LIMPOPO PROVINCE

INFORMATION SECURITY POLICY

EXECUTIVE COUNCIL APPROVAL

On the 31 October 2001 the Executive Council of the Limpopo Province Government approved the Information Security Policy.

LIMPOPO PROVINCIAL GOVERNMENT INFORMATION SECURITY POLICY

CHAPTER 1

1. INTRODUCTION

1.1 With the dawn of democracy effect is given to the constitutional right of access to any information held by the state and any information that is held by another person and that is required for the exercise or protection of any rights, and to provide for matters connected therewith.

1.2 However the **PROMOTION OF ACCESS TO INFORMATION ACT NO 2 OF 2000** acknowledges the need for protection of sensitive information and therefore provide for justified exemption from disclosure of such information, that category of information which is exempted need protection.

1.3 Information in the wrong hands can damage operational relations between Government put people out of work, and can also result in declaration of war.

1.4 With the dawn of the computer age, people have a new technology to use and abuse.

1.5 The threat of espionage activities through theft of sensitive information and illegal eave dropping in South Africa is real. Widespread and the security of our information are at risk. Security hazards exist which are exploited by growing number of foreign hostile intelligence agents and unauthorised people.

1.6 The only way to counter the threat of espionage activities and unauthorised disclosure of sensitive information is to apply security measures in full. This policy is aimed at providing the necessary procedures and measures to protect sensitive information from unauthorised disclosure. These procedures are not contrary to transparency, but indeed necessary for responsible government.

1.7 This policy document contains security guidelines, which are aimed at protecting the Government's assets, interests and activities, as well as classified matters and/or information about such maters, and the personnel involved. The procedures and measures taken up in this volume are based on general security principles and are in essence the minimum

standard for handling classified information.

1.8 Apart from the above, it is important to note the philosophy stating that management (on all levels) must accept responsibility for security, and therefore become involved in protecting the assets of the Government, the so-called top-down approach. Generally it is the view that there can be no security –

- If there are no security standards or institutionalised policy on security.
- If these standards do not form a comprehensive system of measures;
- If this system of measures is not properly managed;
- If these measures are not adhered to or enforced; and
- If personnel are not security-conscious.

1.2 PURPOSE

1.2.1 The purpose of this document is to establish a security policy for the Provincial Government.

1.3 SCOPE

1.3.1 In view of the fact that security is to be implemented and maintained in accordance with specific acts and legal directives, this policy document was drafted to conform with such acts and directives, and makes provision for the following:

- Statutory requirements.
- Definitions.
- Responsibility for the establishment and implementation of security measures.
- Security of classified documents, information and material (document security).
- Personnel security.
- Computer security.
- Communication security.
- Physical security measures.
- Project security.

- Security breaches.

1.4 SUPPLEMENTS

1.4.1 Addenda to detail procedures or to elucidate policy aspects or applications will be issued as and when necessary.

1.5 THE NEED FOR INFORMATION SECURITY POLICY

1.5.1 It is believed that Governments worldwide have lost control over sensitive information at their disposal. Espionage or illegal eavesdropping has affected many Governments operations, as they have no effective internal counterintelligence policies in place.

1.5.2 Information in wrong hands can destroy the Government. Major decisions are often made orally long before they are committed to writing. Technological developments allow illegal eave dropper's access to locations where sensitive discussions are held and where decisions are made.

1.5.3 Information of whatever nature that has possible importance to a foreign hostile intelligence agent or an illegal eave dropper, and sufficient value to compensate for the trouble, expense and risk associated with the clandestine effort, forms the basis for a counterintelligence programme and the conduct of regular counter intelligence assessment.

- **The first step is to recognize the potential to be a target**
- **The next or second step is assessing the threat of unauthorised disclosure of sensitive information and eave dropping**
- **The third step is assessing how vulnerable you or your facilities are to leakage of sensitive information and eave dropping and to develop a risk acceptance posture**

CHAPTER 2

2. OBLIGATION AND SECURITY RESPONSIBILITIES BY STATUTE.

2.1 A number of Departments / Institutions have been appointed custodians of certain specific security functions and responsibilities on national level. These Departments have been designated the duty of creating guidelines, giving and enforcing policies and procedures throughout the departments, Parastatals, national key points, etc.

2.2 The responsibilities are allocated as follows:

- Communication Security - SANDF through SACSA
- Computer Security - NIA
- Documentation Security - NIA
- Information Security - NIA
- Personnel Security (Vetting and Awareness) – NIA
- Physical Security - SAPS into MEC Homes & Offices
- Security Training - SAPS, NIA and ICTS

2.2.1 Notwithstanding the above responsibilities, the Director General, as Head of the Limpopo Provincial Government, remains responsible according to the Public Service Act, 1994 in as far as all security matters are concerned. He/She may, however delegate all or certain security responsibilities to the Heads of departments.

2.2 Administrative responsibilities

2.2.1 As the DG and HOD'S are unable to personally address the security needs of each department, authority and responsibility in respect of security is delegate to the Security and Risk Management Services in the Office of the Premier as well as those Security Managers who have been appointed in other government departments. These security structures are responsible to administer all aspect of security within the departments in the Limpopo Provincial Government.

2.2.2 The Security and Risk Management Services as well as Security Managers are empowered by the following Acts or Statutes to perform their specific duties and responsibilities:

- The Constitution of the RSA
- Public Service Regulation of 1996

- The Interception and Monitoring Prohibition Act, Act 127 of 1992.
- The Protection of Information Act, 1982 (Act 84 of 1982).
- Control of Access to Public Premises and Vehicles Act, 1985 (Act 53 of 1985).
- The Security Official Act, 1987 (Act 92 of 1987).

2.3 Functional responsibilities

2.3.1 The functional /operational responsibilities of various security measures and procedures are primarily the responsibility of each and every member of the department, irrespective of rank. All managers and supervisors must ensure that all times and that the relevant procedures are adhered to and that any discrepancies be reported timorously to the Security Manager or Head of Security and Risk Management Services. Such discrepancies should be reported to the department designated e.g. NIA if it concerns Information Security, Document Security etc and SAPS if it concerns Physical Security etc. Such report should be made immediately after the incident even if an internal investigation would be conducted by the department or the Security and Risk Management Strategies.

2.3.2 The performance of physical security duties, access control and guarding duties should be done by either the members of the in – house security personnel or by members of private security contractors in line with the Provincial Contract Management Policy.

2.3.3 The authority to take necessary actions in all security related matters are delegated to the Head: Security and Risk Management Strategies and Security Managers within the departments.

CHAPTER 3

DEFINITIONS

3.1 ACCESS CONTROL

(a) The process and measures by which access to and exit from an e.g. a government premises is controlled or restricted. The authority for these

measures is outlined in the *Control of Access to Public Premises and Vehicles Act, 1985* (Act 53 of 1985) as amended.

3.2 ACCESS CONTROL CARD

(a) A card that is issued in accordance with the Government directives to a qualifying person subject to certain conditions, allowing that person access to specific areas.

3.3 AUTHOR (ORIGINATOR OF DOCUMENTS)

(a) Any person acting on behalf or in the interest of the state whether employed by the state or not, but who generates or prepares a document whether it is classified or not.

3.4 CLASSIFIED INFORMATION

(a) Information that is regarded as sensitive in terms of the activities of the Government, and must by reason of its sensitive nature be exempted from disclosure and therefore enjoy protection against compromise. Such information is classified as Restricted*, Confidential* and Top Secret. Remark. "Information" used as a descriptive term in this security policy refers to all forms of communication, that is, verbal, written, magnetic or electronic. "Activities" of the Government refer to any design, development, product, planning, cooperation or function of a proprietary nature.

3.5 CLASSIFY/RECLASSIFY

(a) The grading/categorising or regarding / re-categorising of information, in accordance with its sensitivity or in compliance with a security requirement.

3.6 CRITERIA FOR CLASSIFICATION

(a) To avoid confusion, Departments must maintain uniformity with respect to the classification system and assign to documents the same rating in accordance with degree of security warranted by the contents and nature of the documents. All departments as defined below should therefore apply the security classifications.

(a) Note: Security measures are not intended and should not be applied to cover up misadministration, corruption, criminal actions, etc, or to protect individual / officials involved in such cases. The following descriptions should be understood accordingly:

3.7 Restricted

(a) Definition: RESTRICTED is that classification allocated to all information that may be used by hostile / opposing /malicious elements to hamper the activities or inconvenience the Department or any institution dealing with the Provincial Government or an individual.

3.8 Confidential

(a) Definition: The classification CONFIDENTIAL should be limited to information that may be used by hostile /opposing / malicious elements to harm the objectives and functions of the Department or institutions dealing with the Department or individuals.

3.9 Secret

(a) Definition: SECRET is the classification given to information that may be used by hostile / opposing / malicious elements to disrupt the objectives and functions of the Department and / or institutions dealing with the Department.

3.10 Top Secret

(a) Definition: TOP SECRET is given to information that can be used by hostile opposition / malicious elements to neutralize the objectives and functions of Departments and or the Provincial Government.

