KWAZULU-NATAL PROVINCE

HUMAN SETTLEMENTS
REPUBLIC OF SOUTH AFRICA

SECURITY POLICY

DEPARTMENT OF HUMAN SETTLEMENTS

KWAZULU NATAL

1. INTRODUCTION

The Security Policy sets out the fundamental responsibilities and security programs for the Department of Human Settlements (DOHS). The Security Policy is a directive or guideline which is informed by the Minimum Information Security Standard (MISS), the Minimum Physical Security Standards (MPSS) and other security prescripts that regulate Security. This document outlines the formulation, implementation and effective monitoring of security risk measures in the Department and complies fully with the provisions of the MISS as approved by Cabinet in December 1996. This policy gives the Security Manager the authority to take the necessary actions in all security related matters on behalf of the Head of Department (HOD), and must have the total backing or support of the senior management of the Department. There is an absolute need for effective security measures to be developed and implemented in order to counterespionage, subversion, sabotage, terrorism, fraud, corruption and general crime, and to protect human lives (employees, contractors, consultants and visitors), unauthorised disclosure of information.

2. DEFINITIONS AND ACRONYMS

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

"Assets" means material and immaterial property of an institution. Assets include but are not limited to information in all forms and stored on any media, networks or systems, or material, real property, financial resources, employee trust, public confidence and international reputation;

"Availability" means the condition of being usable on demand to support operations, programmes and services;

"Business Continuity Management Plan (BCMP)" includes the development of plans, measures, procedures and arrangements to ensure minimal or no interruption of the availability of critical services and assets;

"Candidate" means an applicant, an employee, a contract employee or a person acting on behalf of a contract appointee or independent contractor;

"Certification" means the issuing of a certificate certifying that 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;

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

"Confidential" is the limiting of access or places restrictions on certain type of information;

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

"Document" means –

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

"DOHS" means Department of Human Settlements

"HOD" means head of the department;

"Information security" includes, but is not limited to, —

a) document security;
b) physical security measures for the protection of information;
c) information and communication technology security;
d) personnel security;
e) business continuity planning;
f) contingency planning;
g) security screening;
h) technical surveillance counter-measures;
i) dealing with information security breaches;
j) security investigations; and
k) administration and organization of the security function at organs of state;

"National Intelligence Structures" means the National Intelligence Structures as defined in section 1 of the National Strategic Intelligence Act, Act 39 of 1994;

"Need-to-know" means that employees are expected to limit their request for information to that which they have a genuine need to know and they are expected to ensure that anyone to whom they gave classified information has a legitimate need to know for that information.

"Personnel information" means any information concerning an individual person in respect of which the individual has demonstrated his or her desire to keep it private and not to disclose it to the public in general.

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

"Risk" means the likelihood of a threat materialising by exploitation of vulnerability;

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

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

"Security clearance" means a certificate issued to a candidate after the successful completion of a security screening investigation, specifying the level of classified information to which the candidate may have access subject to the need to know;

"Site access clearance" means clearance required for access to installations critical to the national interest;

"SM" means security manager;

"State secrets" means information known only to limited number of people of which ought to be kept secret in order to prevent safety or interests of the Republic from being endangered.

"Technical Surveillance Countermeasures" (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, 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;

"Trade secret" means any information concerning commercial or industrial activities of a specific organisation or an individual which needs to be kept secret in order to protect the economic interests of the state, organisation or the individual concerned.

"Vulnerability" means a deficiency related to security that could permit a threat to materialise.

3. PURPOSE

3.1 The Security Policy of the Department of Human Settlements seeks to prescribe to the application of security measures to reduce the risk of harm that can be caused to the Department if threats should materialise. It has been designed to protect employees, preserve the confidentiality, integrity, availability and value of information and assets, and assure the continued delivery of services. Since the Department of Human Settlements relies extensively on information management systems and technology (IMST) to provide its services, this policy emphasizes the need for acceptable use of IMST equipment as well as IMST protection measures to be complied with by employees.

3.2 The main objective of this policy therefore is to support the regional interests and the Department of Human Settlements' strategic objectives by protecting employees, information and assets and assuring the continued delivery of services to the citizens of KwaZulu-Natal.

4. SCOPE

4.1 This policy applies to the following individuals and entities:

a) all employees of the Department of Human Settlements in all offices;
b) all temporary employees of the Department of Human Settlements
c) all contractors and consultants delivering a service to the Department of Human Settlements, including their employees who may interact with the Department of Human Settlements;
d) all information assets of the Department of Human Settlements
e) all intellectual property of the Department of Human Settlements;
f) all fixed property that is owned or leased by the Department of Human Settlements;
g) all moveable property that is owned or leased by the Department of Human Settlements.

4.2 The policy further covers the following seven elements of the security program of The Department of Human Settlements:

a) Security organization
b) Security administration
c) Information security
d) Physical security
e) Personnel security
f) Information Management System and Technology (IMST) security
g) Business Continuity Management Planning (BCMP)/ Contingency Planning

5. LEGISLATIVE AND REGULATORY REQUIREMENTS

5.1 This policy is informed by and complies with primary and secondary national legislation and national security standards

a) Constitution of the Republic of South Africa, 1996 (Act 106 of 1996)
b) Protection of Information Act, 1982 (Act no 84 of 1982)
c) Promotion of Access to Information Act, 2000 (Act no 2 of 2000)
d) Copyright Act, 1978 (Act no 98 of 1978)
e) National Archives of South Africa Act, 1996 (Act no 43 of 1996) and regulations
f) Public Service Act, 1994 (Act no 103 of 1994) and regulations
g) Occupational Health and Safety Act, 1993 (Act no 85 of 1993)
h) Criminal Procedures Act, 1977, (Act 51 of 1977), as amended.
i) Private Security Industry Regulations Act, 2001 (Act 56 of 2001)
j) Control of Access to Public Premises and Vehicles Act, 1985 (Act 53 of 1985)

j) Control of Access to Public Premises and Vehicles Act, 1985 (Act 53 of 1985)
k) Trespass Act, 1959 (Act 6 of 1959)
l) Electronic Communication and Transaction Act, 2002 (Act 25 of 2002)
m) Electronic Communications Security (Pty) Ltd Act, 2002 (Act 68 of 2002)
n) State Information Technology Agency Act, 1998 (Act 88 of 1998)
o) Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act 70 of 2002)
p) General Intelligence Law Amendment Act, 2000 (Act 66 of 2000)
q) National Strategic Intelligence Act, 1994 (Act 39 of 1994)
r) National Key points Act, 1980 (Act No 102 of 1980)
s) National Personnel Security Vetting Policy
t) Labour Relations Act, 1995 (Act 66 of 1995)
u) Employment Equity Act, 1998 (Act 55 of 1998)
v) Fire-arms Control Act, 2000 (Act 60 of 2000) and regulations
w) Protection of Constitutional Democracy Against Terrorism and Related Activities Act, 2004 (Act 33 of 2004)
x) National Building Regulations and Building Standards Act, 1977 (Act 103 of 1977)
y) Protected Disclosures Act, 2000 (Act 26 of 2000)
z) Intimidation Act, 1982 (Act 72 of 1982)
aa) Prevention and Combating of Corrupt Activities Act, 2004 (Act 12 of 2004)
bb) Public Finance Management Act, 1999 (Act 1 of 1999) and Treasury Regulations
cc) Protection of Personal Information Act, 2013 (Act 4 of 2013)

Other regulatory framework documents and policies

a) Minimum Information Security Standards (MISS), Second Edition March 1998
b) Minimum Physical Security Standards (MPSS)
c) White paper on Intelligence (1995)
d) SACSA/090/1(4) Communication Security in the RSA
e) SSA Guidance Documents: ICT Policy and Standards: Part 1 & 2
f) ISO 17799
g) National Building Regulations
h) Chapter 2, Page 14 of the Public Service Handbook (SMS)
i) Cabinet Memo dated 2006 December 06
j) Protection of Personal Information Act (POPIA) Compliance Policy Framework
k) IMST Information Security Policy

6. GENERIC PRINCIPLES

a) Employees of the Department of Human Settlements must be protected against identified threats according to baseline security requirements and continuous security risk management.

b) Information and assets of the Department of Human Settlements must be protected according to baseline security requirements and continuous security risk management.

c) The principles relating to the information security within the Department of Human Settlements are governed through the POPIA Compliance Policy Framework and IMST Information Security Policy.

d) Continued delivery of services of the Department of Human Settlements must be assured through baseline security requirements, and continuous security risk management.

