MINIMUM

INFORMATION SECURITY

STANDARDS

CABINET APPROVAL

On 4 December 1996 Cabinet approved the Minimum Information Security Standards document as national information security policy

PREFACE

The world and especially South Africa has changed dramatically during the last few years, with profound implications for our society, our government, the South African Police Service, the Defence and Intelligence Communities. Our understanding of the range of issues that impact on national security is evolving. Economic and environmental issues are of increasing concern and compete with traditional political and military issues for resources and attention.

The Republic of South Africa has to serve and protect its own interests just like every other sovereign state in the modern world. The National Intelligence Agency (NIA) has a statutory responsibility to protect the interests of the State through counter-intelligence measures. (National Strategic Intelligence Act 39 of 1994) Counter-intelligence embodies two distinctive dimensions, namely security (the defensive) and counter espionage (the offensive dimension).

With these imperatives in mind, NIA in conjunction with the other members of the intelligence community have focused their attention on the process used to formulate and implement information security policies on a national basis. The processes being used to formulate policies and deliver information security services must be sufficiently flexible to facilitate change.

* Our need for secrecy and therefore information security measures in a democratic and open society with transparency in its governmental administration according to the policy proposals regarding the intended Open Democracy Act have been taken into account.

* Our security standards and procedures must result in the fair and equitable treatment of those upon whom we rely to guard the nation's security. (Interim Constitution have been taken into account).

* Our security policies must realistically match the threats against the country and its people.

* Our security policies, practices, and procedures must provide the needed information security in a cost effictive way that will benefit the socio- economic development of the country.

With these aspects in mind the Minimum Information Security Standard (MISS) was compiled as an official government policy document on information security, which must be maintained by all institutions who handle sensitive/ classified material of the Republic. This will ensure that the national interests are protected.

Any comments or recommendations in respect of this policy must please be forwarded in writing to the Chairperson of the Functional Security Committee of NICOC.

All amendments to this policy will be issued by the National Intelligence Agency being the department nationally responsible for counter-intelligence. Government departments, institutions, parastatals and private companies will be responsible for the distribution of such amendments within their own organisations.

T A B L E O F C O N T E N T S

CHAPTER 1

INTRODUCTION

1. The need for secrecy and therefore security measures in a democratic and open society, with transparency in its governmental administration, is currently the subject of much debate, and will continue to be for a long time.

2. However, the issue need not be controversial, since the intended Open Democracy Act (not yet promulgated at the time of going to press) itself will acknowledge the need for protection of sensitive information, and therefore, will provide for justified exemption from disclosure of such information.

3. Although exemptions will have to be restricted to the minimum (according to the policy proposals regarding the intended Open Democracy Act), that category of information which will be exempted, as such needs protection. The mere fact that information is exempted from disclosure in terms of the Open Democracy Act, does not provide it with sufficient protection. Such information will always be much sought after by certain interest groups or even individuals, with sufficient access to espionage expertise, and highly sophisticated technological backing. The extent of espionage against the new South Africa should never be under estimated - it has actually escalated alarmingly during the past few years.

4. Where information is exempted from disclosure, it implies that security measures will apply in full. This document is aimed at exactly that need: providing the necessary procedures and measures to protect **such** information. It is clear that security procedures do not concern **all** information and are therefore not contrary to transparency, but indeed necessary for responsible governance.

5. The procedures and measures taken up in this volume are based on general security principles. It should, however, be remembered that in drawing up security directives it was not possible for the National Intelligence Agency (NIA) to take into account the particular circumstances and operations of each of the institutions where classified information is handled. Institutions should therefore compile their own rules of procedure to fit their own circumstances and operations. In the development of an own effective information

security system, institutions should use this volume as a minimum standard on which to base it.

6. As stated above, this document lays down a minimum standard for the handling of classified information in all institutions, so that various institutions may send classified information to one another in the knowledge that the risk of compromising such information has been eliminated.

7. An effective security system, based on certain principles, is characterised by the following features:

7.1 Security prescriptions must be simple, comprehensible and capable of being carried out in practice.

7.2 Security prescriptions should not needlessly interfere with the actions of the individual. If this happens, the goodwill of the individual, which is essential for effective security, can be repressed. This can also lead to individuals treating security measures with disrespect.

7.3 In addition to what has been mentioned above, it is necessary to strive for a reconciliation between the requirements of sound administration with those of effective security.

7.4 It is necessary to constantly guard against both the overclassification and the underclassification of information. Misuse of classifications can result in the system being treated with contempt. The consequence will be carelessness with respect to the security system.

8. The security advisers of the National Intelligence Agency (NIA) are, in accordance with the responsibilities assigned to them (see Annexure A), constantly available to assist institutions in drawing up their own procedural directions. The security advisers may be contacted at the following address:

The Director-General
National Intelligence Agency
Private Bag X87
Pretoria
0001 (Attention: Information Security)

Telephone number: (012) 317-5911

9. Although every effort has been made to take into consideration different and new perspectives on security issues, this document is by no means final. To reach finality on all matters would have meant that authorising and distributing this document would have had to be postponed indefinitely, while it is being awaited urgently by all institutions. Matters that still need to be ironed out, e.g. criteria for the different security classifications, definitions of new terms and concepts related to the security field, etc, will receive attention after this volume has been issued and will be contained in a revised edition at a later stage.

10. This document replaces the former **Guidelines for the Protection of Classified Information** (SP 2/8/1) of March 1988.

CHAPTER 2

DEFINITIONS

1. **ACCESS CONTROL**

The process by which access to a particular area is controlled or restricted to authorised personnel only. This is synonymous with controlled access. See the Control of Access to Public Premises and Vehicles Act (Act 53 of 1985) as amended.

2. **AUTHOR**

The head of an institution, or the person acting on his behalf, who prepares, generates, or initially classifies a document or has it classified.

3. **CLASSIFICATION**

3.1 All official matters **requiring the application of security measures** (exempted from disclosure) must be classified "Restricted", "Confidential", "Secret" or "Top Secret".

3.2 Upgrading, downgrading and regrading of documents may take place and will involve changing the classification in accordance with the system prescribed (see Chapter 4, paragraph 1.4).

3.3 To avoid confusion, it is essential for all bodies/institutions to maintain uniformity with respect to the classification system, and to assign to documents the same rating in accordance with the degree of security warranted by the contents and nature of the documents. The security classifications as defined below should therefore be applied by all institutions. By "document" is meant those matters as set forth in the definitions section of the Protection of Information Act (Act 84 of 1982).

3.4 The classifications mentioned above are described below.

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

3.4.1 **Restricted**

Definition: RESTRICTED is that classification allocated to all information that may be used by malicious/opposing/hostile elements to hamper activities or inconvenience an institution or an individual.

Test: Intelligence/information must be classified as RESTRICTED when the compromise thereof could hamper or cause an inconvenience to the individual or institution.

Explanation: RESTRICTED is used when the compromise of information can cause inconvenience to a person or institution, but cannot hold a threat of damage. However, compromise of such information can frustrate everyday activities.

3.4.2 **Confidential**

Definition: The classification CONFIDENTIAL should be limited to information that may be used by malicious/opposing/hostile elements to harm the objectives and functions of an individual and/or institution.

Test: Intelligence/information must be classified CONFIDENTIAL when compromise thereof can lead to:

- the frustration of the effective functioning of information or operational systems;
- undue damage to the integrity and/or reputation of individuals;
- the disruption of ordered administration within an institution; and
- adverse effect on the non-operational relations between institutions.

Explanation: CONFIDENTIAL is used when compromise of information results in:

- undue damage to the integrity of a person or institution, but not entailing a threat of serious damage. The compromise of such information, however, can frustrate everyday functions, lead to an inconvenience and bring about wasting of funds;

- the inhibition of systems, the periodical disruption of administration (eg logistical problems, delayed personnel administration, financial relapses, etc) that inconvenience the institution, but can be overcome; and

- the orderly, routine co-operation between institutions and/or individuals being harmed or delayed, but not bringing functions to a halt.