3.11 COMMUNICATION SECURITY

(a) That condition created by the conscious provision and application of security measures for the protection of classified information communicated through electronic means, ensuring that the confidentiality, integrity, accountability and authentication of data during and after transmission is maintained.

3.12 COMPROMISE

(a) The unauthorised disclosure/exposure or loss of classified information, or information qualifying for classification, or exposure of sensitive activities, people or places, whether by design or through negligence.

3.13 CONFIDENTIALITY AGREEMENT

(a) An undertaking given by a person who will have, has or has had access to

classified information, that he/she will treat such information in accordance with its sensitivity and security classification (see Annexure A for an example).

3.14 CONSULTANT

(a) Any institution, or member thereof, providing a specific service as consultant.

3.15 CONTINGENCY PLANNING

(a) The prior planning of any steps that have the purpose to prevent and/or combat, or counteract the effect and results of an emergency situation where lives, property or information of the Government is threatened. This includes compiling, approving and distributing a formal, written plan, and practising this, in order to identify and rectify gaps in the plan, and to familiarise staff and coordinators with the plan.

3.16 CONTRACTOR

(a) Any institution, or member thereof, providing a specific service as contractor or subcontractor.

3.17 COPYING/DUPLICATING/REPRODUCING

(a) The making of a copy of information (irrespective if in document, mechanical or electronic format), whether by copying it out by hand, by photographic means, audio recording, electronic or any other means.

3.18 DELEGATE/ALTERNATE

(a) A delegate/alternate is a person who is granted certain powers/authorities or functions in order to represent a higher authority in performing a specific task.

3.19 DOCUMENT

(i) In terms of the Protection of Information Act (Act 84 of 1982) a document is;

a. Any note or writing, whether produced by hand or by printing, typewriting or any other similar process;
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.

3.20 DOCUMENT SECURITY

(a) That condition which is created by the conscious provision and application of security measures in order to protect documents with sensitive contents.

3.21 ESPIONAGE

(a) The methods by which individuals, organisations, business enterprises or states attempt to obtain classified information to which they are not entitled.

3.21 HEAD OF DEPARTMENT

(a) The person who is serving as the head of a department, whether defined by directive or otherwise, including the official acting in his place.

3.22 IDENTIFICATION

(a) The identification of a person for the purpose of access to a security area (that is, an area that is being secured by security regulations because of activities that necessitate such measures), which entails positive recognition through a Government identification card, a national identity document, a passport or similar document, or by physical identification through another identified Government employee.

3.23 INFORMATION

(a) Information is any recorded or displayed data or knowledge or content of communication, regardless of its format.

3.24 INFORMATION SECURITY

(a) That condition created by the conscious provision and application of a system of document, personnel, physical, IT and communication security measures to protect classified information.

3.24 INFORMATION SECURITY AUDIT

(a) An information security audit is the physical inspection of official files containing classified documents to ensure that they are classified, marked and handled according to the provisions contained in this security policy and of all registers used by the divisions for managing the whereabouts of such documents or classified information, including copies and facsimiles. Remark. An information security audit forms part of a security audit (see “Security

Audit").

3.25 INFORMATION TECHNOLOGY SYSTEM (ITS) SECURITY

(a) ITS security is that discipline of the security practice that aims to protect information technology systems, data, applications and transactions/processes against unauthorised access, and to protect computer hardware, software and data from accidental or deliberate unauthorised changes, destruction, disposal, removal and/or disclosure.

3.26 INSTITUTION

(a) "Institution" means any department of State, body or organisation that is subject to the Public Service Act, or any other law or any private undertaking that handles information classifiable by virtue of national interest.

3.27 SECURITY VETTING

The process followed to determine whether a person is able to maintain confidentiality and whether his/her trustworthiness is without reproach. It includes the person's ability to handle information of a classified or proprietary nature in such a manner that he/she does not cause this information or material to fall into unauthorised hands, thereby harming or endangering the interests of the Government.

3.28 IRREGULARITY

(a) Any deviation from the directives of this policy, as well as any other circular concerned with security and the protection of Government interests.

3.29 MANAGER: SECURITY AND RISK MANAGEMENT SERVICES

(a) A senior authority of the section responsible for security within a Department. The Head of the Security and Risk Management Services.

3.30 NEED-TO-KNOW PRINCIPLE

(a) The furnishing of only that classified information or part thereof that will enable a person(s) to carry out his/her task, normally in accordance with that person's level of security competence.

3.31 PERSONNEL SECURITY

(a) Personnel security is that condition created by the conscious provision and application of security measures in order to ensure that any person who gains access to classified information or information of a sensitive proprietary nature, does have the necessary security grading or proof of security competence (irreproachable trustworthiness), and conducts him/herself in a manner not endangering him/her or the information to compromise.

3.32 PHOTOGRAPHY

(a) The term photography relates to the action of taking photographs and includes all negatives and prints of negatives. This is inclusive of cine films, slides, films, television transmissions, aerial photography films, video tapes, and other forms of reproduction such as drawings, sketches, models, maps, plans, annual reports, advertising brochures and industrial magazines.

3.33 PHYSICAL SECURITY

(a) That condition which is created by the conscious provision and application of physical security measures for the protection of persons, property and information.

3.34 PROJECT SECURITY

(a) The application of all security disciplines to ensure that the existence, contents or outcome of a project or plan is not compromised at any stage. Project security principles are applied from conception and maintained until a decision is taken to change the classified nature of the project or plan, or part thereof.

3.35 ROOF OF SECURITY COMPETENCE

(a) Proof of security competence is a written approval by the Manager: Security and Risk Management Services or of a Security section within a Department that the security competence of an employee of the Government has been determined through a security vetting process, and that such a person is thus authorised to have access to information with a specified grade of security classification, or which is of a proprietary sensitive nature, which the person needs for the execution of his/her official duties.

3.36 PROTECTION OF PERSONS

(a) The physical protection of identified important persons against violence and insults, as well as the protection of information in the possession of such persons against unauthorised exposure or disclosure to

malicious/opposing/hostile elements or persons.

3.37 RECEIPT OF CLASSIFIED DOCUMENTS

(a) The receipt and documentation or taking on record of classified documents.

3.38 SECURITY

(a) That condition free of risk or danger to lives, property and information created by the conscious provision and application of protective security measures.

3.39 SECURITY AREA

Any area to which the general public is not freely admitted and to which only authorised persons are allowed.

3.40 SECURITY AUDIT

(i) That part of security control undertaken to:

a. Determine the general standard of physical, personnel and information security and to make recommendations where shortcomings are identified;

b. Evaluate the effectiveness and application of security policy/standards/ procedures and to make recommendations for improvement where necessary;

c. Provide expert advice with regard to security problems experienced; and

d. Encourage a high standard of security awareness.

3.41 SECURITY AND RISK MANAGEMENT SERVICES

(a) The Section in the Government responsible for overseeing the design and implementation and monitoring the full spectrum of security measures in the Government.

3.41 SECURITY LOCK

(a) A lock with at least six levers or five checks of which the tumblers are not

springy (e.g. Chubb, Abloy and Real).

3.42 SECURITY MEASURES

(a) All actions, measures and means employed to achieve and ensure a condition of security commensurate with the prevailing threat against the interests of the Government.

3.43 STORAGE

(a) The safekeeping of classified documents in appropriate (prescribed) lockable containers, strong rooms, record rooms and reinforced rooms.

3.44 TRANSMISSION SECURITY

(a) Transmission security is a part of communication security and entails the safeguarding and secure use of systems linked to one another for the sake of communication.

3.45 SECURITY COMPETENCE

(a) Persons ability to act in such a manner that he does not cause classified information or material to fall into unauthorised hands, thereby harming or endangering the security or interest of the state. It is normally measured against the following criteria: namely: susceptibility to extortion or blackmail, amenability to bribes and susceptibility to being compromised due to compromising behavior and loyalty to the state or department.

3.46 SECURITY CLEARANCE

(a) an official document that indicates the degree of security competence of a person. This document is normally issued by vetting institutions e.g. NIA, SASS, SAPS, SANDF and any other institution that has been mandated by act of parliament or other policies to do so.

CHAPTER 4

4.1 ESTABLISHMENT OF SECURITY COMPONENTS

(a) Every department shall appoint a security manager who will have to be assisted by security component .The number of persons to assist the security manager would depend on the size of the department. Meaning that each department should establish a security directorate, or sub directorate, which will permanently deal with security matters.

4.2 THE HEAD OF SECURITY AND RISK MANAGEMENT SERVICES IN THE OFFICE OF THE PREMIER

(a) The Head of Security and Risk Management Strategies in the Office of the Premier is responsible, in accordance with statutory provisions, for the functional execution of coordinating with the departments on security activities the Provincial Government.

4.3 SECURITY MANAGERS

(a) Security Managers, appointed to the departments will permanently deal with security matters within the departments.

4.4 PERSONNEL

4.4.1 Departmental Security Managers

(a) Departmental Security Managers are primarily responsible for the safety and security of their respective departments and must ensure that the security directives, that are prescribed in among others this policy, are adhered to at all times.

