not be automatically transferable to the DARD.

9.3.5.4 Security Awareness and Training

9.3.5.4.1 A security training and awareness program must be developed and implemented by Security Manager to effectively ensure that all personnel and service providers remain security conscious.

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

9.3.5.4.3 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 presentations.

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

9.3.5.4.5 Personnel Suitability Checks

The DARD must ensure compliance to personnel suitability checks. The pre-employment security screening is a mere preliminary record check to verify the integrity and does not constitute a security clearance
The pre-employment screening is applicable to all job applicants or employees, for permanent and temporary posts. The process is outlined in the Security Procedure Manual

after an 9.3.6 Electronic Security System (CCTV and Biometric access system)

9.3.6.1 Closed Circuit Television

Video surveillance solutions have three main purposes:

- Deterrence (through visible elements such as cameras and quick-response measures by Security Officers)
- Live monitoring (e.g. perimeter monitoring or vehicle license plate recognition)
- Support of investigations incident occurs (including identification of persons)

9.3.6.2 When installing CCTV in the Department, several components will be taken into consideration, such as the location of the cameras and the reasons for such installations.

9.3.6.3 The deployment of the surveillance or biometric access control system in DARD premises does not automatically result in a secure physical environment. These systems are tools that still require effective security people and processes to administer them and act on alarms or other information generated by the system

9.3.6.4 The CCTV system is accessed from a secure area and controlled by the CCTV managers and operators. The DARD Security Services will ensure the following:

- That a clear procedure exists for requesting, viewing, accessing and disclosing CCTV footages and a record kept of all requests •
- CCTV footage is stored securely and access is protected and limited to authorised personnel
- CCTV footage will be kept for a maximum of 30 days, unless an incident has occurred on DARD premises and the footage is to be kept for a purpose
- CCTV viewing may be carried out on request and upon completion and approval of CCTV Footage Disclosure Register.

9.3.6.5 In cases where disclosure is requested by a third party who does not appear on the footage, extreme caution must be taken and referred to the HOD. Where technology permits, images of third parties will be blurred and unidentifiable if a disclosure request does not pertain to them.

9.3.6.6 The data may be used within the Department's Disciplinary Procedures as required, and will be subject to the normal confidentiality requirements of those procedures

Biometric access system

The following are amongst the reasons the DARD is immigrating to the biometric access system:

- With biometric reader access control, DARD's Security Services can manage entry to its premises and movement between different areas.
- Assign accessible areas to staff members.
- Monitor movement between secured areas and maintain a full record of all accesses.
- Restrict sensitive areas such as MEC's office, HOD's office and more.
- Biometric readers operate by scanning fingerprints or facial recognition, so we will always know who went where, and for how long

Among the biometric modalities, fingerprint is by far the most-used and most mature and well-understood.

However, the need to remove physical contact during COVID 19 pandemic has prompted consideration of alternative touch-less metrics such as face recognition, which DARD is using.

There are rare individuals whose biometrics (whatever type) cannot be accurately captured or measured, and hence they can either not be enrolled in the system, or they cannot be verified by the system. Provision will be made for such users by allowing alternatives such as remotes, passwords or even dual-mode readers (e.g. finger and face).

DARD shall protect and store biometric information in accordance with applicable standards and laws of the Republic

Biometric information will not be disclosed by the DARD unless (a) consent is obtained, or (b) disclosure is required by law, including required disclosure to law enforcement authorities.

Biometric information will be stored using a reasonable standard of care to guard against unauthorized access to and acquisition of the biometric information

DARD will destroy biometric data when the initial purpose for obtaining or collecting such data has been fulfilled or within three (1) year of the individual's last interaction with DARD or whichever occurs first

9.3.6 INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SECURITY

9.3.6.1 Information Security

9.3.6.1.1 A security network shall be established for department 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.

9.3.6.1.2 To prevent the compromise of IT systems, department shall implement baseline security control 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.

9.3.6.1.3 To ensure policy compliance, the IT Manager of department shall:

- Certify that all its systems are secured 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.

9.3.6.1.4 Server room 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.

9.3.6.1.5 Access to the resources on the network of department shall be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals of department shall be restricted unless explicitly authorized.

9.3.6.1.6 System hardware, operating and application software, the network and communication systems of department shall all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.

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

9.3.6.1.8 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.

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

9.3.6.2 Internet Access

9.3.6.2.1 The IT manager shall ensure that the network of department 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.

9.3.6.2.2 The IT Manager shall ensure that all internet users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security breaches and incidents.

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

9.3.6.2.4 Email encryption software must be installed to secure e-mail facilities of the department

9.3.6.3 Use of Laptop Computer

9.3.6.3.1 Usage of laptop computers by employees 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.

9.3.6.3.2 The information stored on a laptop computer shall be suitably protected at all times, in line with the protection measures prescribed in the IT Security Directive.

9.3.6.3.3 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. Employees shall be accountable for the negligent loss of the laptop.

9.3.6.3.4 No employee shall remove any ICT equipment from the Departmental premises without an approved removal permit by an authorised supervisor.

9.3.6.4 Communication Security

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

9.3.6.4.2 All sensitive electronic communications by employees, contractors must be encrypted in accordance with COMSEC standards. Encryption devices shall only be installed by COMSEC and not by any other service provider.

9.3.6.4.3 No unauthorised electronic devices shall be allowed in any boardroom and conference facilities where sensitive information of the Department is discussed. Authorisation must be obtained from the Security Manager.

9.3.6.5 Technical Surveillance Counter Measures (TSCM)

9.3.6.5.1 All offices, meeting, conference and boardroom venues of the department where sensitive and classified matters are discussed on a regular basis shall be identified by the Security Manager 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 the SSA to ensure that these areas are kept sterile and secure.

