# Standing Security Instructions for Government Departments and Offices

## CONTENTS





PARLIAMENT OF KENYA LIBRARY

KENYA NATIONAL ASSEMBLY
cession: 10013782
all No: 342.0684 KEN

CHAPTER ONE

# *Introductory*

## THE THREATS TO CLASSIFIED INFORMATION AND MATERIAL—THE APPLICATION OF COMMON SECURITY STANDARDS

**Definition of Security**

1. In the context of this Manual "security" means the safeguarding of classified information and material.

**The Threats**

2. The two major threats to official secrets are espionage and leakage. Whilst the former poses the greatest danger to National Security, it is safe to say that leakage as a result of carelessness or indiscretion in speech or the handling of classified information is the most common means by which official secrets are compromised.

3. The danger of espionage springs mainly from the activities of the Intelligence Services of foreign powers. These services are continually at work collecting information for intelligence purposes and making a sustained effort to break through our security defences by espionage. Amongst methods likely to be used are the recruitment of agents on ideological grounds or by corruption and blackmail, the use of technical methods for telephone interception, eavesdropping and overlooking etc. No department, whatever its sphere of activity, is immune from attack. No one with actual or potential access to classified material is too unimportant to be cultivated either as a useful contact or possible source of information.

4. In addition there is the constant need to guard against the threat of economic and industrial espionage. Here the threat is posed by those persons with business, financial or sectional interests who could gain unfair advantage, or even endanger the economy of the country, by the exploitation of inside knowledge of secret Government policies and intentions.

5. Of the many ways in which official information can leak out, perhaps careless talk is the most common. Discussion of official information with or in earshot of those who do not need to know, indiscreet telephone conversations and a desire to impress an outsider with one's knowledge of Government affairs, can all have serious repercussions. Carelessness in the handling and transmission of classified information and lack of knowledge of correct security procedures also account for an alarming amount of leakage.

6. A further potential threat to security is posed by subversive or anti-Government groups or individuals within the Republic. Such groups or individuals may try to acquire classified information with a view to using it as anti-Government propaganda or disseminating it in any way which will bring Government into disrepute.

**Common Standards of Security**

7. In order to combat the threats to security it is essential that a common security standard is observed by all Ministries/Departments of the Government. No system of security yet devised can guarantee the complete protection of every item of classified material. However, when a common standard is applied, information can be passed from one Department to another with the confidence that it will at least be handled with equal care by the new recipients.

8. This Manual lays down the principles upon which the common standards must be based. Whilst the security requirements of some Ministries/Departments are greater than others, it is emphasized that the standards laid down herein are the minimum common standards and must be implemented in full wherever practicable.

CHAPTER TWO

# *Departmental Security Arrangements*

**Responsibility for Security**

1. Every civil servant and member of the Security Forces has an individual responsibility for security. The Head of every Ministry/Department is responsible for the formulation of general security policy within his Ministry/Department and should give a firm lead in security matters. Advice and guidance may be sought from the Government Protective Security Officer.

**Appointment of Departmental Security Officers**

2. To deal adequately with the day to day working of security arrangements, the Head of every Ministry/Department must appoint a Departmental Security Officer; in a small office however he may perform the function himself.

3. Under the authority of the Head of the Ministry/Department, the Departmental Security Officer is responsible to the Government for security arrangements in his Ministry, Department, Provincial or District Headquarters, as the case may be. The Security Officer at Ministry level supervises Security Officers at Provincial level and so on.

4. The duties of a Security Officer are:—

(*a*) to organize adequate security within the Ministry/Department;

(*b*) to ensure the observance in the Ministry/Department of all Security Instructions;

(*c*) to ensure the security of Government buildings and property;

(*d*) to ensure that all officers subject to the vetting procedure have been security vetted;

(*e*) to take action where there has been a breach of security;

(*f*) to maintain Departmental Security Files on all persons with access to "Top Secret" and "Secret" material; (*See* Chapter IV, para. 3);

(*g*) to liaise in Nairobi with the Government Protective Security Officer on security matters;

(*h*) to liaise in the Provinces and Districts with the appropriate Special Branch Officer on security matters;

(*i*) to provide Security Education for personnel within their departments.

**Departmental Security Instructions**

5. In all Ministries, and in the larger Departments, Departmental Security Instructions should be issued under the authority of the Permanent Secretary/Head of Department. Instructions should be clear and concise and should detail the methods of implementation in the Ministry/Department of the Government Security Instructions.

**Security Education**

6. Security precautions, if they are to be effective, must be understood by the people who are to carry them out. This is where the need for Security Education arises:—

The objects of Security Education are:—

(*a*) to convince the individual employee of the need for security;

(*b*) to instruct him in the correct procedures and requirements;

(*c*) to ensure that he will remember these procedures and requirements.

(Security Education should not be confused with Security Training, which is the professional training of those with direct security responsibilities).

7. To the average civil servant security procedures often mean extra work with little or no visible result; in other words they appear non-productive. It is essential that the particular security threats affecting his work are explained to the individual officer; also those aspects of the material he handles requiring security protection.

**Methods of Security Education**

8. The responsibility for Security Education within a Ministry/Department rests with the Departmental Security Officer. He can, according to Departmental requirements, utilize various methods. Suggested media are:—

(i) *Lectures.*—These should be illustrated wherever possible with departmental examples or case histories. Questions and discussions should be encouraged with the object of clearing up any misunderstanding of security regulations.

(ii) *Informal Talks to Small Groups* can be useful when:—

(*a*) convincing senior officers of the importance of security measures;

(*b*) introducing staff to the security requirements of a special task;

(*c*) dealing with groups with specialized security problems;

(*d*) dealing with staff who are not used to being lectured and respond better to an informal approach.