7.1 Categorization of information and information classification system

a) The Security Manager in consultation with records management and security committee must ensure that a comprehensive information classification system is developed for and implemented in the Department of Human Settlements. All sensitive information produced or processed by the Department of Human Settlements must be identified, categorized and classified according to the origin of its source and contents and according to its sensitivity to loss or disclosure. Sensitive information is the intellectual property of the DOHS and requires maximum protection from known or unknown adversaries.

b) The "need to know" principle must be applied in respect of all classified information in the Department, to ensure that only authorised persons gain access to such information. Only persons with a relevant security clearance may have access to classified information, unless otherwise approved in writing by the Head of the Department or his/her delegate.

c) Document security is integral or core to information security. Documents should be given the same respect as a person e.g. A Human Resource file qualifies or carries the same status of a person because they have details regarding the personal particulars of a person i.e. copy of the ID, gender, previous employments, persal number, member references, physical and postal addresses, marital status, dependents, telephone numbers, HIV status, declaration of financial interests, criminal records and bank account number. If all this information falls into the wrong hands, it can be used against the person.

d) Information is potential, but the ability to access and control that information is "POWER".

7.2 Classification of Documents

a) The HOD must ensure that every document in the possession or under the control of DOHS and which falls under one of the categories of sensitive information is properly classified in accordance with the relevant classification.

b) All documents must be classified according to the degree of security protection needed. It is the responsibility of the drafter (author) of the document of which the contents are of a sensitive nature, to classify it so that only authorised persons may have access to it. The classification assigned to documents shall be strictly observed and may not be changed without the consent of the author. The author must guard against under-classification, over-classification or unnecessary classification of document.

Three levels of classification which will be used within the department, namely, Confidential, Secret and Top Secret.

7.3 Handling of classified documents

All files and documents, which contain classified information, must be marked in the appropriate manner with the correct classification. The classification awarded to it must be indicated on the top-centre and bottom centre of each page.

a) Incoming classified documents

Only an official with an appropriate security clearance shall open incoming classified documents. All incoming classified documents must be recorded in the prescribed registers.

b) Dispatching of classified documents

i) All classified documents being dispatched must be recorded in the prescribed register. Classified documents must only be transmitted via a secured "encrypted line" and must only be dispatched and secured by a security official or messenger vetted to the minimum level of "Confidential". The messenger/official must use the prescribed lockable briefcase/ attaché case.

ii) Classified and unclassified documents dispatched to South African missions abroad must be dispatched via the Department of Foreign Affairs. Classified documents must be dispatched by means of diplomatic bags and unclassified documents by means of freight bags.

c) Storage of Classified documents

i) All classified documents not in immediate use must be locked away in the appropriate cabinet, safe or strong room as prescribed in the Security Procedure Manual. All offices where classified documents are being kept must be equipped with a security lock with the minimum of five (5) levers.

ii) Classified documents not in use shall be stored in the following manner:

Classification	Filing system
Confidential	Reinforced steel filing cabinet
Secret	Strong room or reinforced filing cabinets
Top Secret	Strong room, safes or walk-in safe

iii) Strict access control shall be implemented to registries where classified documents are being kept.

iv) Classified documents may under no circumstances be left unattended in offices, homes and vehicles; such documents must be kept in a secure and lockable facility – e.g. briefcase.

7.4 Removal of Classified Document from Premises

Removal of classified documents from the premises must be avoided, unless otherwise authorised by the Head of the Department or his/her delegate for emergency and essential meeting outside the premises. All classified documents being removed from the premises must be recorded in the prescribed register.

7.5 Destruction of Classified Documents

a) The destruction of classified documents must be done in accordance with the National Archives of South Africa Act (43 of 1996).

b) Security Manager or a person appointed by the HOD (with Top Secret Clearance) is responsible for the destruction of classified documents and a certificate of destruction

must be issued in this regard.

c) All the draft notes, used carbon papers, etc. of classified information identified for destruction must not be placed in waste paper bins, but should immediately be destroyed or safeguarded until it can be destroyed in terms of the prescribed document destruction methods.

7.6 Copying of Classified Documents

Copies of secret and top secret documents must only be made with the approval of the Security Manager or his/her designee. Such authorisation must be indicated on the original document. A register must be used to record all the reproductions of classified documents.

7.7 Categories of information

a) State secret, information becomes a state secret if its disclosure may be harmful to the security or interests of the state or could cause embarrassment to the Republic in its international interests.

b) Trade secret, information becomes a trade secret if its disclosure may cause financial loss to the institution or may cause embarrassment to the institution in its relations with its clients, competitors, contractors.

c) Personal information, information becomes personal if the disclosure of such may constitute an invasion of privacy of any individual.

7.8 Handling of requests in terms of the Promotion of Access to Information Act

A procedure to request documents from public bodies will be developed and communicated to all staff in compliance with Promotion of Access to Information Act.

7.9 Contingency planning in respect of Classified Document

All classified documents must be locked away in the event of an emergency, or should have an electronic version stored in offsite storage in line with the departmental Contingency Plan.

8. PERSONNEL SECURITY

8.1 Security Screening/Vetting

a) All employees and potential employees shall be subjected to security screening when taking appointment with the Department of Human Settlements. When security screening is positive, the potential employee will be employed on probation, during which proper security vetting will commence. Human Resources (Recruitment and Selection) must issue an appointment letter to the new employee which has a subjective clause of a positive security clearance from SSA.

b) The permanent appointment of the prospective employee will depend on the outcome of the results of proper security vetting and such results must be positive.

8.2 Security vetting

a) The main focus of the security vetting process is to determine the integrity, reliability

and loyalty of an official towards the Republic of South Africa and the Constitution.

b) Security vetting must be regarded as the basic line of defence that can be taken to protect classified and sensitive information.

c) The degree of security clearance given to an employee is determined by the contents and/or access to sensitive or classified information entailed by the post already occupied or to be occupied by the official.

d) All personnel working in the DOHS who in the execution of their duties have access to sensitive and classified information shall be subjected to security vetting (to the applicable level) prior to taking up employment. In the event where employment is taken up prior to vetting and such results is negative an official must be deployed where there is no sensitive or classified information.

e) All service providers who have access to sensitive information contracted to guard government buildings or buildings rented by the state will be subjected to a vetting process prior to taking up the contract. This will include the screening of all company directors as well as the staff that will be used during the duration of the contract period.

f) A security clearance gives access to classified information in accordance with the level of security clearance, subject to the need-to-know basis.

g) All persons who are to be employed by the DOHS on a task that will expose them to classified information must be issued with a security clearance equivalent to his/her level of access, before having access to such classified information.

h) All employees in the office of the HOD must be security screened by the State Security Agency, before assuming duty in those offices.

i) All employees, contractors (service providers) and consultants of the Department of Human Settlements, who require access to classified information and critical assets in order to perform his/her duties or functions, must be subjected to a security screening investigation conducted by the State Security Agency (SSA) in order to be granted a security clearance at the appropriate level.

j) The level of security clearance given to a person will be determined by the content of access to classified information entailed in the post occupied or to be occupied in accordance with their respective responsibilities and accountability.