9.3.6.5.2 The Security Manager shall ensure that areas that are utilized for discussions of a sensitive nature as well as offices or rooms that house electronic communication equipment are physically secured in accordance with the standards laid down by the SSA.

9.3.6.5.3 No unauthorized electronic devices including cellular phones shall be allowed in any boardrooms and conference facilities where sensitive information is discussed.

9.3.7 BUSINESS CONTINUITY PLANNING (BCP)

9.3.7.1 The Security Manager must establish a security Business Continuity Plan (BCP) to provide for the continued availability of critical services, information and assets if a threat materializes and to provide for appropriate steps and procedures to respond to an emergency situation to ensure the safety of employees, contractors, consultants and visitors.

9.3.7.2 The security BCP shall be periodically tested to ensure that the management and employees understand how it is to be executed.

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

9.3.7.4 The security BCP shall be kept up to date and re-tested periodically by the Security Manager.

10. SPECIFIC RESPONSIBILITIES

10.1 Head of Department

10.1.1 The HOD bears the overall responsibility for implementing and enforcing the security program of department. Towards the execution of this responsibility, the HOD shall:

- Establish the post of the Security Manager and appoint a well- trained and competent with security background 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 department in the activities of the committee.
- Approve and ensure compliance with this policy and its associated Security Directives by all it is applicable to.

10.2 Security Manager

10.2.1 The delegated security responsibility lies with the Security Manager who will be responsible for the execution of the entire security function and program within the department (coordination, planning, implementing, controlling, etc.).

Towards execution of his/her responsibilities, the Security Manager shall, amongst others:

- Chair the security committee;
- Draft the internal Security Policy and Procedure Manual (containing the specific and detailed Security Directives) in conjunction with the security committee; Review the Security Policy and Procedure Manual at regular intervals;
- Conduct a security TRA with the assistance of the security committee and SSA;
- Advise management on the security implications of management decisions;
- Implement a security awareness program;
- Conduct internal compliance audit and inspection at regular intervals;
- Establish a good working relationship with both the SSA and SAPS and liaise with these institutions on a regular basis.

10.3 Security Committee

10.3.1 The Security Committee referred to in Para 10.1.1 above shall consist of senior managers of department representing all the main business units of department.

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

10.3.3 The Security Committee shall be responsible for, amongst others:

- Assisting the Security Manager in the execution of all security related responsibilities in drafting/reviewing of the Security Policy and Procedure Manual,

- Conducting of a security TRA, conduction of security audits, drafting of a security BCP and assisting with security awareness and training.

10.4 Line Management

10.4.1 All managers of department shall ensure that their subordinates comply with this policy and the Security Directives as contained in the Security Procedure Manual at all times.

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

10.5 Employees, Consultants, Contractors and other Service Providers

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

11. AUDIENCE

11.1 This Policy is applicable to all officials of the department, management, consultants, contractors and any other service providers. It is further applicable to all visitors and members of the public visiting premises of or may officially interact with department.

12. ENFORCEMENT

12.1 The HOD and the Security Manager are accountable for the enforcement of this policy.

12.2 All employees are required to fully comply with this policy and its associated security directives as contained in the Security Procedure

Manual. Non-compliance with any prescripts shall be addressed in terms of the Disciplinary Code/Regulations.

12.3 Prescripts to ensure compliance to this policy and the security directives by all consultants, contractors or service providers 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 the 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.

13. EXCEPTIONS

13.1 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 the people;
- During unavoidable emergency circumstances e.g. natural disasters;
- On written permission of the HOD (reasons for allowing non-compliance to one or more aspects of the policy and directives shall be clearly stated in such permission; no blanket non-compliance shall be allowed under any circumstances).

14. OTHER CONSIDERATIONS

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

- Occupational Health and Safety issues
- Disaster Management

14.1.3 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.

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

15 COMMUNICATING THE POLICY

15.1 The Security Manager 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.
The Security Manager will further ensure that all security policy and directive prescribes are enforced and complied with.

15.2 The Security Manager must ensure that a comprehensive security awareness program is developed and implemented 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 department.

16. REVIEW AND UPDATE PROCESS

16.1 The Security Manager must manage the implementation process of this policy and its associated security directives is reviewed and updated on annual basis. Amendments shall be made to the policy and directives as the need arise.

17. IMPLEMENTATION

17.1 The Security Manager must manage the implementation process of this policy and its associated security directives (contained in the Security Procedure Manual) by means of an action plan.

17.2 Implementation of the policy and its associated security directives is the responsibility of each and every individual this policy is applicable to (see para 6.1 above).

18. MONITORING OF COMPLIANCE

18.1 The Security Manager with the assistance of the security component and security committee must ensure compliance with this policy and its associated security directives by means of conducting internal security audits and inspections on a frequent basis.

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

19. DISCIPLINARY ACTION

19.1 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 department;
- Dismissal;
- Suspension;

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

Policy review

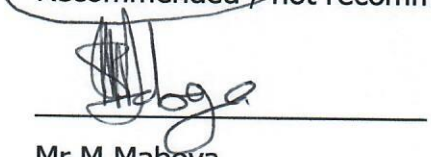
This policy will be reviewed once per annum or as and when a need arise and the HOD will approve all amendments.

Sign Off

HOD approval

Security Manager

Recommended / not recommended



Mr M Maboya

Deputy Director: Security Services

Date: 2024/11/27

Approved / not approved

Mr TZ Mokhatla

Head of Department: DARD

Date: 04/12/2024