4.4.2 The Heads of Departments

(a) The Head of departments must ensure that all Government staff (within their particular department) are kept informed of the security measures

applicable in the Provincial Government and on the particular premises, as well as the implications of these. Should a staff member deal with classified information or material or have access to such matters, the directives set out in this policy must be brought to the attention of such a person.

4.4.3 Personnel

(a) It is the duty of each staff member to report any security risk or potential security risk, or any action or incident which may be detrimental to the interests of the department, to the Security Manager in a department, who in turn must report it to the Head of Security and Risk Management Strategies in the Office of the Premier.

4.4.4 Personnel Handling Classified Material

(a) Conversance with Manuals and Statutes. Protection of classified matters, in whatever form, is the responsibility of every official of the Government, regardless of the manner in which such knowledge of such matters was gained. It is also the responsibility of every official to be conversant with security directives.

(b) Non-divulgence. It is the responsibility of all the Government personnel not to discuss classified matters in the presence of persons not authorised to have knowledge of such matters.

(c) Safekeeping and Handling. It is the responsibility of the person in charge of classified matters to ensure that all aspects of such matters are handled and stored as prescribed.

CHAPTER 5

5.1 DOCUMENT SECURITY

(i) This part of the Provincial Government's security policy describes the way in which documents with classified contents that have their origin within the Department, as well as those with a similar status received from external sources, should be handled. Obviously, the contents and type of document, or activity, will determine if security measures should be applied and the appropriate level of such measures. The way documentation containing classified contents is handled, is one of the pillars of an encompassing corporate security profile.

5.2 CLASSIFICATION OF INFORMATION

(i) All Departments handles on their day-to-day basis information that is to some extend sensitive and obviously require security measures. The level of security grading of information of a sensitive nature is determined by the degree of sensitivity of such information. It is the responsibility of any person who is writing a document that contains information of a sensitive nature to classify it accordingly.

(ii) The classification assigned to documents shall be strictly observed and may not be changed without the consent of the author of the document or the Head of the Department where the information originates from or his delegate.

(1) If the receiver of a classified document who is of the opinion that the document concerned must be reclassified, must obtain oral or written authorization from the author, the Head of the Department or his delegate. Such an authorization must be indicated on the relevant document when it is reclassified.

(2) The classified document or file will be determined by the highest graded information it contains. The same classification as that of the original must be assigned to extracts from classified documents, unless the author or the Head of the Department consents to a lower classification.

(3) Every document must be classified on its own merit and in accordance with the origin of its contents .We must guard against the under classification, over classification or unnecessary classification of documents.

5.3 ALLOCATING CLASSIFICATION TO INFORMATION

(a) **Test:** Information must be classified as RESTRICTED when compromise thereof could hamper or cause an inconvenience to the Department or any institution dealing with the Department or individuals, but cannot hold a threat of damage. However, compromise of such information can frustrate everyday activities.

(b) The degree of sensitivity of the activity or message determines the level of the security classification allocated, and would under normal circumstances rest with the

5.4 Test: Information must be classified CONFIDENTIAL when Compromise thereof leads to:

(a) The frustration of the effective functioning of information & Operational systems:

(b) Undue damage to the integrity of a person or Department or Dealing with a Department, but not entailing a threat of a serious damage. Compromise of such information, however, can frustrate everyday functions, led to an inconvenience and bring about wasting of funds.

(C) The inhibition of systems, the periodical disruption of administration (e.g. logistical problems, delayed personnel administration, financial relapses, etc) that inconvenience the Department, but can overcome; and the orderly, routine co-operation between institutions and / or individuals being harmed or delayed, but not bringing functions to a halt.

(d) The disruption of ordered administration within the Department and adverse effect on the non-operational Relations between institutions.

5.5 Test : information must be classified as SECRET when the compromise thereof:

(a) Can result in disruption of planning and fulfilling of tasks, i.e. the objectives of a Department or institution dealing with the Department in such a way that it cannot properly fulfill its normal functions ; and

(b) Can disrupt the operations co-operations between the Departments in such a way that it threatens the functioning of one or more of the Departments .

(c) Can damage operational relations between Departments and diplomatic relations between states.

(d) Can endanger a person's life .

5.6 **TOP SECRET** is used when the compromise of information results in:

(a) The functions of the Provincial Government being brought to a halt by disciplinary measures, boycotts or mass actions;

(b) the severing of relations between states can disrupt the effective execution of information or operational planning and / or plans;

(c) can seriously damage operational relations between Governments.

(d) can lead to discontinuation of diplomatic relations between states or Governments and

(e) can result in declaration of war .

5.7 It is the responsibility of the originator of a document to allocate copy numbers to the document, including to documents distributed as drafts, to establish the distribution list of this classified information, including the principle of an "Only Copy" or attaching exclusivity, and to attach an embargo on making copies or extracts, should it be necessary. The number of copies, including the number of the particular document, should be clearly indicated on the first page in the right-hand corner, for example, Copy One of Three Copies. At the end of the message after the signature block, the distribution of these copies should be indicated, for example, Copy One (for attention) to the Director General, Copy Two (for attention) to Head of the Department and Copy Three placed on the relevant file. Should the possibility of future reclassification exist, that is, after a certain period or upon the occurrence of a particular event, it must be indicated.

5.8 Situations could arise where documents are received from other companies or the government, which already bears a security

classification. When this classification implies particular handling or limiting normal access, such documents must be handled accordingly.

5.9 ACCESS TO CLASSIFIED INFORMATION

(i) The rules and prescriptions as to who may have access to or inspect classified matters are as follows:

(a) A person who has an appropriate security clearance or who is by way of exemption authorized by the Accounting Officer of that Department or his or her delegate with due regard being paid to the need – to-know principle .

(b) The authorized person shall take prescribed oath and or declaration of secrecy .

(c) Persons who must necessarily have access to that classified information in the execution of their duties (the need to know principle) on condition that a suitable clearance has been issued or authorization has been granted , as explained above .

(d) Persons such as secretaries and personnel at smaller sections who in general do not have access to classified material and who do not have relevant security clearance, but are expected to have access to this information on an ad-hoc basis owing to the circumstances ,will have access to such information on condition that the prescribed oath / declaration of secrecy was taken .

5.10 HANDLING OF CLASSIFIED INFORMATION

5.10.1 Storage of classified documents

(a) Classified documents that are not in immediate use must be locked away in a safe storage place.

(b) The doors of all offices in which classified documents are kept must at least be fitted with security locks, and must be locked when vacated, even for a short period, by the person (s) using the room.

(c) There must be proper control over access to and effective control over movement within any building or part of a building in which classified information is handled.

(d) All classified documents that are dispatched, made available or

distributed, must be subjected to record keeping in order to ensure control thereof . This provision does not apply to documents that are classified as Restricted.

(e) Various departments may draw up interim standard registers in which the particulars of classified material are to be entered.
When classified documents are not in use, it must be stored in the following way :

- **Restricted :** Normal filing cabinet
- **Confidential:** Reinforced filing cabinets
- **Secret :** Strong room or reinforced filing cabinet
- **Top Secret:** Strong room , safe or walk-in safe

(f) The keys to any building , part of building , room , strong room , safe , cabinet or any other place where classified material is kept must be looked after with utmost care and effective key control must be instituted.

5.11 REMOVAL OF CLASSIFIED DOCUMENTS

(a) The removal of classified documents from office buildings is prohibited.

(b) Classified material (with the exception of Restricted documents) shall not be taken home without the written approval of the Accounting Officer or his delegate; a list of the documents to be removed must be taken to a person in control of record keeping. Removal of classified documents form must be completed affected copy attached.

5.12 THE TYPING OF CLASSIFIED INFORMATION

(a) Classified documents may be typed only by persons having appropriate security clearance or authority from the Accounting Officer of the Department. Such typing must be done in a manner that will ensure that the information is not divulged to unauthorised persons.

(b) Drafts of classified documents, copies and floppy disks must at all times be treated as classified documents.

5.13 MAKING PHOTOCOPIES OF CLASSIFIED DOCUMENTS

(a) All mechanical / electronic reproduction appliance should be properly controlled to prevent the unauthorised or uncontrolled copying of classified documents. The photocopy machines must be centralised and be under the direct control of an authorised and aptly cleared officer.

(b) Every Department must keep a record of all the productions of classified documents at its disposal. The register must contain the following particulars: Date, Person requesting copies / reproduction, Classification , File reference , Heading / nature of documents , Purpose of the copies , Number of copies , Meter reading before and after copying .copy attached.

(c) Written authorization for copying of secret and or top secret documents by the author , head of the Department or his delegate is required . Such authorization must be indicated on the original document .

(d) Copies of all secret and top-secret documents must receive a copy number and be registered in the same way as the original document.

5.14 SEALING OF CLASSIFIED DOCUMENTS BEFORE DISPATCH

(a) Classified documents must always be dispatched in a double envelope / cover, i.e. in an envelope placed within another (excluding “Restricted” documents)

(b) The seams of the inside envelope must be properly sealed with paper seals, counter signed and with the name of the office of origin clearly stamped on them .If paper seals are used in this purpose they must be attached with passport glue (seals that can be reused are not suitable for this purpose)
Thereafter wide translucent tape must be put on the seams, covering the seams and the stamps. The reference number of the document, name and address of the addressee and other special instructions for dealing with the documents must appear clearly on the front of the inside envelope, while the security classification of the document must be indicated clearly on the front and back of the envelope by means of rubber stamp.

