dpwr

Department:
Public Works and Roads
North West Provincial Government
Republic of South Africa

SECURITY SERVICES POLICY

Table of Contents

DEFINITIONS

'accreditation'– means the official authorization by management for the operation of an Information Technology (IT) system, and acceptance by that management of the associated residual risk. Accreditation is based on the certification process as well as other management considerations;

'assets' - means material and immaterial property on 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;

'candidate' - means an applicant, an employee, a contract employee or a person acting on behalf of a contract appointee or independent contract;

'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 requirement;

'COMSEC' - means the organ of state known as Electronic Communications Security (Pty) Ltd, which was established in terms of section 2 of the Electronic Communication Security Act, 2002 (Act No. 68 of 2002) and, until such time as COMSEC becomes operational, the South African Communication Security Agency;

'critical service' - means a service identified by an institution as a critical service through a Threat and Risk Assessment and the compromise of which will endanger the effective functioning of the department;

'document' - means:-

- o any note or writing, whether produced by hand or by printing, typewriting or any other similar process, in either tangible or electronic format;

- any copy, plan picture, sketch or photographic or other representation of any place or article;
- any disc, tape, perforated roll or other device in or on which sound or any signal has been recorded for reproduction;

'information security'– includes, but not limited to:-

- document security;
- physical security measures for the protection of information;
- information and communication technology security;
- personnel security;
- business continuity planning;
- contingency planning;
- security screening;
- technical surveillance counter-measures;
- dealing with information security breaches;
- Security investigations; and
- Administration and organization of the security function at organs of state;

'MISS' means Minimum Information Security Standards (MISS) approved by Cabinet on 04 December 1996 which consists of:-

- Personnel Security
- Document Security
- Communication Security
- Computer (IT) Security

'National Intelligence Structures' – means the National Intelligence Structures as defined in Section 1 of the National Strategic Intelligence Act, (Act 39 of 1994);

'reliability check'- means an investigation into the criminal record, credit record and past performance of an individual or private organ of state to determine his/her or its reliability;

'risk' - means the likelihood of a threat materializing by exploitation of a vulnerability;

'screening investigator' – means a staff member of a National Intelligence Structure designated by the head of the relevant National Intelligence to conduct security clearance investigations;

'security breach' – means the negligent or intentional transgression of or failure to comply with security measures;

'Security clearance' – means a certificate issued to an employee or candidate after the successful completion of a security screening investigation, specifying the level of classification information to which an employee or candidate may have access subject to the need-to-know principle;

'site access clearance'–means clearance required for access to installations critical to the national interest;

'Technical Surveillance Counter Measures (TSCM)' – means the process involved in the detection, localization, identification and neutralization 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, that could cause injury to persons, compromise the integrity of information or could cause the loss or damage of assets;

'Threat and Risk Assessment (TRA)' – means, within the context of security risk management, the process through which it is determined when to avoid, reduce and accept risk, as well as how to diminish the potential impact of a threatening event;

'vulnerability' -means a deficiency related to security that could permit a threat to materialize.

1. PURPOSE

1.1 The Department of Public Works and Roads relies on its personnel, information and assets to deliver services that ensure the health, safety, security and economic well-being of all Employees in the Department in particular, as well as the South African citizenry in general. It is therefore incumbent upon them to manage these resources with due diligence and take appropriate measures to protect them;

1.2 Threats that can cause harm to the Department, in the country and abroad, may include, but not limited the following:- acts of terror and sabotage, espionage, unauthorized access to buildings and premises, theft, armed robbery, fraud and corruption, vandalism, fire, natural disaster, technical failures and accidental damage to property. 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 a result to changes in the international environment.

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

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

1.5 This policy complements other Departmental policies e.g. human resource management, occupational health and safety, information management, assets control, immovable property As well as financial resources.

2. SCOPE

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

- all Employees of the Department of Public Works and Roads;
- all Contractors and Consultants delivering a service to the Department, including their Employees who may interact with the Department;
- temporary Employees of the Department;
- all information assets of the Department;
- all intellectual properties of the Department;
- all fixed properties that are owned or leased by the Department;
- all movable properties that are owned or leased by the Department;
- all biological assets of the Department.

2.2 The policy further covers the following seven elements of the security program of the Department:-

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

3. LEGISLATIVE AND REGULATORY REQUIREMENTS

This policy is informed by and complies with applicable national and provincial legislation, security policies and security standards. Refer to **'Annexure A'** for a list of applicable regulatory documents.