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

l) A declaration of secrecy must be signed by every individual issued with a security clearance to complement the entire security screening process. This will remain valid even after the individual has terminated his/her services with the Department of Human Settlements.

m) 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 Head of Department, based on information which impact negatively on an individual's security competence.

n) Security clearances in respect of all individuals who have terminated their services with the Department of Human Settlements must be immediately

withdrawn.

8.3 Screening/vetting of persons who have lived/worked abroad for long periods

a) Where a security clearance is required for an RSA citizen who has resided/studied/worked abroad for a long period (excluding transferred public servants or students) and who applies to a government or semi-government institution or a national key point for employment, such a person is temporarily not eligible for any grade of security clearance. Applications for clearance can, however, be considered after a period, as set out hereunder, on condition that the applicant did not give up RSA citizenship or accepted dual citizenship during the period of absence:

b) A confidential clearance after one year back in the RSA. Such a person can be appointed on condition that a re-application is submitted after one year. On appointment, the subject thus completes and submits all relevant forms for a security clearance. The requesting authority will then be informed as to whether or not there is any negative information on the subject. The subject is also to undertake, in writing, that he/she will resign should the issuing of a security clearance be refused after one year. If such an undertaking is not specifically included in the service contract, a written undertaking to this extent, under signature of the subject, must accompany the application for a security clearance.

c) A Secret clearance after three years back in the RSA.

d) A Top Secret clearance after five years back in the RSA.

8.4 Security vetting: Consultants, contractors supplying services to the Department of Human Settlements

The onus is on the Department of Human Settlements to indicate expressly in documents sent to the media or private contractors whether there are security implications that should be taken into account in advance when they perform their duties for the Department of Human Settlements. If there are such implications, reasons must be given for the inclusion of a clause in the tender document indicating the degree of clearance required, as well as a clause to ensure the maintenance of security during the performance of the contract. The clause could read as follows:

a) "Acceptance of this tender is subject to the condition that the contracting company and its Directors who will provide the service, be subjected to security vetting in the form of record checks by SSA. In addition to this, the personnel of the private company that will be contracted at DOHS must be subjected to the screening process. If the principal contractor appoints a subcontractor, the same provisions and measures will apply to the subcontractor. It is imperative that the Security Manager ensures that the contractors be cleared to the appropriate level (CONFIDENTIAL/SECRET/TOP SECRET). His/ Her decision must be based on the level of access the contractors/subcontractors will have in the department.

b) Acceptance of the tender is also subject to the condition that the contractor will implement all such security measures as the safe performance of the contract may require."

c) The security responsibilities of the contractor will be determined by the Department of Human Settlements.

8.5 Procedure for requesting security vetting

a) Requests for security vetting and re-vetting must be submitted to security management who will forward them to SSA on the Z204 form accompanied by a set of clear fingerprints.

b) The Department of Human Settlements should provide the SSA with a post description of the employee concerned and an indication of the access he/she has/will have and with all other facts that may influence the issue of a clearance.

c) Line functional management must identify employees that need to be vetted in the department and must stipulate the level of the security clearance (confidential, secret or top secret). The Security Manager at the department must verify if it will be necessary for an employee to be vetted to the particular level mentioned in the list. The Security Manager must base his / her decision on access to sensitive information, which the employee might have while conducting his/her duties at the DOHS.

8.6 Period of validity of security clearances

a) The Head of the Department of Human Settlements or his/her delegate must ensure that an officer in respect of whom a security clearance of Secret or Top Secret has been issued, is re-screened every five (5) years and every ten (10) years in respect of a Confidential clearance.

b) Enquiries will be done with the supervisor every five (5) years with respect to the security competence of an official who has received a clearance.

c) This arrangement does not preclude re-vetting before a period of five (5) years has lapsed in the case of occupational change or where something prejudicial has been established about an officer which may affect his or her security competence. Personnel in ultra-sensitive posts should be cleared every three (3) years.

8.7 Polygraph examination

a) A polygraph examination must be utilized to provide support to the security screening process. All employees subjected to a Top Secret security clearance will also be subjected to a polygraph examination.

b) Refusal by the applicant to undergo the examination does not necessarily signify that a security clearance will not be granted.

8.8 Transferability of security clearances

a) A security clearance issued in respect of an officer while he/she is working with the Department of Human Settlements is not automatically transferable to another department. When an officer changes employer, the responsibility for deciding whether the re-screening of such an officer will be requested in the prescribed ways rests with the new employer.

b) However, for the purpose of the meetings and other co-operative functions, clearances are transferable. The employing institution is responsible for informing the chairperson of such meetings as to the level and period of validity of the clearances of the representative involved.

8.9 Issues of Security Clearance

a) The Security Manager must advise the Head of Department on the issue of security clearances and report or advise on any negative security aspects during the security clearance process.

b) Refusal of members to co-operate in the submission of the Z204 forms for vetting purposes will constitute misconduct on the part of the employee and the Head of Department will take necessary steps against such employee.

8.10 Upgrading of a security clearance

a) In case where an employee is appointed in a post that requires a higher level of security clearance, a security screening investigation shall be conducted before an upgraded security clearance may be issued.

b) The period of validity of the higher level of security clearance obtained in this way is calculated from the date the higher clearance is issued.

8.11 Implications of refusal to issue a security clearance

a) The Head of Department must inform in writing the candidate of the fact that he or she was refused a security clearance on the requested level, unless informed by the SSA not to do so.

b) However, if the Head of Department is satisfied that the applicant poses a security threat to DOHS if he or she occupies a position that he or she applied for, the HOD can consider whether such a threat can be neutralised by deploying the applicant in a different position, transferring the employee or change his or her job description that will not require him or her have a security clearance at the level applied for but which will still enable the DOHS to utilise his or her skills and competencies effectively, and, if so, consult the applicant and appoint him or her in that position.

c) But if the threat cannot be neutralised by changing the job description consider terminating the service of the employee, if such employee is appointed in terms of the Public Service Act. 1994 (Proclamation 103 of 1994), in accordance with section 17(2) (h) of that Act or, if the employee is employed in terms of other acts, consider any other manner prescribed by law.

8.12 Oath of Secrecy or Non-disclosure agreements

a) All officials, temporary workers, consultants and contractors shall sign an "Oath of Secrecy" document as defined in the Protection of the Information Act (84 of 1982) before assumption of sensitive duties within the Department. In case of existing employees the Oath will be communicated to the different Heads of sections.

b) A Declaration of Secrecy/Non-Disclosure Agreements or an Oath of Secrecy form must be signed by all employees and one copy be filed in the Human Resource file.

8.13 Re-Vetting

Re-vetting will only be considered when:-

a) the period of the validity of a confidential, secret and top secret clearance has expired.

b) Prior to expiry, should the employer be of the opinion that certain circumstances have influenced or may influence the security competence of a person under his control.

c) When the person is re-employed on a job that requires security screening.

d) When a higher grade of clearance is required.

9. PHYSICAL SECURITY

a) The primary purpose of physical security as outlined in the MPSS is to inform staff and managers of those essential requirements for protecting the assets of the institution, of which the most important are people, property and information. This policy will specify the mechanisms through which these requirements can be met.

b) Another purpose will include the following:
   i) To deter an intruder from entering the premises
   ii) To detect the attempted entry or presence if an intruder succeeds in penetrating
   iii) To limit the harm that can be done if an intruder has managed to gain entry without being detected, using measures such as locks, keys, strong rooms, safes and other physical barriers.
   iv) To detain the intruder by using silent alarms and security patrols.

c) Physical security involves the proper layout and design of facilities of the Department of Human Settlements and the use of physical security measures to delay and prevent unauthorized access to assets of the Department of Human Settlement. 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.