(iii) *Individual Talks.*—These are of special value when an employee is first appointed to secret work or is posted to a job with special security responsibilities. Such talks are also particularly effective when an employee is being reprimanded for a breach of security.

(iv) *Staff Circulars.*—These can be usefully employed either to draw attention to a particular breach of security and its consequences, or to a general security weakness.

(v) *Security Posters.*—These may be obtained from:—

The Director of Intelligence, P.O. Box 30091, NAIROBI.

CHAPTER THREE

# *The Classification of Official Documents*

**Use of Classification System**

1. An official document must be protected if harm would result from the disclosure to an unauthorized person of the information it contains. Not all documents require the same protection, so there are four grades of classification:— "TOP SECRET", "SECRET", "CONFIDENTIAL" and "RESTRICTED". Documents bearing a security classification are known collectively as "classified documents".

**Definitions of Security Classifications**

2. (*a*) *Top Secret.*—Information and material, the unauthorized disclosure of which, would cause exceptionally grave damage to the Republic.

(*b*) *Secret.*—Information and material, the unauthorized disclosure of which, would cause serious injury to the interests of the Republic.

(*c*) *Confidential.*—Information and material, the unauthorized disclosure of which, would be prejudicial to the interests of the Republic.

(*Note*: Confidential Personal Files etc., are in a different category and should be clearly marked "Staff, Confidential", or "Staff in Confidence" etc.).

(*d*) *Restricted.*—Information and material, the unauthorized disclosure of which, would be undesirable in the interests of the Republic.

**Responsibility for Classification**

3. The originator of a document is the person responsible for allocating the appropriate security classification. Committees must nominate a responsible officer, normally the committee secretary, to classify their agenda and minutes etc. Under no circumstances should classification be left to the discretion of typists or personal secretaries.

4. An officer once having decided upon the appropriate classification for a document is responsible for ensuring that correspondence is correctly prepared and despatched according to his instructions.

**Classification of Documents and Files**

5. (*a*) The classification of a document is determined solely on its contents, not the classification of the file upon which it is written.

(*b*) The classification of a file should be the same as that of the highest classified document enclosed therein.

(*c*) The classification of a paper with appendices or enclosures should be that of the highest classification.

(*d*) There is no need to give a subsequent document a classification as high as that of an earlier document to which it refers or quotes, provided the quotation is limited to the reference number, the date, and matter not on its own justifying a classification as high as the original letter.

**Overgrading**

6. Persons concerned with the classification of documents must guard against a natural tendency to over-classify. Use of an unduly high classification causes extra work all round and can lead to a general disregard of documentary security procedures thus giving "security" a bad name.

7. Staff should be encouraged to report to their superiors any obvious instances in which they consider a classification has been omitted or incorrectly used. Senior officers should check classifications either when reading "float" copies of documents or by periodical examination of letter books.

**Downgrading and Declassifying**

8. Ministries/Departments should carry out a periodic review of all classified material to see if the passage of time justifies its being downgraded or declassified. No document received from another Ministry/Department may be downgraded or declassified without the written permission of the originator.

**Access to Classified Material**

9. Only persons who have been security vetted are permitted to handle classified material, and may only handle that grade of material for which they have been cleared.

10. The typing, duplication or copying of classified material may also only be carried out by a person security vetted.

**Codewords**

11. A Codeword is a word used to provide security cover for a particular classified matter. All Codewords are drawn from the Operational Codeword Index held by the Director of Intelligence, to whom application must be made when Codewords are required.

**Nicknames**

12. A nickname does not provide security cover and may be used for administrative convenience for unclassified matters. To avoid confusion with Code-Words, a nickname should always consist of two separate words.

**Accountable Documents**

13. A document may be made an "Accountable Document", in which case the holder is required to certify its safe custody at least once a year. To be made accountable a document should normally:—

(*a*) be classified "TOP SECRET", "SECRET" or "CONFIDENTIAL", with the likelihood that it will retain that classification for a substantial period;

(*b*) bear a serial number and an individual copy number;

(*c*) be of the nature of a manual, work of reference or set of instructions, that is, the sort of document which is often bound in a stiff cover, sometimes loose-leafed, and to which amendments are issued from time to time.

CHAPTER FOUR

# *Access to Classified Material*

**The "Need to Know" Principle**

1. Access to classified material must at all times be restricted on the "Need to Know" principle, that is, no person is entitled, solely by virtue of his rank or appointment, to knowledge of classified material. The "Need to Know" is the essential principle.

**Employment of Staff on "CONFIDENTIAL", "SECRET" or "TOP SECRET" Work**

2. No one may be employed on "CONFIDENTIAL", "SECRET" or "TOP SECRET" work without prior security clearance (security vetting) by the Director of Intelligence. The full vetting procedure is laid down in "Secret" Circular reference GEN. 168/390/001A (141), dated 23rd August, 1967, and issued by Permanent Secretary, Office of the President.

**Access to "SECRET" or "TOP SECRET" Work**

3. Subject to the provisions of the preceding paragraph, no one may be employed on "SECRET" or "TOP SECRET" work without the authority of the Head of Department concerned. The Departmental Security Officer should maintain a separate security file for every person authorized to handle "SECRET" or "TOP SECRET" material. (Chapter II, para. 4 (*f*)). Security Files should contain only:—

(*a*) Form PSC.2 or its earlier equivalent.

(*b*) The Official Secrets Act Declaration signed by the person concerned.

(*c*) The form issued by the Director of Intelligence showing what degree of classification a person may handle.

(*d*) Reports and comments by the Permanent Secretary/Head of Department on any breach of security caused by the person.

4. When an officer is transferred from one Ministry/Department to another his Security File should be sent to the Security Officer of his new office.