4 POLICY STATEMENT

4.1 General

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

4.2 Compliance requirements

4.2.1 All individuals mentioned in Para. 2 above must comply with baseline requirements of this policy and associated Security Directives as contained in the Security Plan of the Department. 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.

4.2.2 Security threat and risk assessment involves:-

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

4.2.2.2 Determining the threats to information, employees and assets of the Department and assessing the probability and impact of threat occurrences;

4.2.2.3 Assessing the risk based on the adequacy of existing security measures and vulnerabilities;

4.2.2.4 Implementing any supplementary security measures that will reduce the risk to an acceptable level.

4.2.3 Staff accountability and acceptable use of assets

4.2.3.1 The HOD shall ensure that information and assets of the Department are used in accordance with procedures as stipulated in the Security Directives as contained in the Security Plan of the Department;

4.2.3.2 All Employees shall be accountable for the proper utilization and protection of such information and assets. Employees that misuse or abuse assets of the Department shall be held accountable and disciplinary action shall be taken against any such Employee.

4.3 Specific baseline requirements

4.3.1 Security Organization

4.3.1.1 The HOD will appoint 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;

4.3.1.2 A Security Manager with sufficient security experience and training will provide institution-wide strategic advice and guidance to Senior Managers;

4.3.1.3 The HOD will ensure that the Security Manager has an effective support structure (security component) to fulfil the functions referred to in Para. 4.3.2 below;

4.3.1.4 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 responsibilities.

4.3.2 Security Administration

4.3.2.1 **The functions referred to in Para 4.3.1 above include:-**

- General security administration (departmental directives and procedures, training and awareness, security risk management, security audits, sharing of information and assets);
- Setting of access limitations;
- Administration of security screening;
- Implement physical security;
- Ensure the protection of Employees;
- Ensure protection of information;
- Ensure ICT security;
- Ensure security in emergency and increased threat situations;
- Facilitate business continuity planning;
- Ensure security in contracting; and
- Facilitate security breach, reporting and investigations.

4.3.2.2 **Security incident / breach reporting process**

4.3.2.2.1 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.

4.3.2.2.2 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.

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

4.3.2.3 **Security incident/breaches response process**

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

4.3.2.3.2 The Directorate Security Services shall conduct preliminary investigations and provide feedback and recommendations;

4.3.2.3.3 It shall be the responsibility of the State Security Agency Structure (e.g. the SSA or SAPS) to conduct an investigation on reported security breaches and provide feedback with recommendations to the Department;

4.3.2.3.4 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;

4.3.2.3.5 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.

4.3.3 **Information Security**

4.3.3.1 **Categorization of information and information classification system**

4.3.3.1.1 The Security Manager must ensure that a comprehensive information classification system is developed and implemented in the

Department. All sensitive information produced or processed by the Department must be identified, categorized and classified according to the origin of its source, content and its sensitivity towards loss or disclosure.

4.3.3.1.2 All sensitive information must be categorized into one of the following:-

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

and subsequently classified according to its level of sensitivity by using one of the following recognized levels of classification viz:-

- Confidential;
- Secret; or
- Top Secret

4.3.3.1.3 Employees who generate sensitive information are responsible for determining information classification levels and the classification thereof subject to management review. This responsibility includes the labelling of classified documents;

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

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

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

4.3.4 Physical Security

4.3.4.1 Physical security involves the proper layout and design of facilities of the Department and the use of physical security measures to delay and prevent unauthorized access to assets of the 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;

4.3.4.2 Physical security measures must be developed, implemented and maintained in order to ensure that the entire Department, its personnel, property and information are secured. These security measures shall be based on

the findings of the Threat and Risk Assessment (TRA) to be conducted by the Security Manager;

4.3.4.3 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.

4.3.4.4 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;

4.3.4.5 All Employees are required to comply with access control procedures of the Department at all times. This shall include producing ID Cards upon entering any sites of the Department, the display thereof whilst on the premises and the escorting of official visitors.

4.3.5 Personnel Security

4.3.5.1 Security Vetting

4.3.5.1.1 All Employees, Contractors and Consultants of the Department who require access to classified information and critical assets in order to perform their 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;

4.3.5.1.2 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;

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

4.3.5.1.4 A declaration of secrecy shall be signed by every Individual issued with a security clearance form to complete the entire security

vetting process. This will remain valid even after the Individual has terminated their services with the Department;

4.3.5.1.5 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;

4.3.5.1.6 Security clearance in respect of all Individuals who have terminated their service with the Department shall be immediately withdrawn.