3.4.3 **Secret**

Definition: SECRET is the classification given to information that may be used by malicious/opposing/hostile elements to disrupt the objectives and functions of an institution and/or state.

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

- can disrupt the effective execution of information or operational planning and/or plans;

- can disrupt the effective functioning of an institution;

- can damage operational relations between institutions and diplomatic relations between states;

- can endanger a person's life.

Explanation: SECRET is used when the compromise of information:

- can result in the disruption of the planning and fulfilling of tasks, ie the objectives of a state or institution in such a way that it cannot properly fulfil its normal functions; and

- can disrupt the operational co-operation between institutions in such a way that it threatens the functioning of one or more of these institutions.

3.4.4 **Top Secret**

Definition: TOP SECRET is the classification given to information that can be used by malicious/opposing/hostile elements to neutralise the objectives and functions of institutions and/or state.

Test: Intelligence/information must be classified TOP SECRET when the compromise thereof:

- can disrupt the effective execution of information or operational planning and/or plans;

- can seriously damage operational relations between institutions;

- can lead to the discontinuation of diplomatic relations between states; and

- can result in the declaration of war.

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

- the functions of a state and/or institution being brought to a halt by disciplinary measures, sanctions, boycotts or mass action;

- the severing of relations between states; and

- a declaration of war.

4. **CLASSIFIED INFORMATION**

Sensitive information which in the national interest, is held by, is produced in, or is under the control of the State, or which concerns the State and which must by reasons of its sensitive nature, be exempted from disclosure and must enjoy protection against compromise.

5. **CLASSIFY/RECLASSIFY**

The grading/arrangement or regrading/re-arrangement of a document, in accordance with its sensitivity or in compliance with a security requirement.

6. **COMMUNICATION SECURITY**

That condition created by the conscious provision and application of security measures for the protection of classified communication.

7. **COMPROMISE**

The unauthorised disclosure/exposure or loss of sensitive or classified information, or exposure of sensitive operations, people or places, whether by design or through negligence.

8. **COMPUTER SECURITY**

That condition created in a computer environment by the conscious provision and application of security measures. This includes information concerning the procedure for the procurement and protection of equipment.

Everything that could influence the following is considered to be relevant to computer security:

- The confidentiality of data (an individual may have access only to that data to which he/she is supposed to).

- The integrity of data (data must not be tampered with and nobody may pose as another - e.g. in the electronic mail environment, etc).

- The availability of systems.

9. **CONTINGENCY PLANNING**

The prior planning of any action that has the purpose to prevent, and/or combat, or counteract the effect and results of an emergency situation where lives, property or information are threatened. This includes compiling, approving and distributing a formal, written plan, and the practise thereof, in order to identify and rectify gaps in the plan, and to familiarise personnel and co-ordinators with the plan.

10. **CONTROLLING BODY**

The body which in terms of the rationalisation agreement, is responsible for controlling the security position within its sphere of responsibility.

11. **COPYING / DUPLICATING / REPRODUCING**

The making of a copy of any document, whether by copying it out by hand, by photographic means or by any other means.

12. **DECLARATION OF SECRECY**

An undertaking given by a person who will have, has or has had access to classified information, that he/she will treat such information as secret
(see Appendix B).

13. **DELEGATE**

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

14. **DELEGATION**

Delegation is the transfer of authority, powers or functions from one person/institution to another.

Delegation takes place in order to effect division of labour since it is physically impossible for a person/institution/body himself/herself to exercise all the powers/authorities assigned to him/her.

Delegatus delegare non potest - A delegate cannot delegate.

15. **DESTRUCTION OF CLASSIFIED MATERIAL**

The doing away with/expunging or destroying of classified documents.

16. **DISPATCHING CLASSIFIED DOCUMENTS**

The transfer of classified documents, in any manner whatever or by any channel whatever, from one point to another.

17. **DOCUMENT SECURITY**

That condition which is created by the conscious provision and application of security measures in order to protect classified documents.

18. **DOCUMENT**

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

- any note or writing, whether produced by hand or by printing, typewriting or any other similar process;

- any copy, plan, picture, sketch or photographic or other representation of any place or article;

- any disc, tape, card, perforated roll or other device in or on which sound or any signal has been recorded for reproduction.

19. **EMPLOYER INSTITUTION**

The institution, whether a public, parastatal or private undertaking (where applicable), that employs any worker, official or officer who actually has, or may probably have, access to classified matters.

20. **ESPIONAGE**

The methods by which states, organisations and individuals, attempt to obtain classified information to which they are not entitled.

21. **HEAD OF AN INSTITUTION**

The person who is serving as the head of an institution, whether defined by law or otherwise, including the official acting in his place.

22. **INFORMATION SECURITY**

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

23. **INSTITUTION**

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.

24. **NEED-TO-KNOW PRINCIPLE**

The furnishing of only that classified information or part thereof that will enable a person/s to carry out his/her task.

25. **PERSONNEL CONFIDENTIAL**

A handling instruction indicated on personnel documents. Although these documents are to be handled in the same way as "restricted" documents, this is not a security classification. Should information regarding a personnel member be more sensitive than justified by the terms "Personnel confidential" or "Restricted" it should be classified according to regulations.

26. **PERSONNEL SECURITY**

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 does have the necessary security clearance, and conducts him/herself in a manner not endangering him/her or the information to compromise. This could include mechanisms to effectively manage / solve personnel grievances.

27. **PHYSICAL SECURITY**

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

28. **PROTECTION OF PERSONS**

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.

29. **RECEIPT OF CLASSIFIED DOCUMENTS**

The receipt and documenting or taking on record of classified documents.

30. **SCREENING/ VETTING INSTITUTIONS**

Screening institutions are those institutions (the SA Police Service, the National Intelligence Agency, South African Secret Service or the SA National Defence Force) that, in terms of the rationalisation agreement, are responsible for the security screening/vetting of persons within their jurisdictions.

31. **SECURITY**

That condition free of risk or danger to lives, property and information created by the conscious provision and application of protective security measures. Not to be confused with national security (i.e. peace, stability, development and progress), which is a far broader concept that encompasses not only absence of threats, risk or danger, but also the basic principles and core values associated with and essential to the quality of life,

freedom, justice, prosperity and development. (Quoted from the White Paper on Intelligence.)

PROTECTIVE SECURITY

Much narrower concept than National Security, although very much a part/element of the latter. This concept deals with the provisioning and maintaining of measures to protect lives, property and information and as such could include : vetting, security investigations, guarding, document, personnel, physical and IT security.

32. **SECURITY AREA**

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

33. **SECURITY AUDIT**

That part of security control undertaken to:

- determine the general standard of information security and to make recommendations where shortcomings are identified;

- evaluate the effectiveness and application of security policy/ standards/ procedures and to make recommendations for improvement where necessary;

- provide expert advice with regard to security problems experienced; and

- encourage a high standard of security awareness.

34. **SECURITY CLEARANCE**

An official document indicating the degree of security competence of a person.

35. **SECURITY COMPETENCE**

This is a person's 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 interests of the State. Security competence is normally measured against the following criteria: susceptibility to extortion or blackmail, amenability to bribes and susceptibility to being compromised due to compromising behaviour, and loyalty to the state / institution.

36. **SECURITY LOCK**

A lock with at least six levers or five checks of which the tumblers are not springy (eg Chubb, Abloy and Real).

37. **SECURITY MEASURES**

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

38. **SECURITY SCREENING/VETTING**

The systematic process of investigation followed in determining a person's security competence.

39. **STORAGE**

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

40. **TRANSMISSION SECURITY**

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.

CHAPTER 3

THE PROVISION AND APPLICATION OF SECURITY MEASURES

1. RESPONSIBILITIES OF THE HEAD OF AN INSTITUTION

1.1 The head of every institution bears overall responsibility for the provision and maintenance of security in his/her institution, under all circumstances.

1.2 Apart from the ordinary or customary powers of delegation to senior officers or employees, it is necessary to prepare a clearly formulated policy signed by the head of the institution with regard to security in order to maintain information security and to ensure physical security. This security function must be delegated in writing to a fit and proper officer/employee and provision shall be made for the effective administration and practice of security.