CHAPTER FIVE

# *The Preparation, Transmission, Receipt and Destruction of Classified Files and Documents*

## GENERAL

**Marking of Classified Documents**

1. Every page of a classified document must clearly show the security classification of the document at top and bottom. Every copy of a "TOP SECRET", or of a more important "SECRET" document must be given a copy number and a distribution list should be retained. Appendix "A" sets out a model procedure which should normally govern the production and recording of "SECRET" and "TOP SECRET" papers.

**Circulation of Classified Material**

2. The circulation of classified documents must be strictly limited on a "need to know" basis. Committees must always lay down the distribution list of their papers and minutes, and should revise such lists at regular intervals.

**Reproduction of Classified Material**

3. The duplication or reproduction of classified material may only be performed by a person authorized access to the grade of material being handled. A separate room should, wherever possible, be used for duplicating, and all unauthorized persons excluded. All waxes, skins and waste from the duplicating of classified material must be treated in the same manner as classified material.

**Use and Protection of Photocopying Machines**

4. Photocopying and similar machines need careful protection to prevent their use for the illegal copying of classified material. The following precautions must be taken in all Ministries and Departments regularly handling classified material.

(*a*) Machines must be kept in a separate and secure room which can be locked when not in use. Where, in exceptional circumstances, through limitation of accommodation this is not practicable, and the approval of the Director of Intelligence has been obtained, the machine may be immobilized or locked away when not in use.

(*b*) Photographic papers and materials should be held by a responsible officer and issued only to persons authorized to use the machine. Papers and materials should *not* be kept in the same room as the machine.

(*c*) It is desirable, wherever possible, that all photocopying should be done by one or more authorized persons depending upon the degree of usage of the machine within the Ministry/Department. Where this is not practicable, use of machines by secretaries, typists and junior clerical staff should only be permitted when required and or authorized by senior officers.

**Wax Sealing of Envelopes**

5. Wax seals on envelopes should be so placed that no one seam or flap can be opened without at least one seal being broken. The distance between seals should not be more than 4″ apart, and all flaps should be stuck down prior to sealing. The over-filling of envelopes may cause damage to the seals in transit and should therefore be avoided.

**Record of Despatch and Receipt—Filing**

6. An accurate and detailed record must always be kept of classified material graded "CONFIDENTIAL" and above. Acknowledgement of classified documents should be by the full signature of the recipient and never by initials alone.

7. All classified material must be correctly filed immediately upon receipt. It is essential that "TOP SECRET" files should contain file folio sheets recording the details of all classified documents therein. This procedure is also strongly recommended for files classified "SECRET" and "CONFIDENTIAL".

**File Location Cards**

8. When in its place in the Registry, each classified file should contain a file location card. (This is a plain card about the size of the file cover, bearing the file's reference). When a file is sent out of the Registry, the card must be retained by the Registry and the file's destination, and the date of despatch entered on it. The officer receiving the file, or his secretary, should enter the file reference and the date in a file record book.

9. In small offices, or where only a small amount of classified material is handled, an officer passing a file to another officer outside the Registry need only make a record of the destination and the date and time of despatch. In large offices the same details should in addition be entered on a file "transit slip" which must be sent to the Registry, where the file's new location should be entered on the file location card. In this way files can be traced quickly and should one be lost it is easy to ascertain who is responsible.

**Mail List System**

10. Where there is only a small quantity of classified correspondence the person in charge of the Security Registry need only record the despatch and receipt of classified material in Inward and Outward Mail Registers. Where a large quantity of classified material is dealt with it is recommended that the Mail List System, (GPK Form P.135) should be utilized as follows:—

(*a*) Mail Lists should be used to record the despatch and receipt of "SECRET" and "TOP SECRET" correspondence.

(*b*) The despatching office should allot a separate mail list number to each addressee.

(*c*) Each Mail List should consist of three numbers separated by an oblique stroke, e.g. 3/25/69. The first number is the Mail List number of the addressee, the second is the serial number of the Mail List, which must always be in sequence. The third number is the last two figures of the year.

(*d*) On the Mail List should be entered the reference number of the letter or document to which it relates.

(*e*) The letter or document should be enclosed in two envelopes. The inner envelope (wax sealed) should bear the classification, the reference number of the contents and the sender's full address. The Mail List should be attached to the inner envelope. The outer envelope should bear only the full address of the addressee.

(*f*) The Mail List should be made out in duplicate, the flimsy copy being filed.

(*g*) The Post Office registration number should be stuck on the outer envelope, and the Mail List number entered against that number in the Post Office Registered Letters Posted in Bulk Receipt Book. (P.O. Book P.121).

(*h*) Upon return of the Mail List receipt, it should be attached to the filed flimsy copy.

## METHODS OF TRANSMITTING CLASSIFIED FILES AND DOCUMENTS

11. **From Registries to Offices, and Between one Office and another, provided Transmission is within the same building.**

| *Classification* | *Method* |
|---|---|
| (*a*) TOP SECRET | Pouch or metal container fastened with combination padlock, carried by authorized courier. |

| *Classification* | *Method* |
|---|---|
| (*b*) SECRET<br>(*c*) CONFIDENTIAL | (i) Closed envelope or container carried by hand of person authorized access to the material. |
| | (ii) Sealed envelope, showing address, classification and (in lower left hand corner) reference, carried by courier. |
| | (iii) Sealed envelope, showing address, classification and (in lower left hand corner) reference, inside closed envelope showing only the address, carried by Government messenger. |
| | (iv) Sealed envelope, showing address, classification and (in lower left hand corner) reference, inside locked bag, carried by Government messenger. |
| (*d*) RESTRICTED | Closed envelope showing address only, carried by authorized courier or Government messenger. |