4.3.5.2 **Polygraph Examination**

4.3.5.2.1 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 information gathered during security screening investigations and does not imply any suspicion or risk on the part of the Applicant;

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

4.3.5.3 **Transferability of Security Clearance**

4.3.5.3.1 A security clearance issued in respect of an Official from other government institution shall not be automatically transferable to the DPWR. The responsibility for deciding whether the Official should be re-screened rests with the HOD.

4.3.5.4 **Security Awareness and Training**

4.3.5.4.1 A security training and awareness program shall be developed by the Security Manager and implemented to effectively ensure that all Personnel and Service Providers of the Department remain security conscious;

4.3.5.4.2 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 shall cover training with regard to specific security responsibilities and sensitize Employees and relevant Contractors and Consultants about the security policy and security measures of the Department and the need to protect sensitive information against disclosure, loss or destruction;

4.3.5.4.3 Periodic security awareness presentations, briefings and workshops will be conducted as well as the periodic distribution of posters and pamphlets in order to enhance the training and awareness program. Attendance of the above programs is compulsory for all Employees identified and notified to attend such events;

4.3.5.4.4 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.

4.3.5.5 **Personnel Suitability Checks**

All Officials/Contractors/ Interns and other third Parties of the DPWR shall, prior to employment/ working within DPWR, be subjected to Personnel Suitability Checks.

4.3.5.6 **Declaration of Confidentiality**

Any Official or Service Provider who accesses classified information must sign a Declaration of Confidentiality form.

4.3.6 Information and Communication Technology (ICT) Security

4.3.6.1 **IT Security**

4.3.6.1.1 A security network shall be established for the 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;

4.3.6.1.2 To prevent the compromise of IT systems, the 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;

4.3.6.1.3 To ensure policy compliance, the IT Manager of the 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 assessment 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;

4.3.6.1.4 Server room and other related security zones where IT equipments are kept shall be secured with adequate physical security measures and strict access control shall be enforced and monitored;

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

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

4.3.6.1.7 All Employees shall make use of IT systems of the 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;

4.3.6.1.8 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;

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

4.3.6.2 **Internet Access**

4.3.6.2.1 The IT Manager shall ensure that the network of the Department is safeguarded from malicious external intrusion by deploying, as a minimum measure, 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;

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

4.3.6.2.3 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 codes.

4.3.6.3 **Use of Laptop Computer**

5.3.6.3.1 Usage of laptop computers by Employees is restricted work related 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;

4.3.6.3.2 The information stored on a laptop computer shall be suitably protected at all times;

4.3.6.3.3 Employees shall also be responsible for implementing the appropriate security measures for the physical protection of laptop computers at all times. **(Employees shall be accountable for the negligent loss of a laptop allocated to them)**

4.3.6.4 **Communication Security**

4.3.6.4.1 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;

4.3.6.4.2 All sensitive electronic communications by Employees and Contractors must be encrypted in accordance with COMSEC standards. Encryption devices shall only be installed by COMSEC and not by any other commercial suppliers;

4.3.6.4.3 Access to communication security equipment of the Department and the handling of information transmitted and/or received by such equipment,

shall be restricted to authorized personnel only (personnel with a Top Secret Clearance who successfully completed the COMSEC course).

4.3.6.5 **Technical Surveillance Counter Measures (TSCM)**

4.3.6.5.1 All offices, meeting, conference and boardroom venues of the Department where sensitive and classified matters are discussed on a regular basis shall be identified 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;

4.3.6.5.2 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 equipments are physically secured in accordance with the standards laid down by the SSA in order to support the sterility of the environment after a TSCM examination, before any request for a TSCM examination is submitted;

4.3.6.5.3 No unauthorized electronic devices shall be allowed in any boardroom and conference facilities where sensitive information is discussed. Authorization must be obtained from the Security Manager.

4.3.7 **Business Continuity Planning (BCP)**

4.3.7.1 The Security Manager shall ensure Business Continuity Plan (BCP) is developed 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;

4.3.7.2 The BCP shall be periodically tested to ensure that the Management and Employees understand how it is to be executed;

4.3.7.3 All Employees shall be made aware and trained on the content of the BCP to ensure understanding of their own respective roles in terms thereof;

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

5. SPECIFIC RESPONSIBILITIES

5.1 Head of Department

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

- establish the position of Security Manager and appoint a well trained and competent Incumbent with extensive security background;
- establish a Security Committee for the institution and ensure participation by all Senior Managers of core business functions of the Department;
- Approve and ensure compliance with this policy and its associated Security Directives by all parties involved.