1.3 The policy shall set forth in unambiguous terms the powers, responsibilities and duties of the security staff, and must require all personnel to submit to security measures. Security being an integral part of the management function, the composition of the security component must be such that the line of authority does not obstruct access to top management.

2. RESPONSIBILITIES OF THE HEAD OF THE SECURITY COMPONENT

2.1 The functional execution of security policy as the primary function of the chief security officer shall place emphasis on, inter alia, the following responsibilities:

- the recruitment and appointment of fit and proper persons as operational security officers;

- the training of and the exercise of control over the security personnel;

- the effective managing / administration of all spheres of security, which includes

    * planning

* organising

* financing

* staffing

* guiding and directing

* controlling/checking.

2.2 The effective practice of security will include:

- raising security consciousness;

- drawing up rules of procedure;

- the updating of relevant knowledge through self-study, attending symposia, etc;

- training personnel to know, understand and apply security procedures and measures;

- constant liaison, co-operation and co-ordination with, and reporting to, the controlling institutions;

- reporting of all breaches or alleged breaches of security, or behaviour posing a security risk, to the appropriate institutions; and

- compliance with security directives, as issued by the controlling institution.

2.3 In order to ensure that information security is undertaken on a sound basis throughout, the head of the security component must have direct access to the head of the institution and/or a seat in management meetings in as far as functional matters and policy are concerned. Following on this, "Security" should be a fixed item on the agenda.

3. OPERATIONAL SECURITY PERSONNEL

The function of such personnel is to carry out policy and rules of procedure with regard to security, as laid down by the head of the institution (see Chapter 3, paragraph 1.2).

CHAPTER 4

DOCUMENT SECURITY

These prescriptions apply to documents classified Confidential, Secret and Top Secret.

1. CLASSIFICATION AND RECLASSIFICATION OF DOCUMENTS

1.1 All bodies/institutions/organisations have at their disposal intelligence/information that is to some extent sensitive in nature and obviously requires security measures. The degree of sensitivity determines the level of protection, which implies that information must be graded or classified according to it. Every classification necessitates certain security measures with respect to the protection of sensitive information which will be known as classified information (refer to Chapter 2, paragraph 6).

1.2 The responsibility for the gradings and regradings of document classifications rests with the institution where the documents have their origin. This function rests with the author or head of the institution or his delegate(s).

1.3 The classifications assigned to documents shall be strictly observed and may not be changed without the consent of the head of the institution or his delegate.

1.4 Where applicable, the author of a classified document shall indicate thereon whether it may be reclassified after a certain period or upon the occurrence of a particular event. **This option is to be applied consistently upon the award of a classification <u>higher</u> than Restricted**.

1.4.1 Should the author of a document on which there is no embargo, reclassify such document, he must inform all addressees of the new classification.

1.4.2 The receiver of a classified document who is of the opinion that the document concerned must be reclassified, must obtain oral or written authorisation from the author, the head of the institution or his delegate(s). Such authorisation must be indicated on the relevant document when it is reclassified.

1.5 The classification of a 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 consents to a lower classification.

1.6 Every document must be classified on its own merit (in accordance with its own contents) and in accordance with the origin of its contents, and not in accordance with its connection with or reference to some other classified document; provided that where the mere existence of a document referred to is in itself information that calls for a **higher** security classification than the document containing the reference, the **latter document** must be classified accordingly.

1.7 The author of a document must guard against the underclassification, overclassification or unnecessary classification of documents. The head of an institution or his/her delegate must on a regular basis test classifications of documents generated in his/her institution against the criteria applicable to the relevant classification (see Chapter 2, paragraph 3).

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

1.8.1 **Documents and bound volumes**

The classification of loose and not permanently bound documents and bound volumes (books, publications, pamphlets) and other documents that are securely and permanently bound is typed/printed or stamped at the top and the bottom (preferably in the middle) of every page (including the cover).

1.8.2 **Copies, tracings, photographs, drawings, sketches, etc**

1.8.2.1 Security classifications shall be indicated on such documents by means of rubber stamps or other suitable means. The exact position of the mark may vary, depending on the nature of the document, so that essential details shall not be obscured by the stamp. An effort must, however, be made to mark the document as clearly as possible, so that the mark will immediately attract attention.

1.8.2.2 Tracings or blueprints shall be marked in such a way that the security classification is visible on all copies. Where this is not possible, rubber stamps should be used to mark all the copies.

1.8.3 **Rolled or folded documents.** Apart from being marked as prescribed on the face, a document such as this shall also be marked in such a way that the security classification will be clearly visible when the document is folded or rolled up.

1.8.4 **Tape recordings and documents on which no marks can be made.** Where, as in the case of tape recordings, certain photographs and negatives, it is physically impossible to place clear classification marks on a document itself; the document should be placed in a suitable box, envelope or other container and, if necessary, sealed. The nature and classification of the contents clearly marked on the outside of the container.

1.8.5 **Files.** A clear distinguishing mark, the significance of which is known to those who deal with the file concerned, should be placed on both the front and the back cover of Secret or Top Secret files.

Note: For an explanation of the classifications, see Chapter 2, Definitions.

2. ACCESS TO CLASSIFIED INFORMATION

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

2.1 A person who has an appropriate security clearance or who is by way of exception authorised thereto by the head of the institution or his/her delegate (see Chapter 5, paragraphs 3.6, 10.2 and 10.3), with due regard being paid to the need-to-know principle.

2.2 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 authorisation has been granted, as explained in Chapter 4, paragraph 2.1.**

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

3. HANDLING OF CLASSIFIED DOCUMENTS

3.1 All classified documents must be stored in accordance with instructions while not in use (see Chapter 4, paragraph 10).

3.2 All incoming classified documents, including official, classified post marked "Personal" must be received and noted in a register by persons with the appropriate clearance. The object of such registration is to enable total control over such documents. This provision does not apply to documents bearing a classification of Restricted.

3.2.1 Officials who usually receive the incoming post of an institution (eg registration officers) must hand the unopened inner envelope of incoming classified correspondence to the appropriate official(s) who is/are authorised to open correspondence in a certain category. The latter is/are responsible for entering the correspondence concerned in the prescribed register.

3.3 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.

3.3.1 Measures must be taken to ensure that classified documents are not physically taken from one institution to another and/or informally handed to a member of another institution during a contact visit, in this way evading prescriptions for the registration of incoming and outgoing post.

3.3.2 The various institutions may draw up standard registers in which the particulars of classified postal material are to be entered. Registers for the particulars of postal material classified as Secret and Top Secret are to be classified accordingly. The registers must include the following particulars:

3.3.2.1 **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, Recipient (signature); Further dispatch (serial number of the entry for outgoing mail in the register); Destruction (date and signature).

3.3.2.2 **Particulars of outgoing post:** Serial number of the 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); Receipt number; Date when receipt was obtained.

3.4 When Secret and Top Secret documents are distributed, dispatched or made available, they must be accompanied by a receipt voucher signed by the addressee, the receipt of which must again be controlled by the sender. The receipt voucher is classified only if the subject/heading of the document itself is classified, in which case the classification must agree with that of the document.

3.5 All Secret and Top Secret documents must be given copy numbers and an indication must be given of the number of copies produced, eg Copy 1 of 7 copies. The copy number should appear on the first page of each document, in the upper right-hand corner. (See paragraph 14 for the procedure to be followed when copies are made of classified documents.)

3.6 A serial number must be allocated to every document filed in a **classified file** as is indexed on a page attached to the inside of the file cover, together with the name/heading of the document concerned.

4. TRANSMITTING DOCUMENTS BY MEANS OF FACSIMILE

4.1 When classified documents are transmitted by means of facsimile, **only** facsimile machines equipped with encryption as prescribed by Communication Security Policy/Instructions must be used.

4.2 Classified reports may only be handled by a suitably cleared operator.

4.3 The Cryptographic equipment and facsimile machines must be kept in a room that is manned **at all times while it is unlocked or in use** by a suitably cleared, trained and appointed official, while care has to be taken that reports received through this apparatus are not accessible to unauthorised persons. The Cryptographic equipment must be handled in accordance with Communication Security Policy/Instructions.