12. **To other Ministries, Departments and Offices within the same Town.**

| | |
|---|---|
| (*a*) TOP SECRET | Sealed envelope showing address, classification and reference, transmitted in container, fastened by a combination padlock and carried by an authorized courier. |
| (*b*) SECRET | Sealed envelope showing address, classification and reference, transmitted in locked bag by authorized courier. |
| (*c*) CONFIDENTIAL | (i) As for SECRET. |
| | (ii) Two envelopes, inner sealed showing security classification and reference, outer showing only address and carried by hand of an authorized messenger. |
| (*d*) RESTRICTED | (i) Carried in locked bag by authorized courier. |
| | (ii) Closed envelope with no security classification by hand of authorized messenger. |

13. All classified material despatched by the foregoing methods must be accompanied by a receipt book which should have entered therein details of the addressee and the reference number of the documents concerned. A full signature and office date stamp of the recipient must be obtained.

14. **To a Destination outside the same Town but within the Republic.**

| *Classification* | *Method* |
|---|---|
| (*a*) TOP SECRET | Sealed envelope showing the classification and address, in a locked container, by hand of official courier or, if none is available, by special messenger. *(*See Note*). |
| (*b*) SECRET | By registered post; two envelopes should be used, the inner (sealed) showing the address, classification and reference, and full postal address of sender. The outer closed envelope showing only the address of the addressee. SECRET files should only be transmitted between Provinces and Districts in very exceptional circumstances, when they should be carried in a locked container, by hand of an official authorized to handle the file, or by the method laid down for the carriage of TOP SECRET material detailed above. |
| (*c*) CONFIDENTIAL | Files and documents should be sent by registered post in the manner laid down for SECRET documents. |
| (*d*) RESTRICTED | Letters and documents by ordinary post in a new single envelope with no security classification shown on the envelope. If RESTRICTED files have to be sent they should be registered. |
| *(*Note*: | TOP SECRET letters should never, in normal circumstances, be sent by registered post). |

15. All registered mail should be carried to and from the Post Office in a locked mail bag. The copy of the Post Office registered mail receipt (which is signed at the Post Office on receipt of registered mail) should be retained as a record of the numbers of registered letters despatched.

**Removal of Documents and Files from Offices**

16. TOP SECRET and SECRET documents should not be taken out of the office unless it is absolutely essential. TOP SECRET documents must never be taken home. If an officer has to work on SECRET or CONFIDENTIAL documents at home he must obtain the consent of his Permanent Secretary/Head of Department. When SECRET or CONFIDENTIAL papers are taken home they must be carried in a locked briefcase, clearly labelled with the owner's name and address. At night the papers should be replaced in the briefcase, which must be locked in a secure container in the officer's house, the officer retaining the keys of the container all the time. When an officer takes files or classified papers home he should give a receipt for them to his Security Registry for retention until he returns them.

**Destruction of Classified Material and Waste**

17. In offices where classified material is handled all waste must be treated as classified waste. This includes waste paper, carbon paper, shorthand notebooks, notepads, waxes, blotting paper and typewriter ribbon. Classified waste should only be destroyed by shredding or burning. When it is burned the waste should be reduced to ashes and the ashes broken up. Classified material should only be destroyed by a person authorized to handle all the matter for destruction and no one who is not authorized to handle it should be present. If classified waste is not destroyed at the end of a working day it must be locked away in a security container. In offices which handle classified material, recording tapes must always be regarded as classified material. When TOP SECRET material is destroyed a certificate should be sent to the originator stating the date and manner of destruction. In addition, when complete SECRET or TOP SECRET files are destroyed a check should be made that no folios are missing from the file, and an account should be kept of all such files destroyed showing the date and manner of destruction, and a certificate that the files were complete on destruction.

CHAPTER SIX

# *Custody of Classified Documents, Security Containers, and Security of Keys and Combination Locks*

**Buildings**

1. Documents classified "TOP SECRET" or "SECRET" will normally only be housed in protected premises, that is, buildings which are under security guard throughout the twenty-four hours and which normally cannot be entered by unauthorized persons unless escorted. Where these conditions do not prevail, the documents may be stored only in a proper steel safe set in concrete or within a properly constructed strongroom or registry fitted with steel doors and security locks.

**Containers**

2. All documents classified "CONFIDENTIAL" and above must be locked up in security containers when not in use. Normally, "RESTRICTED" documents should be kept under lock and key. The following minimum standards must always apply:—

**TOP SECRET**

(i) Steel safe fitted with keyless three wheel combination lock or key lock fitted with combination blister.

(ii) Lockable steel filing cabinet or cupboard housed within a properly constructed steel doored Registry/Strongroom.

**SECRET**

Steel filing cabinet fitted with steel locking bar, hasp and staple secured by an approved padlock or keyless combination lock.

**CONFIDENTIAL**

As for "SECRET" except that in unprotected premises filing cabinets should be secured to a stone wall by bolting through the rear panel.

**RESTRICTED**

(i) Lock and key.

(*Note*: Lockable wooden containers, i.e. desk drawers, stationary cupboards, filing cabinets etc., may *NOT* be used for any material other than that classified "RESTRICTED").

**Security Keys and Combinations**

3. A security key or "combination" is one which gives access to a container of any description holding classified documents or material.

**Compromise of Keys and Combination Settings**

4. Duplicate keys can easily be made by an expert. An impression or photograph of a key can be taken in a few seconds by a person with only limited technical knowledge. It is essential therefore that unauthorized persons never have the opportunity of handling or examining security keys.

5. Combination Lock settings may be compromised in several ways, particularly if an unauthorized person is able:—

(*a*) to remove the cover of the back of the lock and examine the inside;

(*b*) to overlook the operation of opening the lock;

(*c*) to read a written record of the setting.