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

e) The Department of Human Settlements must ensure that physical security is fully integrated early in the process of planning, selecting, designing and modifying of its facilities.

f) The Department Human Settlements must:
   i) select, design and modify facilities in order to facilitate the effective control of access thereto;
   ii) demarcate restricted access areas and have the necessary entry barriers, security systems and equipment to effectively control access thereto;
   iii) include the necessary security specifications in planning, request for proposals and tender documentation;
   iv) incorporate related costs in funding requirements for the implementation of the above.

g) The Department of Human Settlements must also ensure the implementation of appropriate physical security measures for the secure storage, transmittal and disposal of classified and protected information in all forms.

h) All employees are required to comply with access control procedures of the

Department of Human Settlements at all times. This includes producing an ID card/ name tag/ visitors tag or using biometric where applicable upon entering any sites of the Department of Human Settlements, the display thereof whilst on the premises and the escorting of official visitors.

9.1 Private and State property

All private property, e.g. computer equipment, laptops, cameras, recording devices, radios and kitchen equipment etc., brought onto Departmental premises must be declared to the security risk personnel at the reception desk.
In case of the removal of State property a removal permit shall be completed and handed out at the security checkpoint.

10. OFFICE SECURITY

a) Each employee is responsible for the security of the office/ working area allocated to him/ her and must ensure that no unauthorised employee or other person gain access to any sensitive or classified official document or equipment under his/her control.

b) Each employee must inspect his/her own office or work area for signs of intrusion at the beginning of each working day. If the employee detects any sign of intrusion, he/she should notify his/her supervisor and/or the structure responsible for physical security without delay.

c) Cleaning of offices shall only be done during official working hours and shall be conducted under the supervision of the occupant(s) of the office/working area. In the case of offices/ working areas that contain sensitive equipment or documents and that cannot be hidden/ locked away; the occupants of such offices/working areas must take responsibility for cleaning such offices/ working areas. Under no circumstances, shall contractors or visitors be left alone inside any office of the department.

d) The occupant of an office must lock the doors of the office or working area when leaving for any period.

e) At the end of the day, before departure, each employee must ensure that:

   i) lights and electrical appliances over which he/she has control are switched off and unplugged from wall sockets;
   ii) blinds, curtains are drawn; and
   iii) doors and cabinets are locked and windows/curtains/blinds are closed.

f) Where a building or office complex occupied by the DOHS does not have a security component, the head of the concerned office, or his/her designate, must take responsibility for locking and unlocking access doors and to make provision for after-hours inspections. Due to the risk factor, compliance inspections of offices after hours must be conducted by designated officials in accordance with standards operating procedures.

g) A register for after-hours visits to offices of the DOHS must be kept and checked monthly by security management or designated officials at district offices. Any deviation must be reported to the Security Manager and HOD.

11. ACCESS CONTROL

a) Access control will be performed by private or contract security officers. Private security staff will be under the strict supervision of DOHS management.

b) No person shall, without the permission of an authorised security officer, enter any of the buildings occupied by DOHS. Access to the DOHS premises or parts thereof must be limited to employees and persons authorized to have access by the Head of Department or a security official who has been delegated with specific authority to give approval. In cases where private security staff is used, they will be under strict supervision of departmental security management. Access to the security areas of the Department of Human Settlements is subject to compliance with security measures stipulated in this directive and as determined by the Security Manager or Senior management from time to time. All persons desiring access to buildings under the control of the Department of Human Settlements, or wishing to depart therefrom, are subject to searching of their person as well as the search of the contents of their briefcases, handbags, parcels or other containers including a boot of a car. Should a person refuse to declare the contents thereof, he/she may be denied access, or he/she may hand over some to an employee/external security provider responsible for security for safe keeping until he/she departs from the premises.

11.1 Access of personnel to DOHS premises

a) Security officials must control access of Personnel to the Department of Human Settlements premises. Employees may be allowed access to premises upon presentation of:

i) The official photo identity card or name tag issued by the DOHS.

ii) Employees may not enter or depart from a security area without activating the card reader where these are in operation. This may only be overruled during emergency situations; or

iii) Personnel not in possession of approved access cards shall be assisted in the completion of the necessary register when accessing the premises.

b) Where access is granted in terms of point 11.2 a temporary personnel card may be issued after completion of applicable administrative procedures. This card must, upon departure from DOHS premises, be returned to the issuing control room/ access control point.

c) In the case of an employee requiring access to DOHS premises for official purposes after normal working hours, weekends and public holidays, access may be granted; provided that an official has a letter from his/ her supervisor and the copy thereof corresponds with the one given to security officer in charge at the access control point informing them about the particulars of the member, the reason for the visit and duration of stay are entered into the applicable register (occurrence book and after hours register). Security Manager or his/ her delegate must be informed of officials coming to the office after normal working hours, weekend and public holidays.

d) The loss of access cards must immediately be reported in writing to the security access control room, to the Security Manager or his/her delegate, to ensure that the card is disabled to prevent the unauthorized usage of the card. A levy will be paid for the replacement of an access card.

e) Every employee must take reasonable care of his/her access card and lending of access cards from one person to another is considered as a breach of security and it is prohibited.

f) Personnel are by no means allowed on the premises under the influence of liquor or any other illegal and/or intoxicating substance.

11.2 Access of visitors to DOHS premises

a) Access of the following categories of visitors authorized to have access to DOHS premises for any purpose shall comply with the provisions of the Control of Access to Public Premises and Vehicles Act (positive identification by means of a green barcode identity document/Smart ID card, driver's licenses and/or passport). All vehicles entering and exiting the departmental premises must be subjected to a thorough search. Every visitor must positively identify himself or herself at the access control point of the department. Persons refusing to be subjected to the prescribed security procedures will not be permitted access to the premises. Visitors on departmental premises must, at all times, obey lawful orders given by authorized officers. While the supervisory employee of the unit/directorate requesting/authorizing access of such persons must take full responsibility to, where applicable, ensure controlled movement (escort) of such persons at all times on DOHS's premises if not otherwise arranged with the structure responsible for physical security to provide escort:

i) Official VIP's as determined/ prescribed by senior management;
ii) Official visitors (for the purpose of consultation, meetings, etc.);
iii) Service providers contracted to provide a service to the department;
iv) Non-official visitors (family members, friends or acquaintances of the department officials);

b) In addition to the escorting of non-personnel (official, non-official, visitors and service providers) by the host/employee requesting access for such persons, it must be the responsibility of the host/employee requesting access for such persons to department premises to ensure that:

i) the visitor(s) or service provider(s) persons is adequately familiarized with regulatory prescripts relating to security policy, including the carrying of access cards in a clearly visible manner for identification purposes. The host/requesting structure may request the structure responsible for physical security to assist it in acquainting visitors/service providers on security stipulations that must be complied with. **NO** visitors and members of the public must be allowed access to the building during lunch time unless if the host fetches his/her visitor at the security desk/ check point.

c) All visitors to top management must be escorted by the Personal Assistants (PA) or security officers if available, after the necessary access control logistics have been done. Under no circumstance must such visitors be allowed to go to those offices by themselves. Visitors must be escorted back by the security officer on duty.

d) The Security Manager may consider an exception to the rule for member of state security organs – SAPS, SASS, SANDF, VIP guests- provided that such persons are on official duties and provide positive identification and /or appointment certificate. In case of private visits, such officials must be handled as visitors.

11.3 Access procedures

The structure/employee requesting access to DOHS premises by visitors must inform such visitors on the security measures and procedures that must be followed upon entry, as well as on the possibility that searches for prohibited items may be conducted and may be confiscated for safekeeping if found. Persons refusing to be subjected to the prescribed security procedures must not be permitted access to the premises. Visitors on departmental premises must, at all times, obey lawful orders given by authorized officers.