4.4 A record must be kept of the transmission and receipt of classified documents.

4.5 After receiving a message, receipt must be acknowledged immediately. The recipient shall ensure receipt of **all pages.**

4.6 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, he/she shall immediately transmit an acknowledgement of receipt to the sender.

4.7 The recipient shall, on his/her copy, note the copy number as indicated on the distribution list.

4.8 Effective control must be exercised over "open" facsimile machines to ensure that these are **not** used for the transmission of classified documents.

5. TRANSMITTING DOCUMENTS BY COMPUTER

5.1 Encryption as prescribed shall be applied with respect to the computerised transmission of classified documents.

5.2 A record shall be kept of the classified documents transmitted and received, provided that the recipient of documents must always acknowledge receipt of classified documents. It must also be remembered that all magnetic media must be regarded as documents and handled as such.

5.3 Such documents must be supplied with copy numbers (see Chapter 4, paragraph 3.5).

6. DISPATCHING CLASSIFIED DOCUMENTS BY COURIER

6.1 All classified documents (sealed according to prescription - see Chapter 4 paragraph 8) must be noted in a register indicating the title/description of the document and the date and time of dispatch, and must be handed over against the signature of the courier.

6.2 A courier must convey classified documents in a safe locked container. It is recommended that where possible, the container should have a combination lock.

6.2.1 Secret and top secret documents (and where necessary also sensitive confidential documents) should be delivered locally only by hand (ie by a courier. The following shall be adhered to:

- Couriers must have at least a Confidential security clearance).
- Where possible the courier must be accompanied by a second person.
- All classified material must be conveyed under safe conditions, that is preferably in an attache case with a code or combination lock (particularly if the courier is not accompanied by a second person).
- The courier must obtain an appropriate receipt for the material.
- On the return of the courier the receipts for classified deliveries must be checked by a responsible officer.

6.2.2 Control must be exercised over the time taken by the courier to deliver the documents. Upon receipt, the recipient of such documents must check that the documents have not been compromised.

6.2.3 Couriers must be able to identify themselves when fetching or dispatching post.

6.2.4 Cryptographic equipment must be handled according to Communication Security Policy/Instructions.

7. DISPATCHING CLASSIFIED DOCUMENTS BY MAIL

7.1 Classified documents in the Secret and Top Secret categories that cannot be dispatched by courier may, as an exception, be mailed on provision that it be sent by registered mail and then only with the express permission of the head of the institution or his delegate.

8. SEALING OF CLASSIFIED DOCUMENTS BEFORE DISPATCH

8.1 Classified documents that are dispatched (excluding by facsimile and computer) must be sealed and handled in the following way:

8.1.1 A receipt to be signed by the addressee and returned to the sender, must be attached to the document and placed in the inside envelope. This does not apply to "Restricted" documents.

8.1.2 Classified documents must always be dispatched in a double envelope/cover, ie in an envelope placed within another (excluding "Restricted" documents). The following process shall be followed:

- 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 for this purpose, they must be attached with passport glue (seals that can be re-used are not suitable for this purpose).

- Thereafter 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.

- The security classification of the document must be indicated clearly on the front and the back of the envelope by means of a rubber stamp.

Alternative method for sealing postal material in bulk: The inside envelope can be sealed without seals, stamps, tape, reference number and classification by means of a mechanical process of vacuum packaging in plastic. Some of the requirements in this case are:

- A sticker on the envelope bearing the following particulars: reference number of the document, name, address and special handling instructions

- The plastic packaging must be of good quality (ie it may not tear).
- Changeable stamps of the relevant institution must be imprinted on the plastic packaging. For this purpose the ink must not be able to be removed from the plastic.

- Dispatch of such documents may **only** take place by courier. The delivery time must be controlled strictly and consistently.

Remark: Before implementing this alternative, the National Intelligence Agency must be contacted in order that the relevant institution may be advised on the maintaining of security standards.

8.1.2.2 The outer envelope should bear only the name and address of the addressee and the name and address of the sender. Under no circumstances should there be an indication of the nature or classification of the contents, since this could attract undesirable attention to the document.

8.1.3 Persons who normally receive incoming post in an office (such as the registry officers) must make sure that they know who is authorised to open incoming classified correspondence in each particular category and must hand the inner envelope unopened to the authorised officer(s) concerned.

9. BULK CONVEYANCE OF CLASSIFIED DOCUMENTS

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

9.2 **The bulk conveyance of classified documents by train**

9.2.1 The transportation of official documents to and from Cape Town at the beginning and end of the Parliamentary Session should comply with the following minimum requirements:

9.2.1.1 Documents must be packed in steel trunks and the locks of the trunks must be of an acceptable quality. Departments/ministries must apply proper key control at all times, even when the locks are not in use.

9.2.1.2 Each trunk/cabinet must be bound with at least two steel hoops (of the packing type) as an additional precaution to prevent the trunk/cabinet from being opened or opened accidentally during transport as a result of handling.

9.2.1.3 Trunks must not be marked with a mark indicating whether the contents are classified or not; each should merely bear a number to facilitate record-keeping.

9.2.1.4 A list must be kept of the contents of each trunk/cabinet opposite the number allocated to the trunk/cabinet.

9.2.1.5 Departments must co-ordinate the transportation arrangements for their trunks/cabinets of documents with their own ministries. Where more than one department is accommodated in the same building, there can be interdepartmental co-ordination with regard to transportation arrangements (also see Chapter 4, paragraph 9.2.1.12).

9.2.1.6 Departments must make arrangements in good time with Spoornet for trailers/containers (ie a lockable trailer on its own wheels/a lockable container) in which to load the trunks/cabinets.

9.2.1.7 After the trunks have been packed, locked and bound, the record of the numbers of the trunks and their contents, as well as the keys to the locks, must be given to responsible officer (eg the Parliamentary Officer), who will personally take the records and the keys with him to Cape Town or Pretoria as the case may be.

9.2.1.8 The trunks/cabinets must then be carried out of the building and packed directly into the trailer/container, after which the trailer/container is sealed in the presence of the officer concerned. Care should be taken not to stack trunks/cabinets on the sidewalk to wait for the trailer/container.

9.2.1.9 The responsible officer must further ensure that he is present when the trunks/cabinets arrive at their destination, so that the seals of the trailer/container can be broken in his presence and trunks/cabinets (still locked and bound) can be checked.

9.2.1.10 When trunks/cabinets are not in use, proper control must be exercised over the locks and their keys. If possible they should be kept, sealed in envelopes, in a safe or strongroom.

9.2.1.11 Where departments have the capacity of their own for the transportation of documents between Cape Town and Pretoria, the documents must still be packed as prescribed above and the same control measures with regard to trunks/cabinets must be instituted.

9.2.1.12 Arrangements for the transportation of classified documents under accompaniment between Pretoria and Cape Town before and after the Parliamentary sessions can be co-ordinated with the National Intelligence Agency.

9.3 **Diplomatic bags**

9.3.1 Classified and unclassified documents to be dispatched to RSA missions abroad or departmental representatives there must be sent to the Department of Foreign Affairs for dispatch, whether in diplomatic or airfreight bags. Unclassified documents are normally dispatched by freight bag, while Confidential, Secret and Top Secret material must be dispatched by diplomatic bag.

9.3.1.1 The diplomatic bag is classified as a Category A bag, and is therefore opened and handled differently from the freight bag for security reasons. Both types of bag are sent to missions abroad by scheduled flights (usually once a week but in some cases only every second week) and departments must therefore hand such postal items in to the relevant division of Foreign Affairs on or before the dispatch date, making use of a courier. A signature must be obtained acknowledging receipt of classified material.