**Issue and Recording of "Security Keys"**

6. Security keys should be issued against signature to individual members of staff. A register should be maintained recording the whereabouts of each security key, including spares, together with a note of the lock or container to which they belong.

**Safe Custody of "Security Keys"**

7. "Security Keys" when not in use should be locked away in a Combination Wall Key Safe or security container. Only those persons allowed access to the keys should know the combination of the Key Safe or container.

8. Only in very exceptional circumstances should keys be taken out of the office. Such keys should be placed on a key ring attached to a chain; they should not leave the possession of the owner even for a short period and must be kept securely at all times. They should not be marked or labelled since, although this makes recovery of a lost key unlikely, it lessens the risk of a finder or thief making improper use of it.

9. All spare security keys should be held by the Departmental Security Officer. They should be stored in a Key Safe or security container to which only the Departmental Security Officer should have access. Spare keys to safes are held centrally by the Treasury for Ministries/Departments in Nairobi and by Provincial Accountants for Provinces and Districts.

**Loss of Security Keys**

10. The loss of a security key should be reported at once to the Departmental Security Officer for investigation. Any container of which the key

is lost must be considered as technically compromised, and the contents stored elsewhere, until the lock or locks are changed. Even if the key is subsequently recovered the container must still be regarded as compromised unless it is established beyond reasonable doubt that there has been no opportunity for an unauthorized person to copy it.

**Changing Combination Settings**

11. Combination settings should be changed:—

(*a*) when a container or lock is first received by a department;

(*b*) when a person knowing the combination ceases to have authorized access to the contents of the container to which the lock is fitted, for example, on retirement, transfer or dismissal of personnel etc.;

(*c*) when a combination is thought to have been compromised;

(*d*) when a combination has been set for six months.

**Hand-Over/Take-Over Certificates**

12. All Government officers in charge of departments, branches, offices or registries where classified material is kept should, on relinquishing their appointments, render hand-over/take-over certificates to the Head of the Department concerned. The certificates should mention the following:—

(*a*) The responsibilities of the appointment, in so far as it affects all aspects of the handling and protection of classified material.

(*b*) Details of classified files.

(*c*) Details of accountable documents.

(*d*) Details of codes and ciphers.

(*e*) Details of keys to safes and steel filing cabinets.

CHAPTER SEVEN

# *Security of Buildings*

**Responsibility**

1. The responsibility for the safeguarding of Government buildings and their contents rests with the department in occupation. Where a building is shared, the Heads of the Ministries/Departments concerned should discuss and agree upon the apportionment and co-ordination of security responsibilities.

2. The security requirements of Ministries/Departments vary greatly; no rules can be laid down governing internal protective arrangements for all Government buildings, but the following suggestions should be adapted to meet differing needs.

**Control of Access**

3. The Departmental Security Officer should make a survey of all possible means of access to the building in which his Department is located including all doors and other entrances, ground floor windows, etc., and recommend measures to exclude casual intruders. Much can be done to increase the security of buildings by admitting visitors through one entrance only and controlling their movements within the building. Where a Government Ministry/Department shares premises with another Government Ministry/Department or a non-Government organization, control of access should be exercised at the entrance to each floor or landing occupied by the Government Ministry/Department. Particular care must be exercised to ensure that visitors to offices do not gain sight of classified material.

**Door-Keepers and Security Guards**

4. Great care should be exercised in the selection for employment of door-keepers and security personnel (guards, watchmen, etc.). Careful checking of background and previous employment is essential and in cases where doubt arises as to a person's antecedents or suitability, security vetting should be carried out.

5. Door-keepers and security personnel should have precise written instructions from the Departmental Security Officer as to their duties and responsibilities. They must at all times be made to feel that they will have the support of the Permanent Secretary/Head of Department in the correct execution of their duties. Night-watchmen should have access to a telephone or other means of communication in order to be able to summon assistance in the event of trouble. Periodic checks at irregular hours should also be made by either human or mechanical means (clock recording systems) to ensure that watchmen are alert.

**Passes**

6. A pass system can be a useful aid to security, particularly in large Ministries/Departments and in those containing sensitive areas or a large concentration of classified material. Passes can broadly be divided into two classes, for example, permanent passes for employees in the Ministry/Department and temporary passes for visitors.

**Permanent Passes**

7. The following precautions should be taken in the production of passes:—

(*a*) the pass should be of coloured or patterned paper and not capable of being easily copied;

(*b*) passes should be serially numbered;

(*c*) a current photograph and/or the signature of the holder should be affixed;

(*d*) where possible the pass should be stamped or embossed with a prominent hieroglyphic not capable of being easily copied;

(*e*) the pass should not indicate which Ministry/Department issued it nor to which building it gives access;

(*f*) sealing (laminating) in plastic will prevent tampering.

8. Passes should be issued against signature and a record kept of all holders. Persons leaving the Ministry/Department on transfer, etc., must hand in their Passes.

**Temporary Passes**

9. Every visitor not in possession of a valid Permanent Pass admitting him to a building, whether he be an officer of another department or a member of the public, should be provided with a Temporary Pass. Passes should be serially numbered and produced in duplicate (*see* specimen at Appendix "B"). The Temporary Pass should be signed by the officer visited, who is also responsible for seeing that the visitor leaves the building when his business is concluded. At the end of each working day the Passes must be checked against the duplicates and the reason for any missing Passes investigated. It is recommended that all used Temporary Passes be retained for a period of two months before destruction.

**Security of Offices**

10. All office windows must be closed and fastened at the end of the day by the occupier. As a general rule office doors should be left open as a fire precaution and to facilitate inspection by night-watchmen. The keys of any doors left open must be locked away in a secure container.