The following specific procedures must be followed for each of the categories of visitors provided for in paragraph 11.2:

a) Official VIP's

The hosts must arrange for the reception and departure of the persons. Any assistant or helper accompanying the person must be issued with a visitor's card for record purposes. The person (VIP) must be made aware that such an assistant/helper has to accompany him/her constantly and also leave the building/premises with him/her.

b) Official Visitors

This category of persons must report to the access control point, adhere to all applicable access control procedures, and be escorted to the venue of the meeting, workplace, etc. by an official of the structure requesting access of the person. The head of the receiving structure must ensure that the visitor is accompanied/escorted at all times while on department premises. No private cars of visitors must be allowed on DOHS premises unless parking is available and parking arrangements have been made in advance.

c) External Service Providers

i) All contractors who have not been issued with a departmental approved access card, desiring access to the premises, must be registered as visitors and be subjected to the security measures.
ii) All contractors must be escorted and under constant supervision, either by a security officer if available, or responsible DOHS official for the duration of his/her visit whilst on the premises especially after hours and weekends.
iii) All equipment in possession of the contractors must be noted and recorded in a security register to ensure that no departmental property is removed from the premises.

d) Key control

i) The security manager as the Key Control Officer of the department will appoint an official in writing as a "key custodian" to manage and control all office keys of the respective departmental premises and a key register will be utilized for this purpose

ii) Key control will only be the function of key custodians' personnel and under no circumstance will the private security company be responsible for key control or handling the "Master Key" (as outlined in the key control procedure).

e) Firearms

i) All departmental premises are declared "gun free" zones and no firearms will be permitted onto the premises, unless for those exempted (SAPS, SANDF and/or SASS)
ii) All firearms with the exception of those in the possession of authorized persons, e.g. police and other authorized officials, shall be handed in at security for safekeeping. All firearms must be recorded in a relevant firearm register. A firearm register must be signed by both the owner of the firearm and the security officer. A gun holding facility will be created to cater for such circumstances.

f) Physical Search

i) Section 13 (Right to Privacy) of the Constitution of the Republic of South Africa has been well established in the Bill of Rights and subject to the limitation clause applicable. Rights to privacy can only be limited if the limitation is reasonable and justifiable in an open democracy based on human dignity, equality and freedom.
ii) Security officers should perform their duties as required by the security policy and one of their duties will be searching of persons. In realizing the crime prevention and loss control strategies to all DOHS offices, Security Services is committed to a zero tolerance with regards to theft or any criminal activity that may result in losses or intolerance to DOHS.
iii) The HOD or his/her delegated official has a duty to safeguard the property of DOHS and to achieve that duty all visitors, contractors, consultants, staff should be searched when coming in or going out. Caution will be made to maintain the employer and employee relationship of trust.
iv) The HOD or his/ her delegated official as the accounting officer has the right to authorize Security Service at any time to conduct searches on persons and vehicles at entrances and exit points, as and when required. The HOD can issue a directive for searching at any time as he/ she so wishes.
v) A search will always be a condition of access to DOHS. The obvious objective is to prevent prohibited items from being introduced where they can be used to effect destruction and or theft of assets or harm to personnel. Security officers will conduct searches on handbags, suitcases and vehicles on a routine or random basis. Such searches will be conducted with consideration to human dignity (male should search males and females should search other females).
vi) The security officer should take care that weapons are not taken into the building: firearms, explosives and any other dangerous objects which could be used to harm or damage. This includes any object, apparatus or equipment or parts thereof which could be used to intercept record, copy or reproduce information, other than that which is the property of DOHS.
vii) Failure or refusal to abide or submit to security instructions or to declare any dangerous objects to security officers when requested to do so will be viewed as a breach of security and the visitor or official concerned will be denied access and removed from DOHS premises. Resistance to removal of the visitor will be overcome with the use of reasonable minimum forces and where necessary an arrest can be affected.

g) Afterhours Access

i) For the purpose of this policy after hours means 17:00 to 06:30 in the morning from Monday to Friday. Public holiday and weekends will be considered after-hours the entire day.

ii) All employees who require access or exit from the premises after-hours should positively identify themselves and subject to completion of the "After-hours access procedures".

iii) No employees will be allowed to enter the premises after-hours if he or she is under the influence of liquor or any intoxicating substances. Such incident constitutes a breach of security and it will be recorded in the necessary internal registers.

iv) No employee may be granted permission to enter the building after hours, weekend and during public holidays if he/ she does not have an official letter from his/ her supervisor notifying security about his/ her reason to enter the office. Such official will have to comply with security procedures before entering the office. Supervisor should notify security management in writing about employees working or requiring access afterhours.

h) **Use of security registers**

Registers are used as a source of information during risk, threat and vulnerability analysis:

i) It can be presented to a court of law as evidence and in a disciplinary hearing;

ii) It can be an evaluation tool for directorate security services effectiveness;

iii) It can be used to compile periodical security breaches statistics;

iv) It can serve as a deterrent for misbehaviour/misconduct of security personnel or staff;

v) It can also be used as a justification for certain security measures.

All security registers utilised within the department remains the property of the Department of Human Settlements and not of the contracted security company.

i) **Deliveries and courier services**

i) All couriered items/documents should be screened at security check point by the security officer in charge.

ii) The addressees of the couriered document/item should at all times be contacted to confirm if they are expecting a delivery.

iii) Food parcels delivered to the Department official should be collected at security check point.

iv) Person delivering food should not be allowed to pass security check point.

11.4. Control over the movement of assets

a) Any asset being moved, whether redundant or obsolete, from or within DOHS buildings/premises must adhere to the protocols specified in the DOHS's Assets

Policy on asset management with specific reference to the requirement that assets may only be moved if accompanied by the prescribed and authorized documentation.

b) All stock/assets/commodities that are moved onto or from DOHS's premises must be declared to the security officer at the point of entry, and must be accompanied by the applicable authorization documentation.

c) Any vehicles may, upon entering or exiting DOHS premises be subjected to detection searches by security officials at the security access point. Documentation authorizing the movement of DOHS goods/commodities must, on request of the security official, be handed to the latter for notification that the goods/commodities and supporting documentation have been checked. Goods/commodities not properly authorized must be confiscated until such time as an investigation has been completed. Any detected irregularities and unauthorized removals must, without delay, be reported to the manager responsible for security and asset management respectively in a written format.

d) All boxes and packages may also be checked at all points of exit/entry into DOHS's buildings and/or at the security entrances onto DOHS premises to ensure that they are accompanied by the necessary official documentation or proof of ownership.

e) All private property, e.g. computer equipment, cameras, recording devices, radios and kitchen equipment etc., brought onto Department premises must be declared to security personnel at the security check point/ reception desk. In case of the removal of State property a removal permit must be completed and handed out at the security checkpoint.

12 INFORMATION MANAGEMENT SYSTEM AND TECHNOLOGY (IMST) SECURITY

12.1 Computer Security

The Computer Security of the Department of Human Settlements must be managed, controlled and maintained in accordance with the Information Technology (IT) policy, Chapter 7 of the MISS deals with Computer Security.

a) In light of the increasing dependence on and the proliferation of computers in the administration of the country in general, and also to the extent to which classified information is processed by means of computers, security becomes essential.

b) Computer security forms the basis of information and physical security, sensitive information needs to be protected when it is processed by computers before it is stored away in the prescribed locking facilities. It is for this reason that computer security is central to the total information security countermeasures within the department.

c) All computer storage media (usually magnetic or optical) are documents in terms of the definition contained in the Protection of Information Act, 84 of 1982. All computer media which is used to store sensitive information must be handled according to document security standards.

d) Computer security awareness should be conducted annually to sensitize all members of the computer security requirements.

e) Against this background the following measures must be implemented:

i) Essential back-up of computer systems and data
ii) Prescribed physical security measures
iii) Established computer security responsibilities
iv) Prescribed use of passwords

f) Staff members should be responsible for safeguarding of computer equipment issued to them.

g) A secure network shall be established for the Department of Human Settlements 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.

h) To prevent the compromise of IT systems, the Department of Human Settlements must implement baseline security controls and any additional control identified through the security Threat and Risk Assessment. These controls, and the security roles and responsibilities of all personnel, must be clearly defined, documented and communicated to all employees.

i) To ensure policy compliance, the IT Manager of the Department Human Settlements must:

   i) Certify that all IT systems are secured after procurement, accredit IT systems prior to operation and comply with minimum security standards and directives;

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

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

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

k) Access to the resources on the network of the Department of Human Settlements must be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals of the Department of Human Settlements must be restricted unless explicitly authorized.

l) System hardware, operating and application software, the network and communication systems of the Department of Human Settlements must all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.

m) All employees must make use of IT systems of the Department of Human Settlements in an acceptable manner and for business purposes only. All employees must comply with the IT Policy in this regard at all times.

n) 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 Policy. In particular, passwords must not be shared with any other person for any reason.

o) To ensure the ongoing availability of critical services, IT Section of the Department of Human Settlements must develop IT continuity plans as part of its overall Business Continuity Management Plan (BCMP) and Disaster Recovery Plan (DRP).

