

Appendix 3

The 'Protective Security Handbook'

FOR OFFICIAL USE



COMMONWEALTH OF AUSTRALIA

**PROTECTIVE SECURITY
HANDBOOK**

JUNE 1978

PROTECTIVE SECURITY HANDBOOK

© Commonwealth of Australia 1978
Issued by authority of the Attorney-General

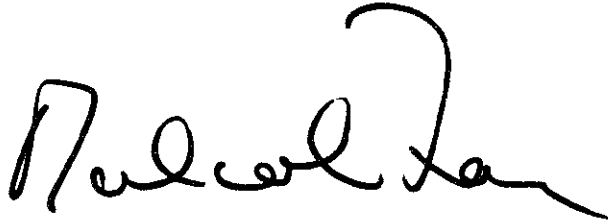
FOREWORD

It is the firm view of the Government that Australian citizens should have access to information held by or on behalf of Government, unless there are strong reasons for non-disclosure.

One of the most important reasons for such non-disclosure is national security. It is hardly necessary to explain why nations must keep secret their defence arrangements; and there are other equally important areas where confidentiality, in the national interest, must prevail over private or public rights to information.

In such cases, it is the responsibility of every citizen—and especially of persons in government employment and members of the Defence Force—to ensure that information is safeguarded and not disclosed without authority.

The purpose of this book is to set out the reasonable and necessary requirements for the protection of such information. I look to all officers dealing with it to observe both the letter and the spirit of these requirements.

A handwritten signature in black ink, appearing to read 'Robert Menzies', written in a cursive style.

PRIME MINISTER

CONTENTS

Introduction	
Chapter 1: Security organisation	<i>Page</i> 1
Chapter 2: System of classification	2
Chapter 3: Procedures for classification	4
Chapter 4: Personnel engaged on classified work	7
Chapter 5: Control of classified documents	8
Chapter 6: Breaches of security	10

INTRODUCTION

The purpose of this book is to outline the main requirements to protect:

- (a) information relating to the national security, that is to say the defence of Australia, the security of Australia or the international relations of Australia, which, if disclosed to unauthorised persons, would prejudice national security;
- (b) Cabinet documents;
- (c) other official information affecting the national interest; and
- (d) information given in confidence to government.

2. Detailed requirements applying to the protection of information of national security significance are contained in classified instructions including departmental security instructions; in relation to protection of Cabinet documents, such requirements are contained in the Cabinet Handbook. This Protective Security Handbook sets out procedures for classification of both of these matters.

3. Detailed requirements as to other official information affecting the national interest (e.g. communications between Commonwealth and State Ministers and Federal Executive Council matters, where appropriate) are contained in departmental security instructions.

4. The final category referred to in paragraph 1 above is information concerning the private affairs of individuals, companies and organisations, or other information obtained by government, under an assurance of confidentiality. Departmental instructions specify the degree of protection to be given to and appropriate measures for safeguarding these privacy matters.

5. Unauthorised disclosure of classified matters or of other official matters affecting the national interest may attract penal sanctions. Unauthorised disclosure of privacy matters may constitute breaches of statutory requirements including special legislation dealing with such matters, e.g. taxation and census.

6. Access to classified matter is to be no wider than is necessary for the efficient performance of duties and is to be restricted to authorised persons. This requirement of access on a 'need to know' basis is fundamental to all aspects of security.

7. The Permanent Head is responsible for ensuring that departmental staff are made aware of the contents of this book and of departmental security instructions. The heads of statutory authorities and other governmental agencies have the same responsibility in relation to their staffs. In the case of Ministerial staff the responsibility rests with the Minister for Administrative Services.

Chapter 1

SECURITY ORGANISATION

1.1 The Permanent Head is responsible for security within his department. The heads of statutory authorities and other governmental agencies and the Chief of the Defence Force Staff and the Chiefs of Staff of the Navy, Army and Air Force are responsible for security within their organisations. All these office holders are included, hereinafter, in the term 'Permanent Head', and all such authorities, agencies and forces are included in the word 'department'.

1.2 All departmental staff, particularly supervisory staff, have a responsibility to the Permanent Head for appropriate security arrangements in their own operational areas.

1.3 The Permanent Head should ensure that there is clear allocation of responsibility for physical and personnel security within his department. Normally, responsibility for security arrangements will be assigned to a senior officer, who may in turn exercise that responsibility through a security officer on a full-time or part-time basis, or through a security section, according to requirements.

1.4 Departmental security instructions, setting out detailed security arrangements for the department, are issued by, or on the authority of, the Permanent Head.

1.5 The Australian Security Intelligence Organisation (A.S.I.O.) is required to advise and assist departments in their security responsibilities. It is not the function of A.S.I.O. to carry out or enforce measures for security.