5.2 Security Manager

5.2.1 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). In executing his responsibilities, the Security Manager shall, amongst others:-

- Chair the Security Committee;
- Draft the internal Security Policy and Security Plan (containing the specific and detailed Security Directives) in conjunction with the security committee;
- Review the Security Policy and Security Plan at regular intervals;
- Conduct a security TRA with the assistance of the Security Committee;
- 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.

5.3 Security Committee

5.3.1 The Security Committee referred to in Para 5.1.1 above shall consist of Senior Managers of the Department representing all the main business units;

5.3.2 Participation in the activities of the Security Committee by the appointed Representatives of business units shall be compulsory.

5.3.3 The Security Committee shall be responsible for, amongst others:-

- Assisting the Security Manager in the execution of all security related responsibilities;
- Completing tasks such as drafting/reviewing of the Security Policy and Plan;

- Conduct security TRA;
- Conduct security audits;
- drafting of a BCP; and
- Assisting with security awareness and training.

5.4 **Line Management**

5.4.1 All Managers of the Department shall ensure that their Subordinates comply with this Policy and the Security Directives as contained in the Security Plan at all times;

5.4.2 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.

5.5 **Employees, Consultants, Contractors and other Service Providers**

5.5.1 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.

6. AUDIENCE

6.1 This Policy is applicable to all Officials of the Department, Consultants, Contractors and any other Service Providers. It is further applicable to all visitors and Members of the public visiting premises in their interaction with Officials of the Department.

7. ENFORCEMENT

7.1 The HOD and the Security Manager are accountable for the enforcement of this policy;

7.2 All Employees are required to fully comply with this policy and its associated security directives as contained in the Security Policy. Non-compliance with any prescripts shall be addressed in terms of the Disciplinary Code/Regulations;

7.3 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.

8. EXCEPTIONS

8.1 Deviations from this Policy and its associated security directives will only be permitted under the following circumstances:;

- Wherein security must be breached in order to save or protect the lives;
- During unavoidable emergency circumstances e.g. natural disasters;
- Upon 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).

9. OTHER CONSIDERATIONS

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

9.1.1 Occupational Health and Safety issues;

9.1.2 Disaster Management;

9.1.3 Disabled persons shall not be inconvenienced by physical security measures and must be catered for in such a manner that they have access without compromising security or the integrity of this Policy;

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

10 COMMUNICATING THE POLICY

10.1 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 the Security Policy and any supplementary prescripts are enforced and complied with;

10.2 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 shall be conducted through the following means:-

- Awareness workshops and briefings to be attended by all Employees;
- Distribution of memos and circulars to all Employees;
- Access to the Policy and applicable directives on the intranet of the Department.

11. REVIEW AND UPDATE PROCESS

11.1 The Security Manager must manage the implementation process of this Policy and its associated security directives is reviewed and updated on an annual basis. Amendments and directives to the Policy shall be made as and when the need arises.

12. IMPLEMENTATION

12.1 The Security Manager must manage the implementation process of this policy and its associated security directives (contained in the Security Plan) by means of an action plan (also to be included in the Security Plan);

12.2 Implementation of the Policy and its associated security directives is the responsibility of each and every individual this policy is applicable to (see para 2.1 above).

13. MONITORING OF COMPLIANCE

13.1 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 regular basis;

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

14. DISCIPLINARY ACTION

14.1 Non-compliance with this Policy and its associated security directives shall result in disciplinary action which may include, but not limited to:-

- re-training;
- verbal and written warnings;
- termination of contracts in the case of Contractors or Consultants delivering a service to the Department;
- dismissal;
- suspension;
- loss of Departmental information, asset resources and access privileges.

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

15. RESIGNATION / TRANSFER

15.1 Upon transfer / resignation / termination of employment, any person in possession of laptops, any devices belonging to the Department of Public Works and Roads shall return all devices and Laptops to Asset Management section a week before their termination notice expires. Under no circumstances should a person delete work related to the Department.

EFFECTIVE DATE

This policy shall become effective from 1 April 2020 and shall be reviewed annually.

MR MS THOBAKGALE
ADMINISTRATOR - DPWR

20/08/2020
DATE

ANNEXURE A

APPLICABLE LEGISLATION AND OTHER REGULATORY FRAMEWORK DOCUMENTS

Applicable Legislation

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

Other Regulatory Framework Documents

- Minimum Information Security Standards (MISS), Second Edition March 1998
- White Paper on Intelligence (1995)
- SACSA/090/1(4) Communication Security in the RSA
- SSA Guidance Documents: ICT Policy and Standards: Part 1 & 2
- ISO 17799