12.2 Internet access

a) The IT manager of the Department of Human Settlements has the overall responsibility for setting up Internet access for the Department of Human Settlements must ensure that the network of the Department is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall. IT section must 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. Internet facility must be monitored for the purpose of information security.

b) The IT Manager of the Department of Human Settlements must be responsible for controlling user access to the internet, as well as for ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security breaches and incidents. Access to internet must be limited and made available under control.

c) 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.

d) The system administrator must run a "password cracker" program at least every three months (or often) and requires the user to immediately change any easily cracked passwords.

The following are the requirements for using passwords:

i) Do not use your login name as a password
ii) Do not use your first name, middle or last name as your password
iii) Do not use the names of your family members as your password
iv) Do not use license plates numbers, phone numbers or street names as your password
v) Do not use consecutive numbers or letters (12345678) as your password
vi) Do not share passwords with anyone. Passwords must be kept confidential like an ATM Pin Number and it should be immediately changed when compromised.
vii) Do not allow group accounts with a common password

12.3 Use of mobile devices

a) Usage of laptop computers by employees of the Department of Human Settlements is restricted to business purposes only, and users must be aware of, and accept the terms and conditions of use, especially the responsibility for the security of information held on such devices.

b) The information stored on a laptop computer of the Department of Human Settlements must be suitably protected at all times in line with the protection measures prescribed in the IT Security Policy.

c) 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 Policy. Laptops should be carried in such a way that it does not draw unnecessary attention from criminal elements in public areas.

d) In the event of the device getting lost the user must report it to the immediate

supervisor and also report to SAPS.

1.3 COMMUNICATION SECURITY

a) No classified/ sensitive information may be conveyed via an open landline, cellular phone, open facsimile and open email communication, unless secure communication software has been installed.

b) The transmissions of classified/sensitive information via any telephone, facsimile and or cellular communication constitutes a breach of security because information can be compromised by interception by the adversaries or enemies. In case of speech transmission of sensitive/classified information, the provided Secure Speech Unit (SSU900) must be used.

c) The South African Communication Security Agency (SACSA)/Comsec are the sole distributing authority of encryption equipments and are also responsible for installation, maintenance, disposal and training on encryption equipments. No other commercial encryption service provider will be allowed to provide, maintain, dispose or train DOHS employees on encryption equipments, other than SACSA or Comsec.

d) Do not discuss sensitive information on a cellular phone (particularly members of top management) unless the required secure communication equipment has been installed. When you make calls from a cell phone consider advising the other party that you are calling from a cell phone that is vulnerable to monitoring and that you will be speaking generally and not getting into sensitive matters.

e) All members of top management must avoid using cellular telephone within several miles of the airport, stadium, shopping centres or other heavy traffic locations. These are areas where radio hobbyists use scanners for random monitoring. If they come across an interesting conversation, your number may be marked for regular selective monitoring for life.

f) The repairs of departmental landlines must be monitored and controlled and a technician rendering repair services must be positively identified.

g) Members must (especially top management) not take cellular phones for repairs at any repair shops and it is also advisable that after repairs of the phone, SSA Operational Support be requested to debug the cell phone after repairs.

13.1 Access to Encryption Equipment

All employees that operate the cryptographic equipments must be security cleared by the SSA to a minimum security clearance of secret and access to, and operation of SACSA encryption equipment installed in the Department, must be restricted to authorised officials only.

13.2 Transmission of Classified Information via Internet

a) The transmission of classified/sensitive information via the Internet is prohibited because the internet is vulnerable for interception (hacking), unless email encryption software has been installed.

b) All staff members in the office of the HOD must be discouraged to communicate sensitive information via the internet.

13.3 Recording of fax transmissions

All incoming and outgoing fax transmission, via the encryption system must be recorded in the appropriate registers provided by SACSA or Comsec.

13.4 Reporting of security breach

Any security breach on the encryption system must immediately be reported to the Security Manager.

14 TECHNICAL SURVEILLANCE COUNTER MEASURES (TSCM)

14.1 The HOD of the department must ensure that areas that are utilised 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 SSA in order to support the sterility of the environment after TSCM examinations.

14.2 The Protection of Information Act also requires departments to provide security measures in all offices and boardrooms where sensitive information is discussed to counter espionage. Espionage is the illegal gathering of business data, information, trade secrets which includes bribery, coercion, breaking and entering and installing of listening devices.

14.3 All offices, boardrooms and conference rooms where sensitive matters are regularly discussed should be subjected to regular electronic surveillance counter measures (sweeping), proper and effective access control. It is essential that proper key and access control is implemented before and after the sweeping exercise has been conducted to keep the office sterile for a longer period. It is fruitless to conduct TSCM exercise where access control is not effectively controlled because the office can be compromised as soon as the exercise is completed.

14.4 No electronic equipment, computers, tape recorders, video cameras, television, projectors and cellular phones (even if the cellular phone is switched-off) shall be permitted into "secure boardrooms" during a meeting in order to prevent eavesdropping, other than those already installed for the functioning of the boardroom. Cellular phone holding facilities must be made available in all boardrooms.

14.5 Access Control to Secure Boardrooms

a) A boardroom is a restricted area; therefore strict access control must be applied and enforced regarding access to "secure boardrooms".

b) Only authorised officials must be allowed into "secure boardrooms".

c) All boardrooms where sensitive information is discussed must be locked at all times and if the boardroom is not locked it constitutes a breach of security and misconduct on the part of the responsible official. Keys to all boardrooms where sensitive information is discussed must be kept by a key custodian who will lock and unlock the boardroom on request.

14.6 Debugging (Sweeping) exercise

A sweeping exercise (TSCM) will be conducted annually in all areas where sensitive information is discussed and also upon request by the HOD or his/ her delegate.

15 SPECIFIC ROLE AND RESPONSIBILITY

15.1 The role of the State Security Agency (SSA)

a) The SSA must coordinate between the Intelligence Structures regarding the implementation of defensive counter intelligence measures at the Department of Human Settlements.

b) SSA is responsible to assist the DOHS (within its legislative mandate but excluding the National Intelligence Structures) to establish effective security within their own environments and to monitor their adherence to these regulations and the Minimum Information Security Standards.

c) SSA advise the DOHS with regards to:

i) Counter Intelligence within the Republic
ii) Document Security
iii) Personnel Security (Preliminary Vetting and Security Clearance)
iv) Information Technology (in consultation with State Information Technology Agency)
v) Information Security Audits and Appraisals
vi) Technical Surveillance Counter Measures (TSCM)
vii) Security Management Training
viii) Investigation of security breaches

15.2 South African Police Service (SAPS)

a) The SAPS is responsible to assist DOHS (within its legislative mandate) to establish effective physical security measures within their environments and to monitor their adherence to these regulations and the implementation of the Minimum Physical Security Standards relating to physical security.

b) Further the SAPS conduct criminal investigation (internal security breaches e.g. theft) and the co-ordination of security officers training.