9.3.1.2 In view of the substantial difference between the airfreight rates for the different types of bag, classified and unclassified documents destined for RSA missions abroad must be carefully separated beforehand by authorised officers in the dispatch offices of departments and made up into two (2) separate envelopes or packages. More than one classified document may be placed in each envelope for each individual mission (except in the case of cryptographic material) and it is therefore not necessary for Secret and Top Secret documents to be sealed individually in double envelopes as indicated in Chapter 4, paragraph 9.3.1.4 below. Cryptographic material must still be dispatched in accordance with the Communication Security Policy/Instructions. Strict precautions must, however, be taken to ensure that classified documents under cover of an unclassified letter are not erroneously placed in the envelope intended for the freight bag.

9.3.1.3 All confidential, secret and top secret documents for a particular mission must, as far as, possible be placed in a single envelope by authorised officers of departments. A schedule recording the titles, reference numbers and dates. of all the classified postal items for the mission concerned, must be made out in triplicate. The original plus one copy should be sealed in the envelope with the classified documents in the prescribed way. The third copy of the schedule is kept for record purposes, while the second copy, which is sealed into the envelope, is signed by the representative of the department concerned at the mission and returned to the department by the next returning freight bag as a receipt for the classified documents. In the case of non-sensitive documents, ie those that are sent by freight bag, a schedule is not required.

9.3.1.4 The envelope containing the classified material must be stamped clearly on the front and the back in the upper right-hand corner with the letters "DIP", (about 4cm x 4cm in size). The other envelope containing the non-classified items must be stamped "FV" in the same way and with the letters of the same size. For the rest only the name of the mission (eg: The SA Embassy, London; or, The Consulate-General, New York) the name of the addressee or the post occupied by him (eg: The Counsellor [Trade]), and the reference number, if any, should appear on the outside of the envelope. The envelope may also bear the address stamp of the sender department.

9.3.1.5 No private or personal items such as gifts, or foodstuffs or bank notes may be dispatched in the diplomatic bags, whether to an officer at a mission abroad or in the RSA. The Vienna Convention also provides that only official material may be dispatched in the bags concerned. In order to ensure that this provision is complied with, the Department of

Foreign Affairs may therefore, where it is considered necessary, examine the contents to ensure that the mentioned provisions are complied with.

9.3.1.6 Diplomatic bags must be conveyed to and from airports by an authorised, security-cleared officer. Where circumstances require this, two officers should be detailed for the task. In the case of RSA missions abroad, one of these may be a locally recruited person. While the bags are in the vehicle it may not under normal circumstances (with due regard to the ordinary traffic regulations) stop along the way for any reason, nor may the bags be left unguarded in the vehicle.

9.3.1.7 An officer travelling abroad must not take secret or top secret documents with him, unless it will be possible for the documents to remain continuously under his personal supervision, he has a courier's letter with him and he has the consent of the head of his department, who may delegate the giving of approval to the chief security officer or other senior officer(s). Officers requiring classified documents abroad should, when at all possible, arrange in advance for the documents to be dispatched by diplomatic bags as described above.

9.3.1.8 **Conveyance of diplomatic and freight bags to and from airports**

9.3.1.8.1 Unless approval has been obtained for a different procedure the bags concerned must be conveyed to and from airports by car by at least two persons from the mission. One of these persons must be a transferred officer at the mission while the second may be a locally recruited staff member. The services of the latter may only be used in a supporting capacity, eg to drive the car and carry the bags. Locally recruited members may not, however, be permitted to sign for the bags.

9.3.1.8.2 While the bags are in the vehicle it may not under normal circumstances, with due regard to the ordinary traffic regulations, stop along the way for any reason, nor may the bags be left unguarded in the vehicle.

9.3.1.8.3 The officer receiving the incoming bags at the airport must satisfy himself that the bags are correctly addressed, that the consignment is complete, that the seals are unbroken and that the bag has not been tampered with in some way or other. Any irregularities in this regard must be investigated immediately and reported to Head Office, Department of Foreign Affairs, by telex or facsimile for the attention of Diplomatic Bags.

9.3.1.8.4 The diplomatic postal service to and from airports concerned remains the joint responsibility of attached divisions (departments) of a mission. Therefore the attached personnel components concerned should undertake trips to the airport on a rotation basis to deliver or fetch diplomatic bags.

9.3.1.8.5 The head of the mission is responsible for, inter alia, the efficient functioning of the mission and therefore also for the handling of diplomatic bags. Accordingly it is his prerogative to make suitable arrangements, at his discretion and in consultation with heads of divisions, for the transportation of the diplomatic bags to and from airports.

9.3.1.8.6 The following applies in terms of the procedures for week-end/after hours duty at a mission by officers of attached departments:

- Where only one officer of another department has been attached to a mission, diplomatic bag duty during normal office hours will be the exclusive responsibility of officers of the Department of Foreign Affairs, and week-end and after-hours duty (including diplomatic bag duty) will be the responsibility of officers of all attached departments.

- Where more than one officer of another department has been attached to a mission, officers of all departments will be responsible for week-end/after-hours duty as for diplomatic bag duty during and outside normal office hours.

- The Standing Committee (ie representatives of all departments at the mission) will be responsible for drawing up a duty roster which will be binding on all officers at the mission. Only the Standing Committee will have the power to make changes to such a duty roster.

9.3.1.9 The Department of Foreign Affairs will from time to time extend/amend instructions regarding the handling of diplomatic bags.

10. STORAGE OF CLASSIFIED DOCUMENTS

10.1 Classified documents that are not in immediate use must be locked away in a safe storage place (see par 10.4.2).

10.2 The doors of all offices in which classified documents are kept must at least be fitted with security locks.

10.2.1 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. The identification of visitors, the issue of visitors' cards or temporary permits, the escorting of visitors, the provision of identity cards for officers/employees working in the building/offices and the use of related documents and registers for this purpose are prerequisites for effective control over access to and within a building or part of a building.

10.2.2 Effective control must be instituted over access to security areas in a building such as cryptographic and computer centres, the registry (where secret and top secret documents and files are kept) and other areas identified as sensitive. An access register must be instituted and kept up to date for all persons/officers not normally working in these areas.

10.3 Where necessary (depending on the sensitivity of the classified material kept or dealt with in a particular room or division) doors, windows, fanlights, passages, stairs, etc, giving access to the room or division should be equipped with locks, bolts, iron bars or metal blinds of adequate strength, as the case may be. In some cases it may be sufficient to equip one room in a building in this way to serve as registry or storeroom for classified material.

10.4 Apart from taking the precautions mentioned above, all the doors of any room in which classified secret or top secret material is dealt with or handled must be fitted with security locks (see Chapter 2: Definitions) and must be locked when it is vacated, even for a short period, by the person(s) using the room.

10.4.1 If the officer(s) leave the room for a longer period, eg during the lunch hour, all classified secret and top secret material must be locked away in a safe or metal cabinet which is of adequate strength and equipped with a security lock.

10.4.2 When classified documents are not in use, it must be stored in the following way:

- **Restricted:** Normal filing cabinet.
- **Confidential:** Reinforced filing cabinet.
- **Secret:** Strongroom or reinforced filing cabinet.
- **Top Secret:** Strongroom, safe or walk-in safe.

10.5 The keys to any building, part of a building, room, strongroom, safe, cabinet or any other place where classified material 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.**

10.6 The keys to safes and strongrooms must be kept in safe custody in accordance with Chapter 23, paragraphs 23.3.6, 23.3.10, 23.3.12 and 23.3.14 of the Provisioning Administration Manual and other relevant directions.

10.7 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:

- When it is suspected that it has been compromised.

- 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.
- When a new user takes over.

10.7.1 Combinations may be compromised by:

- unauthorised persons noting the combination through observation when the lock is opened;

- failure to set the combination in accordance with the manufacturer's specifications;

- failure to change the combination after a reasonable period.

10.7.2 Precautions must therefore be taken by the authorised user to ensure that no other 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 :

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

- Avoid the use of numbers with some personal significance, eg 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. (eg 68-13-57-11)

- Only the user may set a combination lock.

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

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

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

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

11. REGISTRIES AND FILES

11.1 Central Registries for Receiving of Incoming Mail and Dispatching of Outgoing Mail

11.1.1 An effective registry is the core of effective document control and of document security. One registry in an institution 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 (whether electronic or hard copy).