5.15 DESTRUCTION OF CLASSIFIED DOCUMENTS

(a) In terms of the Archives Act, 1962, all documents received or created in the government office during the conduct of affairs of such office are subject to the Act, except where they are excluded due to their very

nature or the prescriptions of some other Act of Parliament .It should be a point of departure that all state documents is subject to the Archives Act, unless justifiably excluded along the above –mentioned lines.

(b) Where destruction has been properly authorized, it should take place by burning or some other approved method, e.g. by means of a shredder (in the latter case – preferably a cross –cut machine), in which case the strips may be no wider than 1,5 mm .The person who has destroyed the documents must give a certified of destruction of the documents concerned to the head of the Department or his delegate.

5.16 BREACHES OF SECURITY

(a) Heads of departments must report all instances of breach of security, or failure to comply with security measures, or conduct constituting security risk as soon as possible to the Security Manager in their departments who will report to the relevant authorized institutions and or the Security and Risk Management Services and other relevant external stakeholders.

(b) Breaches of security must at all times be dealt with using the highest degree of confidentiality in order to protect the officer concerned and prevent him or her from being unnecessary done an injustice to.

5.17 TRANSMITTING DOCUMENTS BY MEANS OF FACSIMILE

(a) When classified documents are transmitted by means of facsimile , only facsimile machines equipped with encryption must be used .

(b) Classified reports may only be handled by a suitably cleared or authorized operator.

(c) A record must be kept of the transmission and receipt of classified documents.

(d) After receiving a message, receipt must be acknowledged immediately. .

(e) The recipient must immediately after receipt transmit an acknowledgement of receipt to the sender.

(f) The receipt must, on his copy, note the copy number as indicated on the distribution list.

(g) Control must be exercised over “open” “open” facsimile machines to ensure that these are not used for the transmission of classified documents.

(h) Irrespective of the way information is communicated, that is, by verbal, documented or electronic means, restrictions are sometimes placed on obtaining access to it. The Government and its employees normally handle the following categories of information:

5.18 ACCESS TO INFORMATION OF A CLASSIFIED NATURE

(a) The rules and prescriptions as to who may have access to or inspect classified matters are as follows :

(b) A person who has an appropriate security clearance or who is by way of exception authorized by the Accounting Officer of that Department or his or her delegate with due regard being paid to the need – to- knows principle .

(c) The authorized person shall take prescribed oath and or declaration of secrecy.

(d) Persons who must necessarily have access to that classified information in the execution of their duties (the need to know principle) – on condition that a suitable clearance has been issued or authorization has been granted , as explained above.

(e) Persons such as secretaries and personnel at smaller sections who in general do not have access to classified material and who do not have relevant security clearance , but are expected to have access to this information on an ad-hoc basis owing to the circumstances ,will have access to such information on condition that the prescribed oath / declaration of secrecy was taken .

5.19 SECURING OF CLASSIFIED INFORMATION

5.19.1 Securing documents with classified contents.

(a) Classified documents should be secured in the most effective and appropriate way, which includes strong rooms, safes or metal cabinets fitted with a vertical security bar and equipped with a security

lock.Important in securing classified documents, is adherence to principles stating that

(b) Documents with classified contents that are not in immediate use must be locked away in a safe storage place as described above;

(c) the doors of those offices in which classified documents are kept must be fitted with at least security locks and must be locked every time they are vacated by staff occupying such rooms (even for a short period); and

(d) if staff leave their offices at the end of the working day, all material bearing a classification of *Confidential* or higher must be locked away in a safe or metal cabinet as described above. Apart from locking the office, staff must ensure that other possible entrances to the office, such as windows, are also closed.

(e) It is preferred that documents bearing a *Confidential* classification be kept in a lockable filing cabinet and depending on its contents or the state of other security measures in the building/office, the cabinet should be fitted with a vertical security bar and equipped with a security lock. Documents of a *Confidential* nature or higher classification should, at least, be kept in the same type of metal cabinet or, preferably, in a safe or strong room, depending on the contents.

(f) Should a strong room or safe which is equipped with a combination lock be used for securing documents with classified contents, the combination must be changed every six months or in the following situations:

(i) When it is suspected that it has been compromised.

(ii) f it was necessary to make the combination known to another person for whatever reason.

(iii) When a new user takes over the safe/safe.

(iv) **Remark.** A register should be used by the Security Section to manage the status of safes and strong rooms in a particular building. Provision

should be made for recording the date when combinations are changed, the location of safes and previous users. The combination of a safe or safe must be kept in a sealed envelope at the security office and its existence could also be recorded in a register.

5.20 Record-keeping of documents

(a) An important principle that must prevail when dealing with classified documents, is that a record must be kept of the way the document is handled. This must include the entire period from the time the document is received, through the process of handling by staff allowed to have access to it, until it is finally filed, archived or destroyed. Registers must be used in this process of receiving and despatching classified documents. This regulation applies to internal communication, as well as to post received from outside organisations (including state departments), or post distributed externally. Registers for receiving and despatching classified documents should make provision for the following:

(i) Incoming documentation/post: Serial number of the entry; date of receipt; from whom received; registered postal material and reference number; classification of the document; subject/ heading; disposal: file number, recipient (signature); further despatch (serial number of the entry for outgoing mail in the register); destruction (date and signature).

(ii) Outgoing correspondence (post): Serial number of the entry; date of despatch; reference number and date of the document; classification; subject/heading; despatched/addressed to; nature of despatch (courier, by hand, registered post, facsimile, by computer); registered number of postal material; signature of the recipient (courier, registration, person despatching); receipt number; date when receipt was obtained.

5.21 Registries and files

(a) With particular reference to the handling of classified information, the aim of a registry (instituted per division) is to enable total control over classified documents, including determining their temporary or permanent location. Access to registries where classified documentation is dealt with, should be strictly controlled. Only those

officials attached to the specific registry or with a line-functional responsibility (providing they have the appropriate security grading) should be allowed inside the work area. Since the classification of correspondence could only be determined once it has been opened (should it not be indicated on the envelope that contained the document) staff attached to the particular registry where all incoming mail is received should have a security clearance that corresponds with *Confidential*.

(b) Files of an official nature should be opened according to an identified need. The file reference number allocated must refer to the department's filing system and its existence should be noted in a central register that is kept in the registry dealing with classified matters. The file should bear the same classification as that of the contents and this must be indicated on the outside. Apart from a file reference number, the subject should also be indicated on the cover of the file. (Remark. Situations could exist where the matter that is being dealt with, is sensitive. In such situations the project name, if applicable, or other similar reference, should rather be used.) Files containing classified documents should be kept in secure facilities, including the office where it is kept and access to the particular office.

(b) A sequential number marked in the right-hand corner of the first page of a document (should it contain more than one page) must be allocated to every document filed in a classified file, as indexed on a page attached to the inside of the file cover, together with the name/heading of the document concerned. In situations where an official receives a classified document in person, he/she must on returning to his/her office (for instance if that document was received while he/she was out of office) send it to the registry for recording in the relevant register. The same procedure will prevail if he/she received such document under other circumstances, such as from a visitor in the office.

5.22 Central Registries for Receiving of Incoming Mail and Dispatching of outgoing Mail

(a) An effective registry is the core of effective document control and of document security. One registry in the department should be the

central/main registry where all incoming mail must be received , opened and from where it must be distributed internally . This receiving and distributing must be recorded in the relevant registers.

(b) Internal distribution should be reflected in registers for incoming and outgoing mail that should be kept at all other registries or office where internal mail are received. These registers should contain the following particulars:

(c) **Particulars of incoming post:** Serial number of the entry; Date of receipt; From whom received; Registered postal material and reference number; Classification (C/S/TS); Subject / heading ; Disposal: File number , Receipt (signature) ; Further dispatch (serial number of the entry for outgoing mail in the register) ; Destruction (date and signature).

(d) **Particulars of outgoing post:** Serial number of entry ; Date of dispatch ; Reference number and date of the document ; Classification, Subject /heading ;Dispatched /addressed to ; Nature of dispatch (courier , by hand ,registered post, facsimile, by computer); Registered number of postal material; Signature of the recipient (courier, registration, person dispatching) Recipient number ; Date when receipt was obtained.

(e) Apart from being registered , system of route cards , or similar , should be implemented to ensure that a document can be traced at any time.

(f) Outgoing mail should be forwarded to the central registry from where it will be dispatched. This forwarding and dispatching must be subject to the control measures as described in the MISS/elsewhere.

(g) **Access to Registration:** Access to registries should be controlled. No unauthorized person (any person that has no direct line functional responsibility inside the registry must be allowed inside.

(h) Management of Files: Files should be opened according to the actual need when the need arises, and not just because the filing system

provides for the existence of such a file.

(i) The particulars appearing on the file should be at least : the name / topic of the file , the file number , the classification , and who are /is authorized to have access to that file.