15.3 The role of COMSEC

a) To advise and assist DOHS on the implementation of the minimum standards relating to communication security contained in the Minimum Information Security Standards. This includes the provision of encryption equipments, installation, training and maintenance.

b) Assess and report on the application of communication security technical safeguards in both the public and private sector.

15.4 Head of Department (HOD)

The Head of the Department of Human Settlements bears the overall responsibility for enforcing the security policy and program of the Department. Towards the execution of this responsibility, the HOD must:

a) Establish the post of the Security Manager and appoint a well-trained and competent security official in the post;

b) Appoint a security committee for the institution and ensure the participation of all management members of all the core business functions of the Department of Human

Settlements in the activities of the committee;

c) The HOD must oversee the development, implementation and maintenance of an internal security policy for DOHS complying with all the requirements of the MISS.

d) The HOD relies on the Senior Managers of the different directorates/components for the execution of the security policy and the implementation and maintenance of security measures in the department. The responsibility to ensure the execution of the security policy and the implementation and maintenance of security measures in the department is therefore delegated to the managers of the different directorates.

e) Approve and ensure compliance with this policy and its associated Security Plan by all it is applicable to.

15.5 Security Manager (SM)

a) The delegated security responsibility lies with the Security Manager of the Department of Human Settlements who will be responsible for the execution of the entire security function and program within the Department of Human Settlements (coordination, planning, implementing, controlling, etc.). Towards the execution of his/her responsibilities, the Security Manager must, amongst others:

i) chair the security committee of the Department of Human Settlements
ii) draft the internal Security Policy and Security Plan of the Department of Human Settlements in conjunction with the security committee;
iii) review the Security Policy and Security Plan at regular intervals;
iv) conduct a security Threat and Risk Assessment (TRA) of the Department of Human Settlements with the assistance of the security committee;
v) advise management on the security implications of management decisions;
vi) implement a security awareness program;
vii) report breaches and security incidents directly to the HOD
viii) conduct internal compliance audits and inspections at the Department of Human Settlements at regular intervals; and
ix) establish a good working relationship with both SSA and SAPS and liaise with these institutions on a regular basis.

15.6 Security Committee

a) The Security Committee must consist of managers of the Department of Human Settlements representing all the main business units of the Department.

b) Participation in the activities of the Security Committee by the appointed representatives of business units of the Department of Human Settlements must be compulsory.

c) The Security Committee of the Department of Human Settlements must be responsible for, amongst others:

i) assisting the Security Manager in the execution of all security related responsibilities at the Department of Human Settlements, including completing tasks such as;
ii) drafting/reviewing of the Security Policy and Plan,
iii) conducting of a security Threat and Risk Assessment (TRA),
iv) conducting of security audits,
v) drafting security BCMP and

vi) assisting with security awareness and training.

15.7 Line Management

a) All managers of the Department of Human Settlements must ensure that their subordinates comply with this policy at all times.

b) 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.

15.8 District offices

a) The District Manager is responsible for the implementation of the internal security policy and other security requirements in the Districts. The service provider at district, reports to the District Manager on all security issues of that region with the direction and guidance and consultation with the Security Manager at Head Office.

b) The District Manager must ensure that security policy, procedures, and standards are maintained in the District Office.

15.9 Employees, Consultants, Contractors and other Service Providers

a) Every employee, consultant, contractor and other service providers of the Department of Human Settlements shall know what their security responsibilities are, accept it as part of their normal job function, and not only cooperate, but contribute to improving and maintaining security at the Department of Human Settlements at all times.

16 COMMUNICATING THE POLICY

a) The Security Manager of the Department of Human Settlements must 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 of Human Settlements. The Security Manager must further ensure that security policy is enforced and complied with.

b) The Security Manager must ensure that a comprehensive security awareness program is developed and implemented within the Department of Human Settlements to facilitate the above said communication. Communication of the policy by means of this program must be conducted as follows:

i) awareness workshops and briefings to be attended by all employees;
ii) distribution of memos and circulars to all employees;
iii) access to the policy and applicable directives on the intranet of the Department of Human Settlements

17 ENFORCEMENT

a) The Head of Department and the appointed Security Manager are accountable for the enforcement of this policy.

b) All employees of the Department of Human Settlements are required to fully comply

with this policy. Non-compliance with the policy shall be addressed in terms of the Disciplinary Code/Regulations of the Department of Human Settlements.

c) Prescripts to ensure compliance to this policy by all consultants, contractors or service providers of the Department of Human Settlements must be included in the contracts signed with such individuals/institutions/companies. The consequences of any transgression/deviation or non-compliance must be clearly stipulated in said contracts and shall be strictly enforced. Such consequences may include the payment of prescribed penalties or termination of the contract, depending on the nature of non-compliance.

18 AUDITING AND MONITORING OF COMPLIANCE

a) The Security Manager, with the assistance of the security component and security committee of the Department of Human Settlements must ensure compliance with this policy by means of conducting internal security audits and inspections on a regular basis.

b) The findings of said audits and inspections must be reported to the Head of Department after completion thereof.

19 REVIEW AND UPDATE PROCESS

a) The influence of environmental factors (e.g. legislation, technology etc.) will directly or indirectly affect certain security measures, procedures and terminology in future. In order to keep abreast with the changing environments, and being proactive to any security risks/threats, this policy document will be subject to review in order to render quality service and thus to maintain a crime-free, safe working environment in which security threats and risks are mitigated.
b) The policy will be reviewed two years after implementation date; or as and when the need arises.

20 SPECIFIC BASELINE REQUIREMENTS

20.1 Security Organisation

a) The Head of the Department of Human Settlements has appointed a Security Manager (SM) to establish and direct a security program that ensures co-ordination of all security policy functions and implementation of policy requirements.

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

c) The Head of the Department of Human Settlements must ensure that the SM has an effective support structure (security component) to fulfill the functions referred to in par.15.5 above.

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

20.2 Security administration

The security functions include:

a) general security administration (departmental directives and procedures, training and awareness, security risk management, security audits, sharing of information and assets);
b) setting of access limitations;
c) administration of security screening;
d) implementing physical security;
e) ensuring the protection of employees;
f) ensuring the protection of information;
g) ensuring IMST security;
h) ensuring security in emergency and increased threat situations;
i) ensuring security in contracting; and
j) facilitating security breach reporting and investigations.

20.3 Security incident/breaches reporting process

a) Whenever an employee of the Department of Human Settlements becomes aware of an incident that might constitute a security breach or an unauthorized disclosure of information (whether accidentally or intentionally), he/she must report that to the SM of the Department of Human Settlements by utilizing the formal reporting procedure using prescribed incident report form.

b) The SM of the Department of Human Settlements must report to the HOD all cases or suspected cases of security breaches, for investigation purpose.

c) The SM of the Department of Human Settlements must ensure that all employees are informed about the procedure for reporting security breaches.