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

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, Recipient (signature); Further dispatch (serial number of the entry for outgoing mail in the register); Destruction (date and signature).

Particulars of outgoing post: Serial number of the 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); Receipt number; Date when receipt was obtained.

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

11.1.2 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.

11.2 Access to Registries

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.

11.3. Management of Files

11.3.1 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.

11.3.2 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.

11.3.3 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 file number.

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

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

11.3.6 Classified files must be stored in facilities as prescribed for classified documents.

11.3.7 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 document.

11.3.8 A subfile 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 subfile to whom the main file has been issued, and when. The subfile 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.

11.3.9 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.

11.3.10 **Only** authorized persons may be allowed access to classified files. Internal policy should dictate who may authorize such access, subject to the need-to-know principle.

12. REMOVAL OF CLASSIFIED DOCUMENTS FROM PREMISES

12.1 The removal of classified documents from office buildings shall be prohibited as far as possible.

12.2 Classified material (with the exception of "Restricted" documents) may not be taken home without the written approval of the Head of the Institution or his delegate; a list of the documents to be removed must be handed to the person in control of record keeping. (The form in Appendix C can be adjusted to suit this purpose.) Persons may take classified documents home only if they have proper lock-up facilities (see Chapter 4, paragraph 10.1), in other words, if a person has no such facilities, the documents may not be kept at such a person's home for the purpose of work after hours.

12.3 Classified documents taken out of a building with a view to utilisation at meetings or appointments must be removed in a lockable security attache case. Furthermore, all guidelines included in Chapter 4, paragraph 10 apply in this regard.

13. THE TYPING OF CLASSIFIED DOCUMENTS

13.1 Classified documents may be typed only by persons having the appropriate security clearance. Such typing must be done in a manner that will ensure that the information is not divulged to unauthorised persons.

13.2 Drafts of classified documents, typewriter ribbons, and copies and floppy disks must at all times be treated as classified documents.

13.3 In this regard also see the **Manual for Computer Security**.

14. DESTRUCTION OF CLASSIFIED DOCUMENTS

14.1 In terms of the Archives Act, 1962, all documents received or created in a 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 or other Act of Parliament. It should be a point of departure that all state documentation is subject to the Archives Act, unless justifiably excluded along the above-mentioned lines. It should be noted that no document is to be excluded merely because it is classified. Heads of Departments will have to decide, after consultation with their legal advisers as well as the Director: State Archives whether the document(s) concerned is/are of such a nature that there is a legitimate demand for secrecy that goes beyond the degree of safekeeping by the State Archives.

14.2 Where destruction has been properly authorised, it should take place by burning or some other approved method, eg 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 officer who has destroyed the documents must give a certificate of destruction of the documents concerned to the head of the institution or his delegate.

14.2 The process of destruction must be such that reconstitution of the documents destroyed is impossible.

14.3 If the necessary precautions are not instituted, access to waste-paper baskets is probably one of the easiest ways for unauthorised persons to obtain sensitive information. Special attention should therefore be given by all those concerned to the disposal of drafts, notes, used carbon paper, typewriter ribbons, etc, that may contain information. Such waste must be stored separately under lock and key and must be periodically collected by an officer(s) specially designated for this purpose and destroyed by means of burning or shredding.

14.4 In terms of the procedure for the destruction of classified documents from other departments/institutions, a destruction certificate must be supplied to the author.

15. MAKING PHOTOCOPIES OF CLASSIFIED DOCUMENTS

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

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

15.3 Oral or written authorisation for the copying of secret and/or top secret documents by the author, head of the institution or his delegate(s) is required for the copying of secret and/or top secret documents. Such authorisation must be indicated on the original document.

15.4 Copies of all secret and top secret documents must receive 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 addressees/departments, individuals concerned and the corresponding copy numbers must be written in the file and record copy. Alternatively a distribution list can be attached to all copies of the relevant document concerned, indicating the addressees and the applicable copy number.

15.5 No copies or duplicates may be made of the documents of The National Intelligence Co-ordinating Committee (NICOC). Only NICOC may make available additional copies on request.

16. THE HANDLING OF RESTRICTED DOCUMENTS

16.1 Documents classified as "**Restricted**" are deemed to be restricted to only the relevant institution.

16.2 Precaution must therefore be taken to prevent unauthorised persons from gaining insight into **Restricted** documents.

17. CONTINGENCY PLANNING

17.1 The contingency plan of an institution must provide for the destruction, storage and/or moving of classified/sensitive documents in the event of an emergency in order to prevent the risk of being compromised.

CHAPTER 5

PERSONNEL SECURITY:
GUIDELINES WITH RESPECT TO SECURITY VETTING

1. INTRODUCTION

1.1 Security vetting is the systematic process of investigation followed in determining a person's security competence.

1.2 The degree of security clearance given to a person is determined by the content of and/or access to classified information entailed by the post already occupied/to be occupied by the person.

1.3 A clearance issued in respect of a person is merely an indication of how the person can be utilised, and does not confer any rights on such a person.

1.4 A declaration of secrecy should be made on an official form by an applicant to any government post, before he/she is appointed or during the appointing process.

1.5 Political appointees (Director Generals, Ambassadors, etc) will not be vetted, unless the President so requests or the relevant contract so provides. From the lowest level up to Deputy Director General all staff members and any other individuals who should have access to classified information, must be subjected to security vetting.

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

2. VETTING CRITERIA

2.1 Vetting/screening criteria need to be adjusted continuously owing to the development in the political field and changes in the social and socio-economic fields. On a macro level, screening criteria must be adjusted to the norms and values of the community of which the person is a part. However, on the micro level, screening criteria must provide for the unique nature of individuals and organisations. The overall picture of an individual's security competence (which is the result of individual differences and the individual's

unique way of handling situations) has to play a determining role in a vetting recommendation/decision.

2.2 Aspects such as gender, religion, race and political affiliation do not serve as criteria in the consideration of a security clearance, but actions and aspects adversely affecting the person's vulnerability to blackmail or bribery or subversion and his loyalty to the State or the institution do. This also includes compromising behaviour.

3. SECURITY SCREENING IN RESPECT OF IMMIGRANTS AND PERSONS WITH MORE THAN ONE CITIZENSHIP

3.1 **Confidential Clearance.** A confidential clearance may be considered in respect of an immigrant who has been resident in the RSA for ten consecutive years of which at least those five years preceding the clearance were spent as a South African citizen. He/she must provide sufficient proof that any former citizenship has been relinquished.

3.2 **Secret Clearance.** A secret clearance is only considered in respect of an immigrant who has been resident in the RSA for fifteen consecutive years of which at least those ten years preceding the clearance were spent as a South African citizen, also on the condition that the person has relinquished his/her former citizenship.

3.3 **Top Secret Clearance.** After an immigrant has been resident in the RSA for a period of twenty consecutive years (of which fifteen years were spent as a South African citizen), a top secret clearance may be considered, on the condition that such a person has relinquished his/her former citizenship. Every case will be dealt with on merit owing to the unique nature of each situation. This means that not all immigrants who comply with the requirements will automatically qualify for a top secret clearance.

3.4 **Dual Citizenship.** Each application for a security clearance in respect of persons with dual citizenship must be assessed on the merits of each individual case.

3.5 **Persons without valid Identification Documents.** No clearance can be issued in the following cases:

3.5.1 Any person who is not in possession of a valid identification document or residence permit for the RSA.

3.5.2 Naturalised RSA citizens who have not applied for a new identification document after naturalisation, since the document that was issued before naturalisation expires on naturalisation.