(j) A register should be kept of all files opened /in existence. As and when a file is opened , the particulars must be entered in the register. This register must indicate the number of volumes in existence for any given number.

(k) A file must be classified according to the highest level of classification of the documents it contains.

(l) The classification mark must be affixed on the file as described elsewhere /in the MISS.

(m) Classified files must be stored in facilities as prescribed for classified documents.

(n) All documents filed in a file must be given a serial or index number , in the sequence as it is filed , but preferably in chronological order .An index page must be fixed in the file , on which should be recorded the index/serial numbers of the documents on that file, as well as the topic /heading of each documents.

(o) A sub file must be opened for each file and kept inside the main file. It should have the same particulars as the main file. When the main file is drawn and taken out of the registry (which should not be common practice), an indication must be made on the sub file to whom the main file has been issued, and when . The sub file should remain in the registry and all documents that should be filed on the main file must be placed on this until the main file has been returned.

(p) No file must be allowed to remain outside the registry for more than one working day – all files must be returned to the registry before closure on the same working day . Exceptions can be allowed , provided that storage facilities in the relevant office are on standard (as prescribed)

and that the return of the file is followed up on a daily basis by the head of the registry.

(q) Only authorised persons may be allowed access to classified files.

R Despatching classified information:

(i) Classified information in a documented form (excluding that sent by facsimile or computer) must be sealed and handled in the prescribed way to ensure that it reaches its destination unopened. Should a classified document be distributed internally, that is, to another employee in the same division or to another division, it could occur via registries in the file dealing with the subject. Files, in particular those classified as *Confidential*, should be distributed in an envelope to prevent unnecessary interest from outsiders. Where the services of a registry clerk are used, it must be noted that the official should have a security grading that corresponds with this task on his job description. When classified documents are distributed as an independent item and where the services of a courier are used, it is important to note that a receipt must accompany all documents despatched and that this receipt must be returned to confirm arrival of the document. (Remark. Receipts are cardinal in any investigation into the disappearance or mishandling of classified information.) Despatching classified documents with the aid of a courier, occurs via the registry where the incident is recorded in the despatch register. It is preferred that the courier should convey the document(s) in a secure container that can be locked (combination-type lock). Couriers must identify themselves when they collect and deliver documents. Since couriers handle classified information, it is important that they satisfy the security clearance requirements. Classified documents, in particular *Confidential*, should preferably not be despatched externally through commercial mail channels. However, in cases where a courier or alternative form of delivery is not available, the use of commercial postal facilities are allowed under the following conditions:

(i) It must be sent by registered mail.

(ii) The addressee must be informed that he/she will receive a classified

document by registered mail and must be requested to inform the sender's registry immediately when this document is received.

(iii) The head of the department (or delegate) must have given his/her express permission.

(iv) The circumstances or reason for this decision, approval by the Government official concerned and confirmation from the relevant registry official that there was no alternative, must appear on the file copy of the document that was sent.

S Sealing of classified documents before despatch.

(i) Classified documents must always be despatched in a double envelope/cover, that is, in an envelope placed within another. In the case of the inner envelope the seams must be properly sealed with paper seals, counter-signed and the name of the division clearly stamped on them. (Remark. If paper seals are used for this purpose, they must be attached with passport glue. Seals that can be re-used are not suitable for this purpose.) Wide translucent tape must be put on the seams, covering the seals and the stamps. The reference number of the document, name and address of the addressee and other special instructions for dealing with the document must appear clearly on the front of the inside envelope.

T Transmitting documents by means of facsimile:

(i) When it is necessary to transmit documents containing classified contents by means of facsimile, it is preferred that only facsimile machines equipped with encryption are used. In this regard the classified information may only be handled by staff who have a corresponding security grading, or by a member who was given authority to do so by the head of the department. Record must be kept of the transmission and receipt of all classified information sent or received through facsimile. It is also important to note that the room in which the facsimile(s) is kept, must be manned at all times or locked when not in use. The recipient or the communication centre of the recipient, upon receiving the document, must ensure that it has been received clearly, accurately and in full. Thereafter, acknowledgement

of receipt must immediately be transmitted to the sender, who must note the successful transmission on his copy of the document.

U Effective control must be exercised over those facsimile machines not equipped with encryption to ensure that these are not used for the transmission of classified information. However, situations could arise where the contents of classified documents must be sent over facsimiles, which are not equipped with encryption. This should be the exception rather than the rule and the following guidelines are given to maintain an acceptable standard of information security:

(i) Where *Confidential or higher classified* documents are transmitted, the head of the department (or delegate) should give his/her approval for this step.The approval must be indicated on the original copy.

(ii) The recipient should be notified and, where possible, wait at the receiving facsimile to receive the document and confirm it with the sender.

(iii) The fact that the particular document was sent over an open facsimile must be indicated clearly on the original copy, including the particulars of the facsimiles involved.

V Transmitting documents by computer:

(i) it is preferred that classified information sent through computerised transmission is encrypted in some or other way. A record must be kept of the classified information transmitted and received. The recipient of information having classified contents should always acknowledge receipt thereof. All magnetic media should be regarded as documents and handled as such. Classified information generated through a computer must also be supplied with copy numbers.

W Making photocopies of classified documentation:

(i) Photocopying classified documentation is generally also a major problem and a security risk in any environment where information of a classified nature is handled. *The following minimum requirements*

apply:

(ii) Photocopying of classified documents should only be allowed after approval for such copy has been obtained from the staff member entitled to give such , as officially appointed by the particular head of the department.

(iii) Photocopiers should be properly controlled to prevent the unauthorised or uncontrolled copying of classified documents. This apparatus must preferably be centralised and under the direct control of an authorised staff member with the appropriate security grading. A central record of all reproductions of classified documents made in a particular division must be kept. For this purpose a register is suggested which should be available at the photocopier, making provision for the date, person requesting copies/reproduction, classification, file reference, heading/nature of documents, purpose of the copies, number of copies, meter reading before and after copying. It is preferable that the staff member in charge of the reproduction apparatus, or an assistant entitled to do so and who has the appropriate security grading, makes these copies.

(iii) In situations where copies of classified documents received from another originating authority that is part of the Government are required, written authorisation for the copying of these documents must be obtained from the author or head of the particular division or his/her delegate(s) before copying and indicated as such on the original and the document received. (Remark. Authorisation could occur via facsimile and the approval should be filed with the particular document.) In situations where classified documents are received from institutions other than the Government, it is preferred that the same procedure be followed. However, practical considerations will normally prescribe the method to be followed and it is suggested that a clear record be kept (as mentioned earlier or written on the document concerned) of copies made and then on the principle that the head of the department (or delegate) must give authorisation for such duplication.

(iv) Apart from recording the existence of copies in a register kept at every department, (as referred to in paragraph @@), a rubber stamp should be used for marking the original or file copy on the back, where the

number of copies and distribution are indicated.

(v) Copies of all classified documents must be assigned a copy number and be registered in the same way as the original document. The number of copies of such documents must be restricted to a minimum, and copies of appendices and addenda must be numbered in accordance with the relevant classified document. All departments or individuals who received copies and the corresponding copy numbers must be recorded in the particular file (if applicable) or noted on the original used for copying. Alternatively, a distribution list can be attached to all copies of the document concerned, indicating the addressees and the applicable copy number. The distribution list should be filed with the copy or on the particular file (concerning the subject) and there should be a reference to the exact location of this list on the copy.

X Removal of classified documents from premises

(i) As a principle for sound information security, no classified information (in particular that classified as *Confidential or higher*, including electronic media containing such information) may be removed from the department where it has its origin for reasons other than despatch, unless it is absolutely essential. If required, the staff member wishing to remove such information must obtain written permission beforehand from the employee or alternate appointed by the department's head (indicated on the persons' job descriptions) who have the authority to grant such permission. (Remark. The head of the department could determine, prescribe and then authorise the particular manager(s) and the particular types of information, including the level of sensitivity.) The written permission, of which a copy will be placed on record for future inspection (auditing) by the Security and Risk Management Services, must include:

(1) identifying particulars of the document(s)/electronic media to be removed (file reference, date, subject/description, copy number and security classification);

(2) the personnel or ID number, and name of the staff member removing

the information;

(3) the reason for removing the document(s) from the premises;

(4) the place/address where the information is taken to or is to be kept;

(5) the date on which the information is to be returned; and

(6) the signature of the staff member removing the documents, which shall be regarded as proof that the person removing the information accepts full and personal responsibility for safeguarding the relevant information, that is, ensuring that its contents are not disclosed to unauthorised persons, organisations or institutions while in his/her possession.

(7) information may not be taken home without the written approval of the staff member's manager or his/her delegate (as appointed by the department's head). A list of the information to be removed must be put on record in a system designed for this purpose. Staff may take classified information home only if they have proper lock-up facilities. The manager who gives the approval for removing classified information must ensure that it is returned on the date specified. If the classified information concerned is not returned by the determined date, the issue shall be considered to constitute a breach of security and must be reported to Security and Risk Management Services. It is suggested that no standing authority be granted to remove classified information from the department's offices.

(8) It sometimes happens that a visitor or a person temporarily assigned to departments needs to remove classified information. In such situations the procedure of written permission must prevail.