Chapter 2

SYSTEM OF CLASSIFICATION

National security information

2.1 National security information is information affecting the defence, security or international relations of Australia. According to the estimated prejudice to national security which might result from unauthorised disclosure, national security information should be given one of the four national security classifications—TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED—which are defined hereunder:

TOP SECRET

National security information which requires the highest degree of protection, is to be classified TOP SECRET. The test for assigning the classification is whether its unauthorised disclosure could cause *exceptionally grave damage* to the national security. Very little information in fact belongs in the TOP SECRET category, and the classification should be used with the utmost restraint.

SECRET

National security information which requires a substantial degree of protection is to be classified SECRET. The test for assigning the classification is whether unauthorised disclosure of the information could reasonably be expected to cause *serious damage* to the national security. It should be sparingly used.

CONFIDENTIAL

National security information which requires a decided degree of protection is to be classified CONFIDENTIAL. The test for assigning the classification is whether its unauthorised disclosure could reasonably be expected to *cause damage* to the national security. Most national security information will merit classification no higher than CONFIDENTIAL. All Cabinet documents are also to be classified CONFIDENTIAL unless requiring a higher national security classification.

RESTRICTED

National security information which requires some protection but does not warrant a higher classification is to be classified RESTRICTED. The test for assigning the classification is whether unauthorised disclosure could possibly be *harmful* to the national security.

2.2 Documents which do not contain more information than has been published in the press or otherwise issued by unofficial agencies may nevertheless confirm the accuracy or otherwise of such published material, or give official views thereon. Provided they are related to national security, such documents should be appropriately classified.

Cabinet documents

2.3 Cabinet documents are those covered by the Cabinet Handbook. Cabinet documents are given the appropriate national security classification of CONFIDENTIAL, SECRET or TOP SECRET.

Other official information affecting the national interest

2.4 Documents containing other official information affecting the national interest (e.g. communications between Commonwealth and State Ministers, and Executive Council matters, where appropriate) may be given the marking of **IN CONFIDENCE**. Detailed requirements for handling documents of this nature are included in departmental security instructions.

Privacy information

2.5 Certain documents containing information concerning the private affairs of individuals, companies and organisations, or other information obtained under an assurance of confidentiality, may require the protection of an '-in-Confidence' marking and appropriate special measures for safeguarding, as provided for in departmental instructions. This marking can be varied depending upon the area concerned, e.g. Staff-in-Confidence; Medical-in-Confidence; Census-in-Confidence; Commercial-in-Confidence. Many privacy matters presently being marked **CONFIDENTIAL** should be marked '-in-Confidence'.

Importance of proper classification

2.6 Over-classification is a problem of continuing importance since it has the following undesirable effects: information and material that is properly classified may be inadequately protected because the volume of classified material is too large; unnecessary and costly administrative arrangements have to be made to protect information and material improperly classified; and classification and security procedures generally are brought into contempt.

2.7 Over-classification constitutes a serious defect in the security system. It may stem from a genuine uncertainty as to the proper standards of classification or from a tendency to be over cautious. Whatever the cause, the result is a loss of confidence in the various levels of classification and a tendency to over-classify by way of compensation.

Guidance to staff

2.8 For the guidance of staff, departmental security instructions set out examples to assist with proper classification.

Chapter 3

PROCEDURES FOR CLASSIFICATION

Requirements for classifying and confirming classification

3.1 The originator is responsible for the initial classification of a document. In the interests of accuracy and uniformity, the initial classification given by the originator is to be confirmed by a confirming authority prior to the distribution of the document unless the originator himself is listed below, under the appropriate security classification, as a confirming authority.

3.2 The requirements for confirming authorities are:

TOP SECRET matter

To be confirmed by:

- (a) Commonwealth Government Ministers, for those areas under their control;
- (b) any person in a department listed at, or above, the public service rank of Assistant Secretary or its equivalent;
- (c) the head of a diplomatic mission or special mission or the head of a consular post or the chief representative of a department in an overseas country; and
- (d) in special circumstances, any person or class of persons in a department below the Assistant Secretary level as authorised by a Minister or Permanent Head.

SECRET matter

To be confirmed by:

- (a) any person having authority to confirm the classification of matter as TOP SECRET;
- (b) any person in a department listed at, or above, the public service level Class 9 or its equivalent; and
- (c) in special circumstances, any person or class of persons in a department below the public service level Class 9 as authorised by a Minister or Permanent Head.

CONFIDENTIAL, RESTRICTED and IN CONFIDENCE matter

To be confirmed by:

- (a) any person having authority to confirm the classification of matter as TOP SECRET or SECRET; and
- (b) any person or class of persons in a department as authorised by a Minister or Permanent Head.