3.6 **Employing Immigrants who do not meet Clearance Requirements.** If on account of his/her indispensable expertise, it is considered essential to employ an immigrant while he/she does not satisfy the clearance requirements as laid out above and he/she is to be utilised in a post, the work of which is classified, the vetting authority will be unable to make a positive recommendation with regard to the issue of a security clearance in respect of such a person, but can merely institute an investigation to determine whether such an immigrant is suitable from a security point of view for the post concerned. In such an event the head of the employing institution may authorise that the immigrant be used in the post (see Chapter 5, paragraph 10.2), on the condition that the employing institution must

- submit a certificate to the National Intelligence Agency and the responsible screening institution in which the absolute necessity of employing such immigrant is set forth and it is also declared that no **RSA citizen** with the same expertise is available or can be recruited in the RSA and, in cases where an immigrant from a state formerly seen as controversial has been employed, that an immigrant from **a non-controversial country** could not be obtained;

- provide the responsible screening institution with a description of and an indication of the sensitivity of the responsibilities attached to the post to be occupied by the immigrant;

- declare that it accepts full responsibility for compliance with the security requirements connected with the employment of such immigrant;

- ensure that no classified information or material that is not needed for the performance of his duties comes into the possession of the incumbent of the post; and

- reconsider the authorisation every year and relate in writing to both the National Intelligence Agency and the responsible screening authority any incident which could pose a threat to security or any incidence which may bring his/her security competence into question.

3.6.1 **Take note:** When the person concerned changes his/her posting, the authorisation is automatically terminated.

3.7 In respect of immigrants already employed in sensitive positions and in whose case the conditions laid out in Chapter 5, paragraph 3.6 above have not yet been complied with, the employing institution must immediately give effect to those conditions as set out in paragraph 3.6.

4. SCREENING / VETTING OF PERSONS WHO HAVE LIVED/WORKED ABROAD FOR LONG PERIODS

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

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

4.1.2 A Secret clearance after three years back in the RSA.

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

5. SECURITY SCREENINGS : CONTRACTORS SUPPLYING SERVICES TO GOVERNMENT DEPARTMENTS OR OTHER GOVERNMENT INSTITUTIONS

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

"Acceptance of this tender is subject to the condition that both the contracting firm and its personnel providing the service must be cleared by the appropriate authorities to the level of **CONFIDENTIAL/SECRET/TOP SECRET**. Obtaining a positive recommendation is the responsibility of the contracting firm concerned. If the principal contractor appoints a subcontractor, the same provisions and measures will apply to the subcontractor.

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

5.2 The security responsibilities of the contractor will be determined by the department/institution concerned.

6. PROCEDURE FOR REQUESTING SECURITY SCREENINGS

6.1 Requests for security screening and re-screening must be submitted to the appropriate screening authority on the prescribed form (see Appendix D) accompanied by a set of clear fingerprints.

6.2 The requesting institution should provide the screening authority with a post description of the employee concerned and an indication of the access he/she has/will have and with all other facts that may influence the issue of a clearance.

7. PERIOD OF VALIDITY OF SECURITY CLEARANCES

7.1 The head of an institution or his/her delegate must ensure that an officer in respect of whom a security clearance of Secret or Top Secret has been issued, is rescreened every five (5) years and every ten years in respect of a Confidential clearance.

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

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

8. TRANSFERABILITY OF CLEARANCES

8.1 A security clearance issued in respect of an officer while he/she is attached to a particular institution is not automatically transferable to another institution, for example when the officer is transferred. When an officer changes his employer, the responsibility for deciding whether an applicant's existing clearance will be accepted or whether the rescreening of such an officer will be requested in the prescribed way rests with the new employer.

8.2 However, for the purpose of meetings and other co-operative functions clearances are transferable. The employing institution is responsible for informing the chairman of such a meeting in writing as to the level and period of validity of the clearances of the representatives involved.

9. RESPONSIBILITIES OF THE SCREENING AUTHORITY

9.1 The screening authority will investigate and advise on the security competence of a person on the basis of prescribed guidelines.

9.2 After the investigation the screening authority will merely make a recommendation regarding the security competence of the person concerned to the head of the requesting institution, and this should in no way be seen as a final testimonial as far as the utilisation of the person is concerned.

10. RESPONSIBILITIES OF THE HEAD OF THE REQUESTING INSTITUTION

10.1 The head of an institution or his delegate must make a decision and issue a clearance after receiving the recommendation made by the screening institution, and in accordance with circumstances/information at his/her disposal.

10.2 Notwithstanding a negative recommendation from the screening authority, for whatever reason, the head of the institution may still, after careful consideration and with 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 RSA or his/her institution, on the understanding that a person satisfying the clearance requirements is not available.

10.3 When **any** person is utilised without a clearance, the responsible screening institution and the National Intelligence Agency must be furnished every year with a certificate regarding such person's security conduct (see Chapter 5, paragraph 3.6). Any conduct entailing a security risk must be reported immediately to the screening authority concerned (also see Chapter 9: Breaches of Security).

10.4 Heads of institutions whose officers attend meetings where classified matters are discussed must inform the chairperson of such a meeting in writing of the level of security clearance of such officers. It is the responsibility of the chairperson to satisfy himself/herself regarding the security clearance of all those present at the meeting.

10.5 Further, it is also the responsibility of the head of the institution or his/her delegate to

- ensure that there is continuous supervision of persons in respect of whom security clearances have been issued;

- present security awareness programmes for his/her employees and to warn staff members not to supply personal particulars of colleagues/officers to unauthorised persons;

- ensure that persons dealing with classified matters sign the prescribed declaration of secrecy (see Appendix B, a draft declaration that can be modified to suit the requirements in each particular case);

- pertinently bring to the attention of the officers working with classified matters any other legislation, regulation and/or orders that entail secrecy and/or the protection of activities, installations, etc, of any particular institution.

- to point out to employees dealing with classified matters when they resign or leave the service that they will continue to be the target of foreign intelligence services and that they remain subject to the declaration of secrecy.

- to ensure that all classified documents in the possession of the person concerned are returned when such person resigns or leaves the service; and

- to ensure that no information comes into the possession of an individual that is not essential for the performance of his or her duties.

11. OFFICERS TRAVELLING ABROAD

11.1 In the event where an official with a clearance travels abroad, the head of the institution employing the official or his/her delegate must keep a thorough record of such visits.

11.2 When officials are travelling abroad they must be on their guard against any attempt by a foreign intelligence service to recruit them. If a person is approached, he or she must, immediately on returning, report the fact to the head of the institution or his/her delegate for transmission to the responsible screening authority and the National Intelligence Agency. While travelling, officials should maintain a low profile and be careful not to place themselves in compromising situations.

12. PROTECTION OF EXECUTIVE OFFICIALS

12.1 Since executive officials are constantly the target of enemies of the State, the necessary precautions should be taken to protect these officials against threats of blackmail or violence. Such threats should be reported to the NIA or the SAPS or the SANDF (MI), as the case may be. The necessary precautionary and protective measures must be undertaken by the various institutions to ensure the safety of the officials concerned. More particulars in this regard may be obtained from the National Intelligence Agency.

13. STATUTORY AND OTHER PROVISIONS FOR THE PROTECTION OF INFORMATION

13.1 The attention of all persons dealing with classified matters should be drawn specifically to the provisions of the Protection of Information Act (No 84 of 1982) as amended.

13.2 Any other legislation, regulations and/or directives relating to secrecy and/or the safeguarding of the activities, installations, etc of a particular institution must also be specifically brought to the attention of officers dealing with classified matters.

CHAPTER 6

COMMUNICATION SECURITY

1. Policy/ standards in the computer/ communications security field will be more frequently updated (because of technological advances) than policy in the other security fields. As the computer/ communications security policy is currently being updated and integrated in order to reflect the amalgamation of the previous Computer Security Task Group and the Joint Communications Security Council, computer/ communications security policy will be separately promulgated. The computer and communications security policy is however regarded as part of the Minimum Information Security Standard.

2. The authority to promulgate computer and communications policy is hereby delegated to the Chairman of the Functional Security Committee of the National Intelligence Co-ordinating Committee (NICOC) after :

- the Chairman has ensured that it is integrated and in line with policy regarding other security disciplines;

- legal principles were taken into account.

3. Communication security may be described as a condition that is created by the deliberate application of measures to safeguard sensitive communication, whatever form it may take.

4. Communication may be divided into two main categories:

4.1 Communication taking place with the aid of communications equipment, telex equipment, computer equipment, radio and facsimile equipment and the telephone. The Communications Security Policy serves as the minimum communication security standard.