11. At the end of each working day a room check should be carried out in each office to ensure that:—

(i) no classified documents have been left lying about unprotected;

(ii) all classified waste has been locked away or destroyed;

(iii) all safes and security containers are closed and locked;

(iv) all outside windows are shut.

CHAPTER EIGHT

# *Personal Security and "Secure Behaviour"*

**The Initiation of a Secret**

1. All secrets are initiated by man and therefore the first thing to guard against are human weaknesses and vices. Man's carelessness and indiscretions, his vanity and curiosity, and the exploitation of his vices or moral weaknesses can all lead to breaches of security.

**Careless Talk**

2. Careless talk and indiscretions amongst family, friends, acquaintances and even fellow workers must be guarded against at all times. Conversations can often be overheard where offices have ill-fitting doors, thin partition walls or open fanlights. Great care must be taken to ensure that conversations in conference rooms cannot be overhead from outside the door or through open windows. Vanity—the desire to impress by one's knowledge and curiosity—the desire to find out more than one needs to know, can both lead to breaches of security.

**Vices and Moral Weaknesses**

3. The exploitation of vices or moral weaknesses is perhaps one of the most successful, though difficult to guard against, methods of extracting secrets. Bribery, corruption and blackmail are commonly used methods. Homosexuality, illicit sex, criminal activities, indebtedness, gambling, drunkenness and extravagances are weaknesses which are all exploitable by a determined agent in search of secrets.

4. From the foregoing it can be seen that good personal behaviour, both during and out of office hours, is of paramount importance amongst officers with access to classified material. Any cases of insecure behaviour or obvious moral laxity should be treated as a potential threat to security and investigated thoroughly.

**Use of Telephone**

5. No form of telephone conversation, whether by ordinary or radio telephone is secure. The principle risk of leakage arises from casual interception by cross-connexion and the possibility of telephone operators and engineers overhearing conversations in the performance of their duties. Deliberate telephone interception is a risk that cannot be disregarded, and therefore the general rule must always be the TELEPHONE IS NOT SECURE.

6. The "secraphone" or "scrambler" used by certain Ministries/Departments affords only a very limited degree of security; an expert with the proper facilities or even a trained listener can intercept and "de-scramble" at least parts of "scrambled" conversations.

7. From the foregoing it is essential to realize that classified information should only be conveyed by telephone when the need for speed outweighs the need to guard against leakage. Even so, every effort should be made to render the conversation as obscure as possible to an eavesdropper. Great care must be exercised in telephone conversations to foreign countries, particularly with our missions and representatives abroad where the likelihood of deliberate interception is far greater than within Kenya.

**Information to the Press**

8. Great care must be taken to avoid unauthorized or premature disclosures to the Press. The problems involved are dealt with at length in Regulations D.23 and G.7 of the Code of Regulations, and any officer who is likely to have dealings with the Press must make himself familiar with these regulations.

9. By the very nature of their profession journalists become extremely adept in building up a story from seemingly unconnected scraps of information. Civil Servants must ensure that they do not unwittingly become quoted as "the Government spokesman" or "a normally reliable Government source".

**Pen Friends and Overseas Correspondents**

10. Officers who maintain "pen friends" or similar correspondence with persons or organizations overseas must, at all times, be alert to the possibility of themselves being used or cultivated as a possible source of information. Any attempt by an overseas correspondent to obtain official information of any description should be reported to the Permanent Secretary/Head of Department or Departmental Security Officer.

**Unofficial Questionnaires**

11. No civil servant should reply to an unofficial questionnaire, from whatever source, which requires information about his position in Government; nature of work carried out or any other information relating to his employment. This does not, of course, preclude a civil servant from giving potential new employers sufficient details of his experience.

**Duty to Report Suspicious Incidents and Breaches of Security**

12. It is the duty of every civil servant to report to his superior any breach of security or suspicious incident, or any attempt, by persons outside Government to obtain official information to which they are not entitled.

CHAPTER NINE

# *Breaches of Security*

**General**

1. No practicable system of security can afford complete protection against the skilled agent; it can only make his task more difficult. When security is compromised, however, the existence of an efficient security system greatly aids investigations, by bringing to early notice the fact that something has gone wrong and by narrowing the field of enquiry.

2. When a breach of security occurs it must at once be reported to the Departmental Security Officer whose objectives will be:—

(*a*) to find out what happened;

(*b*) to minimize the danger done;

(*c*) to prevent a recurrence.

3. Departmental Security Officers or other persons investigating breaches of security should report all serious cases in Nairobi to the Government Protective Security Officer and in the Provinces and Districts to the nearest Special Branch Officer at the earliest possible moment.

**All Officers must be Security Conscious**

4. The contravention of any security regulation is a breach of security. Every Government employee whatsoever his rank must at once report to the Departmental Security Officer any breach of security, however trivial. Only if all the employees are security conscious, and all breaches of security thoroughly investigated, can these instructions be enforced and Government secrets safeguarded.

CHAPTER TEN

# *The Official Secrets Act*

**No. 11 of 1968**

**General Principles**

1. The Official Secrets Act provides for the preservation of State Secrets and State Security. Insofar as official information is concerned the general object of the Act is to prevent unauthorized persons from obtaining information relating to official matters.

**Declaration Under the Act**

2. It is the duty of every Permanent Secretary/Head of Department to ensure that every person who has access to classified material signs the requisite declaration under the Official Secrets Act.

**Official Secrets Act 1968**

3. Part II, Section 3 of the Official Secrets Act 1968 governs certain responsibilities of Government Servants and others. They are reproduced at Appendix "C". All Government employees should study this Act in relation to the Official Secrets Act Declaration Form (reproduced at Appendix "D") which they sign on appointment. Also reproduced at Appendices "E", "F" and "G" respectively, are the Declaration Forms to be signed by Civil Servants on leaving the service of Government and, in certain circumstances, by persons outside Government service on obtaining, or ceasing to have, access to classified information.