(9) It is suggested that classified information taken out of the building with a view to using this at meetings or appointments, must be removed in a lockable security attaché case.

V Destruction of classified documents

(i) Classified information (documentation) which is not needed any more, for instance drafts, or which has become redundant, must be destroyed properly by means of a shredder. It is preferred that the originator of the (classified) document, or the staff member who has used this information, depending on its sensitivity, destroys it him/herself. The process of destruction must be such that reconstitution of the documents destroyed is impossible. Electronic media on diskettes could be destroyed through incinerating or rewriting over the existing data, using a particular program for that purpose, allowing unintelligible characters to write over the data, or through introducing the contents of the diskette to a magnetic field which will erase the contents. Depending on the level of sensitivity of drafts, control must also be exercised over their destruction. It is important to note that a regulation exists which stipulates that a declaration (destruction certificate) must be made out (in writing) when original official classified documents are destroyed and that the originator must be informed of this.

(1) No waste of any nature containing classified material may be discarded in waste-paper baskets or similar containers that cannot be locked away in a secured manner.

(2) **Remark.** If the necessary precautions are not instituted, access to waste-paper baskets is probably one of the easiest ways for unauthorised persons to obtain classified information. Special attention should therefore be given by all those concerned to the disposal of drafts, notes, or any other medium used that may contain classified information.

Z Meetings

(i) When the intention is that documents that contain classified information are to be removed from the division to a venue where a meeting will take place, the particular staff member must ensure that prior to the distribution of the classified information at the meeting,

(ii) the recipients of the documents are in possession of the appropriate security grading, that is, that the outcome of the particular person's integrity assessment corresponds with the sensitivity of the information to be distributed, or that the recipient obtained approval beforehand from executive level to do so;

(iii) the recipients of the documents have a secure means of carrying and transporting the information to their offices;

(iv) the information concerned has been recorded in the register for outgoing documents; and

(v) each recipient is issued with a letter of authority, permitting him/her to remove the documents from the division after he/she has signed for receiving them.

Aa Security inspection of files containing classified documents and registers referring to the position of such information.

(i) To ensure that documents containing classified information in possession of the department are dealt with in the prescribed manner, the Security and Risk Management Strategies must on an annual regular basis undertake information security inspections (audits) of all official corporate files containing classified documents. Inspection of all registers used by the divisions for recording the receipt and despatch of classified information, as well as records of photocopies made and facsimiles sent, or records kept on the movement of classified information such as removal of classified documents from any Government premises, must be carried out.

Bb Handling of classified information in emergency situations

(i) **T**he contingency plan of a division must provide for the destruction, storage and/or moving of classified information in the event of an emergency, in order to prevent the risk of being compromised.

Cc Loss of classified information

(i) Should classified documents be lost or mislaid, this must immediately be reported in writing to the Security and Risk Management Services . An investigation in consultation with the head of department whose department the incident occurred must be instituted and appropriate, corrective steps taken. Such corrective steps must include

(ii) measures to prevent any recurrence of the incident;

(iii) implementing measures that can support efforts instituted to minimise any negative impact that compromising of that particular information could have on the activities of the corporation;

(iv) informing the parties concerned, that is, those divisions affected by the loss or potential loss of the classified information; and

(v) disciplinary steps against the person(s) responsible for the loss, if deemed necessary.

CHAPTER 6

PERSONNEL SECURITY

6.1 SECURITY CLEARANCE LEVELS

(a) Personnel security entails the allocation of a security clearance to a person after a process of security vetting has been followed, and maintaining this level of security conscientiousness. The level of security clearance considered is determined by the content of and/or access to classified information the person is required to deal with in the post he/she already occupies/is to occupy. It will thus give such a person access to classified information in accordance with the level of his security clearance, subject to the need-to-know principle. Since a security clearance is coupled to a particular post (that is, as determined by the security requirements attached to the particular position), a security clearance issued to a person is merely an indication of the limitations under consideration when employing an individual in terms of classified matters, and does not confer any rights on such a person. Security clearances are applicable to all employees handing sensitive information, functioning in strategic positions where information can easily be leaked or prospective employees of the Provincial Government.

6.2 SECURITY VETTING PROCESS

(a) The process of considering security-vetting process (requesting such an action, managing it in terms of the requirements with the institution executing the request (National Intelligence Agency) and finally processing the outcome) is the responsibility of the head of the department. Each department, in consultation with the Security and Risk Management Services or Security section, determines the security requirements of each post in the Provincial Government, including the frequency for revising the particular level of security clearance required. Appointment of Provincial Government personnel functioning in strategic positions shall occur, , according to this requirement and the Security and Risk Management Strategies has the responsibility to process this action. After receiving the recommendation made by the

institution conducting the security vetting on the security competence of the particular employee and in consultation with the Head (or his delegate) Security and Security and Risk Management Strategies, the Head of the department (of the applicant or serving staff member) takes a decision on the acceptability or otherwise of the individual to have insight into classified matters of the Provincial Government. After taking the decision, the said Head of the department requests the Security and Risk Management Strategies to issue a letter indicating the individual's proof of security competence.

(b) Consultants and contractors performing tasks for the Provincial Government are subjected to the same security vetting process, should they be involved with classified matters of the Government. The onus rest with the Provincial Government to indicate expressly in tenders or documents serving the same purpose whether any security requirements or implications are attached to the assignment concerned, including the issue of a required security vetting. A clause to ensure the maintenance of security during the performance of the contract could read as follows:

(c) "Acceptance of this tender is subject to the condition that both the contracting firm and its personnel providing the service must receive a particular level of security clearance which results from a process of security vetting as determined by the Provincial Government. If the principal contractor appoints a subcontractor, the same provisions and measures will apply to the subcontractor."

(d) Acceptance of a 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. The security requirements of the contractor will be determined by the Head of the particular department requiring the services of the consultant, or contractor.

6.3 RESPONSIBILITIES OF THE HEADS OF DEPARTMENTS

(a) Notwithstanding a negative recommendation from the institution conducting the security vetting, for whatever reason, the Head of the department requesting the particular security clearance may still, after consideration and consultation with the Director General and the Head

of Security and Risk Management Services, and with the acceptance of full responsibility, use the person concerned in a post where he/she has access to classified matters if he/she is of the opinion that the use of the person is essential in the interest of the Provincial Government, on the understanding that a person satisfying the security clearance requirements is not available.

(b) It is also the responsibility of all Heads of departments to ensure that there is continuous supervision of persons in respect of whom security clearance have been issued;

(c) ensure that security awareness programmes are presented for their personnel and to warn staff members not to supply any classified information or information of a classified nature to unauthorised persons;

(d) ensure that persons dealing with classified matters sign the prescribed oath of secrecy **(see Annexure A);**

(e) pertinently bring to the attention of the officials working with classified matters any other legislation, regulations and/or orders that entail secrecy and/or the protection of activities, installations, etc, of any particular institution;

(f) point out to employees dealing with classified matters when they resign or leave the service of the corporation that they will continue to be the target of foreign hostile intelligence agencies and that they remain subject to the oath of secrecy;

(g) ensure that all classified documents in possession of the person concerned are returned when such a person resigns or leaves the Provincial Government; and

(h) ensure that no classified information comes into the possession of an individual that is not essential for the performance of his or her duties.

CHAPTER 7

7.1 INFORMATION TECHNOLOGY SYSTEM (ITS) SECURITY

(a) **Remark**.It is suggested that the *Provincial Government IT Information Security Policy* be developed to cover TS security issues.

7.2 PRINCIPLES FOR ITS

(a) The following fundamental ITS security management principles apply to the IT environment in the Provincial Government:

7.3 Individual accountability

(a) All personnel who use/access/perform any function on or manages any part of the Provincial Government ITS are responsible and accountable for following appropriate recommended procedures and for taking all possible steps to safeguard the information handled by that system and any sensitive assets involved. All ITS shall provide means by which individual users can be uniquely identified and held individually accountable for their actions, in respect of which the system must provide for appropriate records.

7.4 Confidentiality

(a) All users of Provincial Government ITS are responsible, within the span of their control, to ensure that no actions are taken which could degrade or compromise the confidentiality levels of the programmes, services and information handled by the system.

7.5 Integrity

(a) All users of the Provincial Government ITS are responsible, within the span of their control, to ensure that no actions are taken which could degrade or compromise the required level of accuracy, completeness and dependability of the programmes, services and information being

handled by the information system or its assets.

7.6 Availability

(a) All users of the Provincial Government ITS are responsible, within the span of their control, to ensure that no actions are taken which could degrade or compromise the required level of responsiveness of programmes, services and information being provided by the information system to support the stated operational or managerial requirements.

7.7 Controlled Access

(a) An employee of the Provincial Government or any system component shall be granted access to only that classified level of information and assets for which appropriate access authorisation(s) and the need to know have been approved. A person or any system component shall be granted access to only those ITS resources necessary to perform the assigned task(s) and only when such access will not lead to a breach of this or any other security principle. Further to the above, appropriate segregation of duties, specifically allocated and defined in writing, shall apply. Controlled access will be achieved via physical and procedural means. Unique identification of the user to the system must be provided. An access authorisation structure shall determine access and privileges, grant such access and privileges and record, control and monitor these.