4.2 Communication taking place without communications equipment, ie mainly personal communication.

5. In terms of Communications Security Policy classified information may be transmitted only under the following conditions:

5.1 Via acceptable and approved apparatus.

5.2 The necessary encryption, as prescribed, must be present.

6. 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:

6.1 the need-to-know principle.

6.2 such conversation should take place in such a way that sensitive information/intelligence does not come into the possession of unauthorised persons or persons who happen to overhear;

6.3 places such as offices, conference rooms etc, where sensitive or classified matters are discussed on a regular basis should be subject to

- proper and effective access control (eg outside maintenance personnel and cleaners);
- regular electronic surveillance counter measures (sweeping). (In this regard the National Intelligence Agency can be contacted in the case of government departments, parastatals and private institutions. The SASS, SANDF and the SAPS are responsible for electronic surveillance counter measures with regard to their own environments).

7. The Chief Directorate Security of NIA or SACSA may be approached for further advice and guidance in respect of communication security needs.

CHAPTER 7

COMPUTER SECURITY

1. Policy/ standards in the computer/ communications security field will be more frequently updated (because of technological advances) than policy in the other security fields. As the computer/ communications security policy is currently being updated and integrated in order to reflect the amalgamation of the previous Computer Security Task Group and the Joint Communications Security Council, computer/ communications security policy will be promulgated separate from this issue of the MISS. The computer and communications security policy will however regarded as part of the Minimum Information Security Standard (MISS).

2. The authority to promulgate computer and communications policy is hereby delegated to the Chairman of the Functional Security Committee of the National Intelligence Co-ordinating Committee (NICOC) after :

   - the Chairman has ensured that it is integrated and in line with policy regarding other security disciplines;

   - legal principles were taken into account.

3. In the light of the increasing dependence on and the proliferation of computers in the administration of the country in general, and also of the extent to which classified information is processed by means of computers, security has become essential in this area.

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

5. It is the responsibility of the head of the institution or his delegate to ensure that all personnel concerned with computers receive the necessary security training. In addition, the security awareness of all personnel using computers must receive regular attention.

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

- essential backup of computer systems and data;
- physical security measures as prescribed;
- computer security responsibilities should be clearly established;
- the allocation and use of passwords as prescribed.

7. Where use is made of computer communications and data is transmitted through an unprotected area, the transmission should be protected in accordance with Communication Security Policy/Instructions.

8. All breaches of security in the computer environment must be reported as soon as possible in accordance with Chapter 9 of this document.

9. In cases of uncertainty regarding the implementation or appropriateness of security measures in the computer environment, the Chief Directorate Security of the NIA should be consulted.

CHAPTER 8

PHYSICAL SECURITY MEASURES

Remark: The SA Police Service acts as advisor in terms of physical security measures (see Appendix A).

1. ACCESS CONTROL

1.1 A system of security measures is essential to create an optimal information security environment. Such system naturally is 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.

1.2 Access control is multidimensional. The **different levels or degrees** thereof must be developed and applied according to the degree of safeguarding required. Factors such as the sensitivity of information handled and the degree in which zoning (placement and isolation of certain regions) is/can be implemented play a role in determining these levels/degrees.

1.2.1 The different levels/degrees of access control can vary from the mere locking of offices, with the accompanying access restriction (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.

1.3 Heads of institutions are responsible for the enforcement of the provisions of the Control of Access to Public Premises and Vehicles Act (Act 53 of 1985) for the purpose of safeguarding buildings or premises occupied or used by or under the control of government departments.

1.3.1 Compliance with the provision of Section 2(2), under which the furnishing of information, the furnishing of identification, declarations concerning hazardous objects and the contents of any suitcase, briefcase, handbag, bag, etc, the subjection of persons or objects to electronic examination and the handing over of any object for examination or custody may be required as a prerequisite for effective access control. The searching of persons under Section 2(2)(g) may take place only if the Minister of Safety and Security or his/her delegate (the Commissioner of the SA Police Service) gives authority for this by notice in the Government Gazette.

1.4 In cases where different government departments occupy or use or control different parts of the same building or where different government departments occupy or use or control different parts of the same building together with other institutions, consensus between the heads of departments and the heads of other institutions is a prerequisite for the uniform application of the provisions of the Control of Access to Public Premises and Vehicles Act. Where government departments or other institutions apply the provisions of the Act, notices should be displayed to inform members of the public who wish to gain access in a reasonable manner that the Act is being applied.

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

2. KEY CONTROL AND COMBINATION LOCKS

2.1 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 and safes or strongrooms 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 (see Chapter 4, paragraphs 10.7 and 10.8).

3. MAINTENANCE SERVICES, REPAIRS AND THE CLEANING OF BUILDINGS/OFFICES

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

4. CONTINGENCY PLANNING

4.1 Institutions must make provisions for contingency planning (see Chapter 2 "Definitions") aimed at preventing and/or combating any disaster or emergency. The contingency plan must be geared for saving lives, safeguarding property and information and ensuring that activities can continue with as little disruption as possible.

4.2 These aims can be achieved only through well-organised action in which all the available means and manpower are used in a co-ordinated and effective way to put preventative and/or control measures into operation, and through regular practise of the contingency plan.

CHAPTER 9

BREACHES OF SECURITY

1. Heads of security or those tasked with the security responsibility of an institution 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 Chief Directorate Security of the National Intelligence Agency, and where appropriate to the SAPS (Crime Prevention Unit) or the SANDF (MI) (see Appendix A). Where official encryption is concerned, a security breach must also be reported to the South African Communication Security Agency (SACSA).

2. When a breach of security occurs, the existing channels must be used to report it. It is the responsibility of the head of the institution to ensure that all breaches of security are reported.

3. 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 unnecessarily done an injustice to.

APPENDIX A

DIVISION OF RESPONSIBILITIES WITH RESPECT TO THE PRACTICE OF PROTECTIVE SECURITY IN THE RSA

Note : This appendix serve only to reflect the situation regarding the division of responsibilities, as agreed upon and approved elsewhere and in other documentation. This appendix therefore has no legal standing and is subject to alteration whenever the original agreements are amended.

NATIONAL INTELLIGENCE AGENCY	SA SECRET SERVICE
• Responsible for its own physical and information security	• Responsible for its own physical and information security
• Advises, co-ordinates, audits and exercises control with regard to information security in the public, parastatal and private environment in South Africa (excluding SASS, SAPS and SANDF responsibilities).	• Advises, co-ordinates and exercises control with regard to physical, personnel and document security abroad (excluding SAPS and SANDF responsibilities)
• Advises, co-ordinates and exercises control with regard to physical security within NIA and as far as it relates to information security, also in the public, parastatal and private environment	• Advises and exercises control with regard to physical security at missions abroad
• Carries out security screening of NIA personnel as well as screening investigations abroad if necessary	• Carries out security screening of SASS personnel as well as security interviews and screening investigations abroad at the request of NIA
• Advises, co-ordinates and exercises control with regard to technological security abroad	

SA POLICE SERVICE

- Responsible for its own physical and information security
- Advises, co-ordinates and controls physical security in South Africa, excluding the NIA, SASS and the SANDF, with the aim of preventing crime
- Security screenings in respect of the government and parastatal environment, excluding NIA, SASS and SANDF personnel
- VIP protection in South Africa.

SA NATIONAL DEFENCE FORCE

- Responsible for its own physical and information security and that of Armscor
- Carries out security screening of its own personnel and those of the Armscor family.
- Administers the National Key Points Act
- Facilitates the South African Communication Security Agency

OATH OF SECRECY

I, ...

(full name)

solemnly declare that

1. I have taken note of the provisions of the Protection of Information Act (Act 84 of 1982) and in particular of the provisions of section 4 of the Act;

2. 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 reasonably know that the security or other interests of the 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 interests 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;

3. 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

4. I am fully aware of the serious consequences that may follow any breach or contravention of the said provisions and instructions.

(Signature) .....
(Place) .....
(Date) .....

WITNESSES 1. .....

2. .....

APPENDIX C

APPENDIX D