*APPENDIX "A"*

## MODEL PROCEDURE FOR THE PRODUCTION AND RECORDING OF DOCUMENTS CLASSIFIED SECRET AND TOP SECRET

Only persons who have been cleared by the Director of Intelligence for access to material classified Secret, or Top Secret, may type or duplicate papers so classified. No person not so cleared should be permitted to assist or attend in the duplication of such material.

2. Top Secret documents should always be given copy numbers, and a record of each copy produced and of its location should be kept, by means of a distribution list. Spares should likewise be numbered. In addition, the following certificate (with only such minor modifications as the sense may demand) should be typed on the file copy of the distribution list, and signed and dated by the person who typed or duplicated the document:—

> Certified that this list is complete and that all other copies, parts of copies, drafts, etc., have been destroyed by me personally. The stencils* have been destroyed/are held by me.
>
> (*Signed*) .....
>
> *Where applicable (*Date*) .....

3. Secret documents likewise require a record of the numbers produced to be maintained, as follows:—

(*a*) *Typed Secret Documents.*—The total of original and copies should be shown at the bottom, at least on the file copy, adjacent to the initials of the person who typed the document. (Such initials are commonly shown in any case, in conjunction with the initials of the originator of the document). The result might be, e g. "ABC/DEF (4)".

(*b*) *Duplicated Secret Documents.*—To the file copy should be attached a summary of the number of copies produced and a certificate (which may require subsequent amendment) regarding stencils, spares, etc., as in the following example:—

| | |
|---|---|
| Distribution .. .. .. .. .. .. | 12 |
| File .. .. .. .. .. .. .. | 1 |
| Spares .. .. .. .. .. .. .. | 3 |

Stencils destroyed/held by me.

Certified that this list is complete.

(*Signed*) .....

(*Date*) .....

4. The procedure outlined above need not apply to Confidential documents. The practice should become automatic and need make for little extra work. It is the only practicable system whereby in the event of a breach of security an estimate can at once be made of the number and location of Secret or Top Secret documents involved.

*APPENDIX "B"*

MINISTRY/DEPARTMENT:—

..... TEMPORARY DAY PASS No. .....

Name of Visitor .....

Officer Required .....

Purpose of Visit .....

Time In ..... a.m./p.m.

Time Out ..... a.m./p.m.

Date .....

Officer's Signature .....

This Pass must be returned to the Security Guard when leaving the building

*APPENDIX "C"*

## EXTRACTS FROM THE OFFICIAL SECRETS ACT 1968

*(printed on the back of Declaration Forms shown at Appendices "D" to "G")*

PART II, SECTION 3 OF THE OFFICIAL SECRETS ACT 1968 provides as follows:—

3. (1) Any person who, for any purpose prejudicial to the safety or interests of the Republic:—

(*a*) Approaches, inspects, passes over, is in the neighbourhood of or enters a prohibited place; or

(*b*) makes any plan that is calculated to be or might be or is intended to be directly or indirectly useful to a foreign power or disaffected person; or

(*c*) obtains, collects, records, publishes or communicates in whatever manner to any other person any code word, plan, article, document or information which is calculated to be or might be or is intended to be directly or indirectly useful to a foreign power or disaffected person,

shall be guilty of an offence.

(2) Any person who takes a photograph of a prohibited place or who takes a photograph in a prohibited place, without having first obtained the authority of the officer in charge of the prohibited place, shall be guilty of an offence.

(3) Any person who has in his possession or under his control any code word, plan, article, document or information which:—

(*a*) relates to or is used in a prohibited place or anything in a prohibited place; or

(*b*) has been made or obtained in contravention of this Act; or

(*c*) has been entrusted in confidence to him by any person holding office under the Government; or

(*d*) has been entrusted in confidence to him owing to his position as a person who holds or has held a contract made on behalf of the Government or a contract the performance of which in whole or in part is carried out in a prohibited place, or as a person who is or has been employed under a person who holds or has held such an office or contract,

and who for any purpose or in any manner prejudical to the safety or interests of the Republic:—

(i) uses the code word, plan, article, document or information; or

(ii) retains the plan, article or document in his possession or under his control when he has no right so to retain it or when it is contrary to his duty so to retain it, or fails to comply with all directions issued by lawful authority with regard to its return or disposal,

shall be guilty of an offence.

(4) Any person who, having in his possession or under his control any plan, article, document or information that relates to munitions of war, communicates it directly or indirectly to any foreign power, or to any other person for any purpose or in any manner prejudical to the safety or interests of the Republic, shall be guilty of an offence.

(5) Any person who receives any code word, plan, article, document or information, knowing or having reasonable grounds for believing at the time when he receives it, that the code word, plan, article, document or information is communicated to him in contravention of this Act, shall be guilty of an offence, unless he proves that the communication to him of the code word, plan, article, document or information was contrary to his wishes.

(6) Any person who has in his possession or under his control any code word, plan, article, document or information of a kind or in the circumstances mentioned in paragraphs (*a*) to (*d*) inclusive of subsection (3) of this section, and who:—

(*a*) communicates the code word, plan, articles, document or information to any person, other than a person to whom he is authorized to communicate it or to whom it is his duty to communicate it; or

(*b*) retains the plan, article or document in his possession or under his control when he has no right so to retain it or when it is contrary to his duty so to retain it, or fails to comply with all directions issued by lawful authority with regard to the return or disposal thereof; or

(*c*) fails to take reasonable care of, or so conducts himself as to endanger the safety of, the code word, plan, article, document or information,

shall be guilty of an offence and liable to imprisonment for a term not exceeding five years.