20.4 Security breaches and investigation

a) The SM must develop and implement security breach response mechanisms for the Department of Human Settlements in order to address all security breaches/alleged breaches which are reported.

b) All security breaches, potential or alleged security breaches must immediately be reported to the Security Manager or security control room. Among others, security breaches shall mean the following:

i) leakage of sensitive information; wittingly or unwittingly to the media and/or unintended recipients;
ii) burglary, robbery, assault, pointing of firearm;
iii) theft of departmental property i.e. laptop, cellular phones, cameras etc.;
iv) intimidations;
v) loss of access cards or keys;
vi) threats (telephonic, verbal and/or physical);
vii) any malpractice that may have potential to cause harm to human lives, damage to assets etc.;
viii) suspicious objects and/or unknown person wandering around the premises;
ix) ex-employees (fired) or employees on suspension wandering in the premises.

c) All security breaches must be reported within 48 hours to the nearest South African Police Service station and immediately to the Security Manager by the responsible official.

d) An affidavit with full descriptions surrounding the circumstances which led to the loss and particulars of equipment (e.g. model, serial numbers and cost etc.) must be indicated and the case number and investigating officer of SAPS must be forwarded to the Security Manager.

e) The reporting protocols: all security breaches must be reported to the Security Manager or his delegate and the Security Manager and/or his delegate will report as follows:

20.5 Security Manager will liaise with

a) The State Security Agency (SSA) in the case where:

i) an incident constitutes a breach of security where sensitive information is lost, stolen and/or tampered with;

b) The South African Police Service (SAPS) in the case where:

i) an incident is of a criminal nature;

c) Comsec and/or SACSA in the case where:

i) an incident involves theft of cryptographic equipment. The SSA must also be notified of the incident and it should also be reported to SAPS because theft is a criminal offence.

d) The purpose of internal investigation is not only to determine what went wrong or to identify the wrongdoer but also to identify vulnerable areas, to assess the damage, determine which specific measures were not adhered to or not effective or even absent. Further, internal investigations are conducted to recommend appropriate security countermeasures and internal control systems to avoid recurrence of the security breach.

e) Breaches of security must always be dealt with the highest degree of confidentiality in order to protect the official(s) concerned and to avoid divulgence of sensitive information.

f) The Security Manager will report internally all security breaches to the HOD and to the Security Committee.

g) All investigations should be conducted within the ambit of the Constitution of the Republic of South Africa (Bill of Rights) and/or Criminal Procedure Act.

h) The Department may outsource the services of a private investigator to conduct investigation within the department.

i) Access privileges to classified information, assets and/or to premises may be suspended by the Head of the Department of Human Settlements until administrative, disciplinary and/or criminal processes have been concluded, flowing from investigations into security breaches or alleged security breaches.

j) The end result of these investigations, disciplinary action or criminal prosecutions may be taken into consideration by the Head of the Department of Human Settlements 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.

21 DISCIPLINARY ACTION

a) Non-compliance with this policy must result in disciplinary action which may include, but are not limited to:

i) Re-training;
ii) Verbal and written warnings;
iii) Termination of contracts in the case of contractors or consultants delivering a service to the Department of Human Settlements;
iv) Suspension and;
v) Dismissal.

b) Any disciplinary action taken in terms of non-compliance with this policy and its associated directives must be in accordance with the disciplinary code/directive of the Department of Human Settlements

22 STAFF ACCOUNTABILITY AND ACCEPTABLE USE OF ASSETS

a) The HOD must ensure that information and assets of the Department of Human Settlements are used in accordance with procedures as stipulated in the Security Policy as will be contained in the Security Plan of the Department of Human Settlements.
b) All employees of the Department of Human Settlements must be accountable for the proper utilization and protection of such information and assets. Employees that misuse or abuse assets of the Department of Human Settlements must be held accountable and therefore disciplinary action must be taken against them.

23. BUSINESS CONTINUITY MANAGEMENT PLAN (BCMP)

a) Every directorate of the department of Human Settlements must make input to the Business Continuity Management Plan (BCMP) which should provide the continued availability of critical services, information and assets if a threat materialises and to provide for appropriate steps and procedure to respond to an emergency situation to ensure the safety of employees, contractors, consultants and visitors.

b) The HOD or duly appointed official is responsible for all the employees of the Department of Human Settlements and must be made aware and trained on the content of the BCMP to ensure understanding of their own respective roles in terms thereof.

c) The HOD or duly appointed official is responsible to ensure the departmental BCMP is kept updated and re-viewed periodically to ensure that management and employees of the Department of Human Settlements understand how it is to be executed and to include inputs from all directorates.

24. AUDIENCE

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

25. EXCEPTION

Deviations from this policy will only be permitted under the following circumstances:

a) When security must be breached in order to save or protect the lives of people during unavoidable emergency circumstances e.g. natural disaster;

b) On written permission of the Head of Department (reasons for allowing non-compliance to one or more aspects of the policy must be clearly stated in such permission; no blanket non-compliance must be allowed under any circumstances).

26. OTHER CONSIDERATIONS

The following must be taken into consideration when implementing this policy:

a) Occupational Health and Safety issues in the Department of Human Settlements

b) Disaster Management at the Department of Human Settlements.

c) Disabled persons must 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.

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

27. IMPLEMENTATION

a) The Security Manager of the Department of Human Settlements must manage the implementation process of this policy by means of an action plan (also to be included in the Security Plan of the Department of Human Settlements).

b) Implementation and adherence to this policy is the responsibility of each and every individual this policy is applicable to.

28. SECURITY AWARENESS AND TRAINING

a) A security training and awareness program must be developed by the Security Manager and implemented to effectively ensure that all personnel and service providers of the Department of Human Settlements remain security conscious.

b) All employees must be subjected to the security awareness and training programs and must certify that the contents of the programme(s) has been understood and will be complied with. The program must 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 of Human Settlements and the need to protect sensitive information against disclosure, loss or destruction.

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

d) Regular surveys and walkthrough inspections shall be conducted by the SM and members of the security component to monitor the effectiveness of the security training

k) Trespass Act, 1959 (Act 6 of 1959)
l) Electronic Communication and Transaction Act, 2002 (Act 25 of 2002)
m) Electronic Communications Security (Pty) Ltd Act, 2002 (Act 68 of 2002)
n) State Information Technology Agency Act, 1998 (Act 88 of 1998)
o) Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act 70 of 2002)
p) General Intelligence Law Amendment Act, 2000 (Act 66 of 2000)
q) National Strategic Intelligence Act, 1994 (Act 39 of 1994)
r) National Key points Act, 1980 (Act No 102 of 1980)
s) National Personnel Security Vetting Policy
t) Labour Relations Act, 1995 (Act 66 of 1995)
u) Employment Equity Act, 1998 (Act 55 of 1998)
v) Fire-arms Control Act, 2000 (Act 60 of 2000) and regulations
w) Protection of Constitutional Democracy Against Terrorism and Related Activities Act, 2004 (Act 33 of 2004)
x) National Building Regulations and Building Standards Act, 1977 (Act 103 of 1977)
y) Protected Disclosures Act, 2000 (Act 26 of 2000)
z) Intimidation Act, 1982 (Act 72 of 1982)
aa) Prevention and Combating of Corrupt Activities Act, 2004 (Act 12 of 2004)
bb) Public Finance Management Act, 1999 (Act 1 of 1999) and Treasury Regulations
cc) Protection of Personal Information Act, 2013 (Act 4 of 2013)

Other regulatory framework documents and policies

a) Minimum Information Security Standards (MISS), Second Edition March 1998
b) Minimum Physical Security Standards (MPSS)
c) White paper on Intelligence (1995)
d) SACSA/090/1(4) Communication Security in the RSA
e) SSA Guidance Documents: ICT Policy and Standards: Part 1 & 2
f) ISO 17799
g) National Building Regulations
h) Chapter 2, Page 14 of the Public Service Handbook (SMS)
i) Cabinet Memo dated 2006 December 06
j) Protection of Personal Information Act (POPIA) Compliance Policy Framework
k) IMST Information Security Policy

6. GENERIC PRINCIPLES

a) Employees of the Department of Human Settlements must be protected against identified threats according to baseline security requirements and continuous security risk management.

b) Information and assets of the Department of Human Settlements must be protected according to baseline security requirements and continuous security risk management.

c) The principles relating to the information security within the Department of Human Settlements are governed through the POPIA Compliance Policy Framework and IMST Information Security Policy.

d) Continued delivery of services of the Department of Human Settlements must be assured through baseline security requirements, and continuous security risk management.

7. DOCUMENT SECURITY

and awareness program.

29. EFFECTIVE DATE

This policy is effective from the date of signatory by the Head of Department.

HEAD OF DEPARTMENT: KZN DEPARTMENT OF HUMAN SETTLEMENTS
DATE: 1 April 2023.