7.8 Levels of Protection

(a) The protection applied to an information system must be commensurate with the sensitivity levels of the information and assets involved and must take into consideration the identified threats to and vulnerabilities of the information system.

7.9 THREATS AND RISK ASSESSMENT

(a) Risks or threats that ITS are exposed to must be identified, analysed, evaluated and quantified in terms of the probability of them occurring and the potential impact of such an event on the Provincial Government and its activities. A documented security plan should exist to manage risk situations, which should be revised on a regular basis.

7.10 DISASTER RECOVERY PLAN

(a) An approved disaster recovery plan and procedure should exist to minimise the impact of any type of disaster on the Provincial Government's ITS. Since these plan details weaknesses of the corporation, it should be classified as Top Secret and handled on a need-to-know basis.

7.11 BREACHES OF SECURITY

(a) Users of the Provincial Government's ITS must report any observed or suspected action/ security weaknesses in, or threats to, systems or services to the IT section. In turn, this section shall inform the Security and Risk Management Services and the National Intelligence Agency of the incident or suspicion in order to effect coordination of the security effort(s) designed to prevent the reoccurrence of similar events.

7.12 SECURITY EDUCATION

(a) The Provincial Government officials who have access to ITS should be subjected to a programme of effective and appropriate security education to foster their security awareness on risks and the approved ITS principles. Staff members should be reminded regularly of their responsibilities and accountability to maintain high ITS security standards.

7.13 SYSTEM ACCESS CONTROL AND PASSWORD SECURITY

(a) Access to computer systems shall be controlled by means of an approved computer access control system which identifies the authorised user and verifies his/her identity. Where applicable, discretionary access control for the protection of files or programs

specifying who may gain access to these, shall also be used. The same applies to database access.

(b) The access control system shall update an audit trail of all authorised and unauthorised efforts to gain access to the Provincial Government's computer systems. Unauthorised access attempts shall be considered a breach of security.

(c) Passwords shall be individual and exclusive, and shall not be disclosed without authorisation in forced exceptional cases, and without documenting the incident. Unauthorised disclosure of passwords shall be considered a breach of security.

7.14 WORKSTATION SECURITY

(a) Workstations shall be located in a physically protected environment where access control measures have been instituted and are applied consistently. Unattended equipment must have appropriate security protection.

(b) All portable computers (e.g. Notebooks, Palmtops, etc) containing and/or communicating classified information shall be equipped with an access control and encryption capability that meets accepted security standards. Portable computers should not be linked to modems or equipped with facsimile cards without approval of the ITS Manager. Where permission is given, a record must be kept of the particular portable computer and its usage.

(c) Access to stand-alone microcomputers and computerised telecommunications equipment on which classified data is processed, must be controlled and limited by means of approved access control software.

7.15 PHYSICAL SECURITY CONSIDERATIONS

(a) Areas where computer-related equipment are accommodated, or office areas where classified information is dealt with using ITS, shall be protected in such a way that unauthorised access is prevented. Access control systems and procedures should regulate, record and monitor

movement in these areas. Depending on the sensitivity, the need-to-know principle should apply for access and identified vulnerable points (data, personnel, equipment and buildings) shall be protected against any type of external or internal security threat. Where applicable, security areas shall also be located and protected in such a way that the effect of negative environmental conditions, natural disasters, radiation and emission is minimised and eliminated as far as possible.

7.16 UTILISATION OF PRIVATE MICROCOMPUTERS

(a) When private microcomputers are used, written approval must be obtained from the relevant authority IT section to use a private computer for official purposes. A computer register must be established containing full personal particulars of the person, as well as details of the computer, such as make, serial number and software used, and reason for this step. Classified information bearing a sensitivity of *Confidential or higher* shall not be stored on a private microcomputer.

CHAPTER 8

8.1 COMMUNICATION SECURITY

(a) To ensure a safe environment in which information of a classified nature could be communicated (electronically or verbally), the following guidelines are supplied:

8.2 SECURITY OF DATA TRANSMISSIONS

(a) All data transmissions should be in accordance with prescribed standards for the purposes of ensuring confidentiality, authentication, integrity and non-repudiation. Communications (including Electronic Data Interchange and E-mail) pertaining to classified information should be encrypted in accordance with the Provincial Government approved cryptographic devices.

8.3 MODEMS/DAIL-UP COMPUTER COMMUNICATIONS

(a) No modems shall be connected to communication networks without authorisation from the ITS and Security and Risk Management Services. Authorisation shall only be given on receipt of a detailed motivation approved by the particular employee's Head of department, requesting such a facility and a security plan detailing the manner in which the use of the modem and classified information transmitted through this modem will be regulated and controlled. A single point of entry where access can be controlled and properly managed must exist. When approval is given to the Provincial Government contractors for modem/ dail - up connection, the above security measures shall apply, as well as security vetting criteria.

8.4 TELEPHONE SYSTEMS AND FACSIMILE TRANSMISSIONS

(a) No classified information should be discussed on ordinary telephones, cordless or cellular telephones unless approved by the Provincial Government and encryption devices are used. No messages should

be left on answering machines or voicemail systems which constitute a risk to information security. Classified information shall only be transmitted by facsimile when approved encryption devices are installed on the network.

8.5 INTERNET CONNECTIONS

(a) The air wall concept, that is, stand-alone computers with modems, or linked to any other system with appropriate firewalling, should apply to all Internet connections. Applications shall be subject to approval by the ITS Section and Security and Risk Management Strategies. No classified information may be communicated via the Internet.

8.6 INTRANET CONNECTIONS

(a) Intranet connections shall be subject to the same security measures as those applied in the ITS environment. Contractors needing access to the Intranet shall obtain such access only after approval by the ITS and Security and Risk Management Services and be subject to this security policy, directives and procedures regulating the use of Provincial Government's Intranet. No classified information shall be communicated over the Intranet unless protected by the approved cryptographic devices.

8.7 ELECTRONIC MAIL (E-MAIL)

(a) Classified information shall not be transmitted via E-mail unless authorised by the particular Head of the department or security official authorised to grant such approval. Only communication systems equipped with the approved encryption devices may be used for transmitting classified information.

8.8 PERSONAL COMMUNICATIONS

(a) Personal communication of a sensitive or classified nature must necessarily be subject to strict self-discipline on the part of the communicator. In this regard the following guidelines apply:

(b) The need-to-know principle should be observed.

(c) Such conversations should take place in such a way that sensitive information does not come into the possession of unauthorised persons or persons who happen to overhear what are said.

8.9 OFFICES USED FOR DISCUSSING CLASSIFIED MATTERS

(a) Places such as offices, conference rooms etc, where sensitive or classified matters are discussed regularly, should be subject to:

(b) proper and effective access control (e.g. visitors, outside maintenance personnel and cleaners) and; regular electronic surveillance counter-measures (sweeping) and maintenance of the area as a secure environment (after sweeping) through the constant application of access control and lock and key security.

8.10 RESENCE OF CELLULAR PHONES DURING MEETINGS.

(a) Because a cellular telephone is fitted with a microphone and a transmission capability, which may be exploited for the unauthorised transmission of classified information, the chairperson of a meeting (both formal and informal meetings) where classified matters are discussed, shall ensure that there are no cellular phones in the conference room, office, etc, where such meetings are held - regardless of whether the cellular phone is switched on or off.

CHAPTER 9

ACCESS CONTROL

9.1 PRINCIPLES FOR REGULATING ACCESS CONTROL

(a) A system of security measures is essential to create an optimal information security environment. Such a system is naturally only as efficient as its weakest link/element. In this regard, access control and movement control are the links or elements that are prerequisites for an effective security system.

(b) Because of its sensitive and contentious nature access control must be applied by officials who have been authorised and trained for the purpose in accordance with statutory requirements.

(c) Access control is multidimensional. Different levels or varying intensity must be developed and applied according to the degree of safeguarding required. Factors such as the sensitivity of information handled and the extent of zoning (placement and isolation of certain sections) that exist or that could be applied play a role in determining these levels.

(d) The different levels/degrees of access control can vary from the mere locking of offices, with the accompanying restriction on access (where effective key control will inevitably play a vital role) to large-scale access control to a building or part of a building where security officials identify, control and conditionally allow visitors access.

(e) The Security Manager is responsible for the enforcement of the provisions of the *Control of Access to Public Premises and Vehicles Act*, *1985* (Act 53 of 1985) for the purpose of safeguarding the Provincial Government buildings and premises. The Director General and Heads of departments shall support the Chairman of the Security Operating Committee in carrying out this responsibility by, inter alia, ensuring controlled access to areas where classified information is concentrated (such as registries, computer rooms), or where discussions of a sensitive nature normally take place.

(f) Effective access control should be applied to areas where photocopiers, printers, facsimile machines, etc are used. This equipment should also be under constant supervision to ensure that no unauthorised transmission of classified documents takes place, or unauthorised copies are made.

(g) To maintain effective access control it is essential that visitors are subject to prior identification, that visitors' cards are issued, that temporary permits are provided, that visitors are accompanied, that employees are issued with identity cards and that control over related documents and registers is exercised.