(7) Any person who:—

(*a*) allows any other person to have possession of any official document issued for his use alone, or communicates to any other person any code word so issued; or

(*b*) without lawful authority or excuse, has in his possession any official document or code word issued for the use alone of some person other than himself; or

(*c*) on obtaining possession of any official document by finding or otherwise neglects or fails to restore it to the person or authority by whom or for whose use it was issued or to a police officer,

shall be guilty of an offence and liable to imprisonment for a term not exceeding five years.

PART IV, SECTION 20 OF THE OFFICIAL SECRETS ACT 1968 provides as follows:—

(20) Any person who is guilty of an offence under this Act for which no penalty is specifically provided shall be liable to imprisonment for a term not exceeding fourteen years.

*APPENDIX "D"*

REPUBLIC OF KENYA

---

## OFFICIAL SECRETS ACT 1968

---

### To be Signed by Civil Servants on Appointment

My attention has been drawn to the provisions of the Official Secrets Act which are set out on the back of this document, and I am fully aware of the serious consequences which may follow any breach of those provisions.

I understand that the sections of the Official Secrets Act, set out on the back of this document, cover material published in a speech, lecture, or radio or television broadcast, or in the Press, or in book form. I am aware that I should not divulge any information gained by me as a result of my appointment, to any unauthorized person, either orally or in writing, without the previous official sanction in writing of the Department appointing me, to which written application should be made and two copies of the proposed publication be forwarded. I understand also that I am liable to be prosecuted if I publish without official sanction any information I may acquire in the course of my tenure of an official appointment (unless it has already officially been made public) or retain without official sanction any sketch, plan, model, article, note or official documents which are no longer needed for any official duties, and that these provisions apply not only during the period of my appointment but also after my appointment has ceased.

Witnessed ..... Date .....

Signed .....

*APPENDIX "E"*

REPUBLIC OF KENYA

## OFFICIAL SECRETS ACT 1968

### To be Signed by Civil Servants on Leaving the Service of the Government

My attention has been drawn to the provisions of the Official Secrets Act which are set out on the back of this document, and I am fully aware of the serious consequences which may follow any breach of those provisions.

I understand:—

(1) that the provisions of the Official Secrets Act apply to me after my appointment has ceased;

(2) that all the information which I acquired or to which I have had access owing to my official position is information which is covered by section 3 of the Official Secrets Act, 1968, and that the Official Secrets Act applies to all such information which has not already officially been made public;

(3) that the sections of the Official Secrets Act set out on the back of this document cover material published in a speech, lecture, radio or television broadcast or in the Press or in book form or otherwise, and that I am liable to be prosecuted if either in Kenya or abroad I communicate, either orally or in writing, including publication in a speech, lecture, radio or television broadcast or in the Press or in book form or otherwise, to any unauthorized person any information acquired by me as a result of my appointment (save such as has already officially been made public) unless I have previously obtained the official sanction in writing of the Department by which I was appointed;

(4) that to obtain such sanction, two copies of the manuscript of any article, book, play, film, speech or broadcast, intended for publication, which contains information which I have acquired or to which I have had access owing to my official position, or of any material otherwise to be published which contains such information, should be submitted to the Head of the Department;

(5) that when my appointment ends I should surrender any sketch, plan, model article, note or document made or acquired by me during the tenure of the appointment (even if such sketch, plan, model, article, note or document is not classified) save such as I have been officially sanctioned in writing by the Department to retain, and that I am liable to be prosecuted if I retain any sketch, plan, model, article, note and document without such official sanction.

Signed .....

Surname (BLOCK LETTERS) .....

Forename(s) .....

Date of Birth .....

Permanent (home) address .....

(*Date*) .....

Witnessed .....

*APPENDIX "F"*

REPUBLIC OF KENYA

## OFFICIAL SECRETS ACT 1968

### To be Signed by Persons Outside Government Service

My attention has been drawn to the provisions of the Official Secrets Act, 1968, which are set out on the back of this document, and I am fully aware of the serious consequences which may follow any breach of those provisions.

I understand that any information which I receive orally or in writing as ..... ..... will be information entrusted to me in confidence within the meaning of Section 3 of the Official Secrets Act, 1968.

I understand that the sections of the Official Secrets Act set out in the back of this document, cover articles published in the Press or in book form, and I am aware that I must not divulge any information gained by me during the period covered by my appointment to any person, orally or in writing, without lawful authority. I understand also that these provisions apply not only during the period of my appointment but also hereafter.

Signed .....

Witnessed ..... Date .....

Surname (BLOCK LETTERS) .....

Forename(s) .....

Date of Birth .....

Permanent (home) address .....

*APPENDIX "G"*

REPUBLIC OF KENYA

---

## OFFICIAL SECRETS ACT 1968

---

### To be Signed by Persons Outside the Government Service on Ceasing to Have Access to Classified Information

My attention has been drawn to the provisions of the Official Secrets Act, 1968, which are set out on the back of this document, and I am fully aware of the serious consequences which may follow any breach of those provisions.

I understand:—

(1) that the Official Secrets Act will continue to apply to me in respect of any information covered by this Act which I may have acquired;

(2) that I may not divulge without lawful authority any such information in any form, whether orally or in any document, article, book, play, film, or otherwise, either in Kenya or abroad;

(3) that I may not retain official documents, plans, models, sketches, photographs or the like without authority.

*(Signed)* .....

Witnessed ..... Date .....

Surname (BLOCK LETTERS) .....

Forename(s) .....

Date of Birth .....

Permanent (home) address .....

RECORD OF AMENDMENTS

| No. | DATE | DETAILS |
|---|---|---|
| | | |