3.3 The file copy of a document originating in a department and classified CONFIDENTIAL or above is to indicate on its face the identity of the person confirming the classification. Where such a classified document is signed by an officer authorised to confirm the particular classification, that person is to be deemed to be the person confirming the classification.

3.4 The sole criterion in the selection of the appropriate classification is the estimated damage unauthorised disclosure would cause to national security or the national interest.

General rules for classifying documents

3.5 The following are the more important requirements to be followed in classifying documents:

- (1) A document is to be classified at the earliest stage necessary during its preparation.
- (2) The classification of each individual document depends solely on its content—not on the classification of the file on which it was drafted or of another document to which it refers. There is no need to allot to a subsequent document a classification as high as an earlier one which it quotes or refers to, provided the quotation is limited to the reference number, the date and matter not in itself justifying a classification higher than that otherwise required for the content of the subsequent document.
- (3) Factors other than the contents of an individual document may need to be considered when classifying it, e.g. protection of the source of information.
- (4) The classification of a file will normally be that of the highest classified document it contains. Certain compilations of information may require a higher classification than that of the component parts because of the greater intelligence value of the comprehensive picture available.
- (5) A document must not bear a lower classification than the highest classification of any of its appendixes or attachments. On brief notes or covering letters which do not require as high a classification as an attachment, a formula such as

CONFIDENTIAL

covering

TOP SECRET

may be used provided that both classifications are stamped in red block letters.

- (6) A classified document may have a lower classified or unclassified attachment.
- (7) Where it is known that any information contained in a document can be 'reclassified after a certain date', that should be indicated in the text or in a sideline.

Classification of committee papers

3.6 The classification of committee papers and minutes of government and inter-departmental committees is ultimately the responsibility of the chairman of the committee who should consult the committee when in doubt. Each document should be classified according to its content. For example, where considered necessary, each item of the minutes should be classified individually according to its content in order to facilitate extraction and separate filing.

Classification of tapes including computer tapes

3.7 The classification of each item recorded on magnetic tape is to be clearly stated at the beginning and end of each recording. Because erasure of information from magnetic tapes is seldom complete, once classified material has been recorded on a tape, the tape thereafter retains, until totally destroyed, the same classification as the highest classified material ever recorded on it, and that classification should be clearly marked on each spool.

Marking of classifications on documents

3.8 All classified books, pamphlets, letters, memoranda, papers and other classified material, and all copies thereof, should be plainly and conspicuously marked with the appropriate classification at the top and bottom of each page, including the front cover, the title page and the back of the rear cover or last page of books and pamphlets. In the case of typed documents the classification marking should be stamped in a contrasting colour, preferably red, and letters should be a minimum of 6.35 mm ($\frac{1}{4}$ ") in height. The classification marking should be stamped in such a manner that it does not interfere with or overstamp any other headings, addresses or instructions. In the case of printed documents the classification marking should be set in type which is larger and heavier than the largest type used in the text of the document.

3.9 The classification on maps and drawings is to be printed or stamped near to the map scale or drawing numbers in addition to being printed at the top and bottom centre of the document.

3.10 Classified photographs, film and microfilm and their containers are to be conspicuously marked with the classification. Photographic negatives are to be marked so that the classification will be reproduced on all copies made from the original.

Reassessment of classified material

3.11 The classification given to national security or other official information affecting the national interest may alter with the passage of time and departments should reassess in accordance with a departmental review program as provided for in departmental security instructions.

3.12 The classification of information received from other departments is not to be changed without the approval of the originating authority.

3.13 When reclassifying a document the old classification is to be deleted in ink and the new one stamped on the document. The amendment is to be signed by the officer making the change and a note made of any documentary authority for the change.

Requirements for marking and reassessment of other official information affecting the national interest and privacy information

3.14 The requirements for the marking and reassessing of IN CONFIDENCE information are to follow, as far as applicable, the requirements set out above for classified information.

Chapter 4

PERSONNEL ENGAGED ON CLASSIFIED WORK

The 'need to know' requirement

4.1 Access to classified matter is to be no wider than is necessary for the efficient performance of duties and is to be restricted to authorised persons. This rule applies both within a department and in dealing with authorised persons outside the department.

Persons in government employment, consultants and contractors

4.2 Permanent Heads or their delegates are responsible for determining and authorising persons employed in their departments, consultants and contractors who are to have access to classified matter.

4.3 Supervising officers are responsible to the Permanent Head for ensuring that effective measures are taken to prevent access to classified matter by unauthorised persons and that authorised persons are familiar with the requirements to safeguard it.