(h) Access to any controlled building, part of a building or room where classified information is handled/stored outside normal office hours should be prohibited to all persons who do not work there. Repairs to and the cleaning of such premises must take place in the presence **and under the supervision** of the persons who work there. Persons who have to gain access to a controlled area after hours must be duly authorised accordingly by the Head of the department or his/her delegate. The Head of Security and Risk Management Strategies (or the person authorised in this regard) must take appropriate steps to arrange access and record keeping.

(i) Heads of departments shall ensure that all personnel under their supervision leaving the service of the Provincial Government return their access control cards. In addition, they shall institute measures to prevent the possible misuse of the cards.

(h) Every employee of the Provincial Government shall immediately report the loss of his/her access control card to his/her Head of the department (or delegate) and to the Manager Security , who will immediately ensure that the particular access card is disabled from the entire access control system (where applicable).

9.2 KEY CONTROL AND COMBINATION LOCKS

(a) The keys to any building, part of a building, room, strongroom, safe, cabinet or any other place where classified information is kept must be looked after with the utmost care and effective key control must be

instituted. The keeping of the necessary key registers and the safe custody of duplicate keys and control over such keys must be strictly adhered to. Keys to safes and strong rooms must be kept in safe custody.

9.3 Changing of lock combinations

(a) If a strongroom or safe is fitted with a combination lock, the combination must, apart from being reset when it is purchased, **be changed at least once every three months**, or on the following occasions:

(b) When it is suspected that it has been compromised.

(c) On resumption of duty after a continuous period of absence, whether on vacation leave or for official reasons, if the combination had necessarily to be made known to some other person for use during the period concerned.

(d) When a new user takes over.

9.4 Compromising of lock combinations

(a) Combinations may be compromised by

(i) unauthorised persons noting the combination through observation when the lock is opened;

(ii) failure to set the combination in accordance with the manufacturer's specifications; or

(iii) failure to change the combination after a reasonable period.

9.5 Reset of lock combinations

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

(b) The figures making up a specific combination should not be used more than once in succession, even if they are in a different order.

(c) Avoid the use of numbers with some personal significance, e.g. age, date of birth, telephone numbers, street addresses and numbers of safes, etc. Also avoid the figures zero (0), five (5), ten (10) and multiples of the last two. High and low numbers should preferably be used alternately, e.g. 68-13-57-11.

(d) Only the user may set a combination lock.

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

(f) After the combination has been reset, the new combination must be handed to the Security Manager of the department or his/her representative.

9.6 Control over duplicate keys

(a) Effective key control, including control over duplicate keys, must be accompanied by the keeping of effective records in order to ensure that the keys to a building on any premises of the Provincial Government and safes or strong rooms or other safe storage places in which classified information is kept are dealt with in a safe manner. Where storage places are equipped with combination locks, the combinations must be used, kept and changed in accordance with the prescribed procedures as described above.

CHAPTER 10

10.1 PROJECT SECURITY

(a) Project security involves the application of a comprehensive spectrum of security measures in order to ensure that the required level of security is maintained throughout the life cycle of a programme, such as a strategic planning process or a particular phase of the planning process, or a project originating from a planning process. The extent

and level of security measures applied will depend on the vulnerability of the result of the planning process or project, particularly in compromising its existence (normally applicable up to a certain phase of the planning process or project) or the contents of the information.

10.2 RESPONSIBILITY FOR SECURITY

(a) The appointed programme manager is ultimately responsible for the security of his/her project. Project security is an integral part of project management and must address.

(b) information security, that is, verbal and electronic communication mediums, as well as document-handling procedures;

(c) personal security and security awareness;

(d) personnel security; and

(e) physical security;

(f) The prescribed level of security is normally determined by the nature and sensitivity of the project. Project security is therefore a prerequisite for the successful execution of a classified project.

10.3 SECURITY PLANNING

(a) The purpose of security planning is to identify risks against the programme/ project and to implement the necessary security measures and guidelines to minimise these risks throughout the life cycle of the programme/project.

10.4 PROJECT SECURITY PRINCIPLES

(a) The lowest possible security classification must be allocated to a project. A breakdown of the project to component level with relevant security classifications is preferable. Security classifications per component must be revised continuously and consequently also the execution of the design. Depending on the level of sensitivity of the project, a record of involvement or knowledge of the project's contents

must be kept from the first time a decision is taken to commence with the project.

10.5 Employee knowledge reviews.

(a) Information security is the responsibility of every employee. Compliance with the Information Security Policy is of vital importance to the Government and its employees.

(b) The policy's prime focus is the protection of classified information of the Provincial Government against unauthorized disclosure.

(c) Every employee shall take reasonable care of information security.

(d) Every employee shall demonstrate his / her ability to follow the appropriate information security precautions through a formal information protection knowledge review.

(e) Information security knowledge reviews will be conducted on a regular basis within the department by the Security and Risk Management Services.

(f) This is applied mainly to check whether the awareness campaign conducted within the department is making any impact towards making employees more vigilant against unauthorized disclosure of information.

CHAPTER 11

SECURITY BREACHES

11.1 RESPONSIBILITY FOR REPORTING BREACHES OF SECURITY

(a) Heads of departments must report all instances of a breach of security, or failure to comply with security measures, or conduct constituting a security risk, as soon as possible to the Security and Risk Management Services. The heads of departments mentioned will in consultation with each other determine future action, including the institution of preventive measures such as amending or suspending the relevant employee's access and privileges in accordancewith the gravity of the actions/omissions/negligence/circumstances concerned.

(b) Breaches of security must at all times be dealt with using the highest degree of confidentiality in order to protect the official(s) concerned and prevent him or her from unnecessary injustice.

11.2 REPORTING OF ASPECTS WHICH MAY INFLUENCE A PERSON'S SECURITY COMPETENCE

(a) Heads of the departments must ensure that all aspects or incidents which may adversely influence the security competence of an employee or any other person executing duties in the Provincial Government are communicated to the Security and Risk Management Strategies, regardless of the security clearance level of the person involved. The following aspects, which may have an influence on a person's security competence, must be reported:

(b) Any action, negligence or behaviour that exposes classified information, plans, human resources, infrastructure, installations or equipment to any exploitation that may be detrimental to the security of the Provincial Government.

(c) Radicalism that manifests itself in fanatical behaviour, acts of violence or terror, murder, intimidation or intimidating behaviour.

(d) Addiction to alcohol, drugs, medicine or other addictive substances (including dagga but excluding tobacco).

(e) The frequent use of addictive substances, drugs or medicines (including dagga but excluding tobacco) indicative of a continued pattern of usage.

(f) Involvement in dealing with or the supply of illegal drugs (including dagga).

(g) A continued pattern of serious alcohol abuse

(h) Multiple relapses after treatment for alcohol abuse, drug abuse (including dagga) or the abuse of other addictive substances (excluding tobacco).

(i) Financial difficulties leading to multiple summonses for debt, the administration of his/her estate, sequestration or the repeated borrowing of money and failure to repay creditors.

(j) Repeated lapses into financial difficulties indicative of a person's inability to manage his/her personal finances.

(k) Illegal enrichment.

(l) Any civil offence (excluding traffic violations).

(m) It must be emphasised that the above-mentioned aspects judged individually, in combination with one another or in combination with other aspects, may have an influence or bearing on a person's security competence.

(n) All reports relating to breach of security or failure to comply with security measures, or conduct constituting a security risk should be conveyed to NIA and appropriate to the SAPS or SADF or SACSA, depending on the type of the breach.

(o) NB. All Counterintelligence (CI) information should be channelled to NIA because NIA is the only department currently has been mandated by an Act of Parliament to take responsibility on CI matters nationally. NIA has the responsibility on a national level to collect and analyse the data and produce threat assessments in a coordinated manner.

CONTROL REGISTER FOR THE COPYING OF CLASSIFIED DOCUMENTS.

DATE……..

DOCUMENT RECEIVED FROM(NAME)……
AUTHORITY ISSUED BY(Full Names)……
AUTHORITY DATE…….

DEPARTMENT…….

DIVISION…….

No of Pages	**Metre Start (Machine)**	**Metre End (Machine)**	**Description**	**Classification R/C/S/TS/**

Signature of Controlling officer……..

DECLARATION OF PROTECTION OF CLASSIFIED INFORMATION

I,……
Declare that,

- I have taken note of the provisions of the protection of information Act(Act 84 of 1982) and in particular of the provision of section 4 of the Act;

  I understand that I shall be guilty of an offence if I reveal any information which I have at my disposal by virtue of my office and concerning which I know or should reasonable know that the security or other interest of thr Republic require that it be kept secret from any person other than a person

  - to whom I may lawfully reveal it:or
  - to whom it is my duty to reveal it in the interest of the Republic; or
  - to whom I am authorised by the Head of the Department or by an officer authorised by him to reveal it;

  I understand that the said provisions and instructions shall apply not only during my term of office but also after the termination of my services with the Department;and I am fully aware of the serious consequensces that may follow any breach or contravention of the said provisions and instructions.

Signature:……
Witness 1 Place:……
2 Date:…….