Persons not in government employment

4.4 Classified matter may be made available on a strict 'need to know' basis to authorised persons or organisations not in government employment, but only with the approval of the originating department.

Authorisation

4.5 Information as to persons authorised for access to classified matter is available from the departmental security officer.

4.6 Before classified matter is passed to authorised persons not in government employment, the Permanent Head is to ensure that such persons are familiar with the special handling procedures required by the department and that adequate arrangements have been made for those procedures to be observed.

4.7 Authorisations are to be reviewed from time to time.

Chapter 5

CONTROL OF CLASSIFIED DOCUMENTS

Storage and access to classified matter

5.1 Classified matter is to be stored securely in locked containers when not in use and keys and combinations are to be safeguarded. Care is to be taken to ensure that unauthorised persons do not view or have access to the classified matter. Detailed information on storage and access is to be found in departmental security instructions.

Combination settings

5.2 Combination settings are to be committed to memory. The only written record of the setting for use in an emergency is to be held by departments in sealed envelopes classified with the highest security classification of the matter held in the container. The setting is to be changed when a container is first received by the department; after servicing of the lock at any time subsequently; when there has been a change of custodian; or when there is reason to believe the setting has been compromised; and, in any case, not less frequently than every six months.

Loss or compromise

5.3 The loss or compromise of a classified document or of a security key or combination setting must be reported immediately to the appropriate departmental security authorities and, as necessary, to the Permanent Head.

Handling classified matter

5.4 Typing, reproduction, recording and transmission of classified matter is only to be made in accordance with departmental security instructions or, in the case of Cabinet documents, in accordance with the Cabinet Handbook.

Removal of classified matter

5.5 Classified matter is not to be taken out of departmental premises without the approval of an authorised officer and then only in accordance with departmental security instructions. In the case of Cabinet documents, the requirements of the Cabinet Handbook are to be observed.

Carriage within that part of a department located within a single building or complex

5.6 National security matter classified TOP SECRET is to be covered and passed by hand between officers who have the need to know. If that is not practicable, it is to be locked in an approved case or enclosed in two envelopes and handed to an authorised messenger for immediate delivery personally to the addressee or authorised representative. Matter classified SECRET may be enclosed in a single envelope endorsed SECRET, where the use of an approved case is not practicable, provided it is delivered direct by hand of an authorised messenger. Other classified matter is to be carried in accordance with departmental security instructions.

Carriage outside a building or complex

5.7 Classified matter is to be carried in accordance with procedures set out in departmental security instructions.

Retention of classified matter

5.8 Classified matter is not to be retained by an officer longer than is necessary for the efficient performance of his duties.

Destruction of classified matter

5.9 As careless disposal of classified matter constitutes one of the most likely sources of leakage of information, destruction of classified matter is only to be made in accordance with departmental security instructions or, in the case of Cabinet documents, in accordance with the Cabinet Handbook.

Use of telephones

5.10 Great caution should be exercised in discussing classified matters on the telephone. The normal telephone, even if fitted with speech privacy equipment of the inverter type (known as secraphone, scrambler, green telephone etc.) does not provide sufficient security for discussion of matter classified higher than RESTRICTED.

Facsimile transmission

5.11 Users of facsimile machines should be aware that the facsimile process, while offering some measure of protection against casual eavesdropping or inadvertent cross connection, also does not provide sufficient security for the transmission of matter classified higher than RESTRICTED.

Chapter 6

BREACHES OF SECURITY

6.1 A communication to any unauthorised person of any classified information is a serious breach of security which may damage national security or the national interest, and may attract sanctions pursuant to the Crimes Act or Defence legislation, or render an officer liable to disciplinary action under the Public Service Act and Regulations.

6.2 The protective security system is intended to safeguard classified information and is aimed at preventing security breaches from occurring. Accordingly, it is necessary that any breaches of protective security measures (including infringement of departmental security instructions) be reported immediately to the appropriate departmental security authorities and, as necessary, to the Permanent Head.

6.3 As regards privacy information, a communication to any unauthorised person may be a breach of statutory requirements that such information is not to be disclosed without proper authority. Such disclosures may lead to disciplinary action under the Public Service Act and Regulations and may also attract sanctions under special legislation dealing with such matters, e.g. taxation and census.

6.4 Officers having access to material of a classified nature or subject to privacy markings should be informed of the relevant legislation relating to the protection of information from unauthorised disclosure. Departmental instructions should list the relevant legislative provisions.

6.5 The security of classified information depends on the integrity, discretion and vigilance of all those who deal with it and on the existence of and compliance with effective security arrangements within each department. The strict observance of these arrangements may involve additional work and administrative inconvenience, but is essential in the national interest.