

DEPARTMENT FOR EMPLOYMENT AND LEARNING

A GUIDE TO PROTECTIVE MARKINGS AND DOCUMENT SECURITY

1. INTRODUCTION

As civil servants, DEL staff should be aware of their duties and obligations in relation to the use of official information (as detailed in paragraph 956 of the NICS Pay and Conditions of Service Code, and CSC 8/94). Those staff who handle protectively marked documents should be particularly conscious of their personal responsibility for ensuring that these are indeed adequately protected - from damage, loss, unauthorised disclosure, etc.

This document contains instructions and guidance on the security of documents and information to help you fulfil these responsibilities. All staff should familiarise themselves with the content and remember where to access it for future reference. It is especially important to ensure that staff have a correct understanding of the protective markings and privacy markings - in particular, the use of the protective marking **CONFIDENTIAL** which currently appears to be widely misunderstood. This document also provides advice on the introduction of a new category of information below **RESTRICTED** to be known as **PROTECT**.

Material protected by this heading should be treated in the same way as **RESTRICTED**. **RESTRICTED** still remains in place, however **PROTECT** will cover material that does not have a national security implication.

All Heads of Branches and Office Managers should review how protectively marked material is dealt with in their areas of responsibility. In particular the common problem of over-classifying material should be addressed bearing in mind that the cost of handling and of storing such material is substantial.

Further guidance on particular aspects of document security can be obtained from Norman McCracken 90 2(57861) or Maureen Doonan, 90 2(57866). Personnel (Services) Branch, Adelaide House.

2. PROTECTIVE MARKING SYSTEM

The NICS is responsible for and handles an enormously wide range of assets that require protection. Assets refer to anything valuable for which government is responsible - not only documents and information, but also materials, equipment, operating systems etc. Some, of particular value or sensitivity, need to be given a special level of protection in order to:

- meet legal, moral or political obligations;
- protect the interests of national security, the economy or national influence; and
- promote good government by maintaining confidence.

The NICS protects these assets because their compromise will cause damage. The range of means by which damage could be caused to assets can be broken down into four general groups:

- disclosure;
- theft;
- destruction; and
- tampering.

Protective markings are labels that show how valuable an asset is. The value is determined by reference to the amount of damage that is likely to occur if the asset is compromised.

When marking **documents or information**, the guiding factor will be the consequences of a breach of confidentiality, so the question to ask yourself is:

- "How damaging are the consequences likely to be if someone who intends to do harm reads this document/ information?"
- "How damaging are the consequences likely to be if an unauthorised person gains access to this document/information?"

When considering **physical assets**, the guiding factor will be the other types of compromise, so you will need to ask yourself:

- "How damaging are the consequences likely to be if this asset is lost, stolen, damaged or destroyed?"

Answering these questions against the background of the definitions of the protective markings will give the most appropriate label for the information. The five protective markings and their definitions are detailed below. If you are in any doubt about the type of compromise to which information or an asset may be vulnerable, you should contact Norman McCracken 90 2(57861) or Maureen Doonan on 90 2(57866), Personnel (Services) Branch.

Each level of protective marking corresponds to a standard of protection. The higher level of protective marking, the greater the damage likely to occur if that asset is compromised and, hence, the more extensive the security measures to be employed in protecting it.

4. DEFINITION OF PROTECTIVE MARKINGS

Documents or material which carry a protective marking must have their marking **printed or stamped** in the centre of the top and also at the bottom of every page. The cover of a file or folder containing documents with protective markings must be stamped to the highest documents it contains.

TOP SECRET:

The compromise of this information or material **would be likely:**

- to threaten directly the internal stability of the UK or friendly countries;

- to lead directly to widespread loss of life;
- to cause exceptionally grave damage to the effectiveness or security of UK or allied forces or to the continuing effectiveness of extremely valuable security or intelligence operations;
- to cause exceptionally grave damage to relations with friendly governments; to cause severe long-term damage to the UK economy.

SECRET:

The compromise of this information or material **would be likely:**

- to raise international tension;
- to damage seriously relations with friendly governments;
- to threaten life directly, or seriously prejudice public order, or individual security or liberty;
- to cause serious damage to the operational effectiveness or security of UK or allied forces or the continuing effectiveness of highly valuable security or intelligence operations;
- to cause substantial material damage to national economic and commercial interests;
- to lead to additional government expenditure on a scale likely to affect the UK economy as a whole.

CONFIDENTIAL:

The compromise of this information or material **would be likely:**

- to materially damage diplomatic relations (i.e. cause formal protest or other sanction);
- to prejudice individual security or liberty;
- to cause damage to the operational effectiveness or security of UK or allied forces or the effectiveness of valuable security or intelligence operations;
- to work substantially against national economic and commercial interests;
- to lead to substantial additional expenditure for or financial loss to government;
- substantially to undermine the financial viability of other major organisations;
- to impede the investigation or facilitate the commission of serious crime;
- to impede seriously the development or operation of major government policies;
- to shut down or otherwise substantially disrupt significant national operations.

RESTRICTED:

The compromise of this information or material **would be likely:**

- to affect diplomatic relations adversely;
- to make it more difficult to maintain the operational effectiveness or security of UK or allied forces;

- to impede the effective development or operation of government policies;
- to undermine the proper management of the public sector and its operations.

PROTECT (this is a sub-national security marking):

The compromise of this information or material **would be likely**:

- to cause substantial distress to individuals;
- to breach proper undertakings to maintain the confidence of information provided by third parties;
- to breach statutory restrictions on the disclosure of information.

Depending on the severity of the circumstances either **RESTRICTED** or **PROTECT** may apply where compromise **would be likely**:

- to cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for individuals or companies;
- to prejudice the investigation or facilitate the commission of crime;
- to disadvantage government in commercial or policy negotiations with others.

5. DESCRIPTORS

Underpinning the need to protect against compromise is the principle of only giving access to material to those who need to have access. This 'need to know' principle is supported by a system of 'descriptors'. These labels serve two functions:

- they show what sort of sensitive material is being protected;
- and they help people handling information to consider what groups of people either should or should not have access to it.

The core descriptors and their definitions are listed below.

Appointments †	concerning actual or potential appointments that have not yet been announced;
Budget	concerning proposed or actual measures for the Budget before its announcement;
Commercial ≠ Contracts ≠	relating to a commercial undertaking's process or affairs; concerning tenders under consideration and the terms of tenders accepted;
Honours †	concerning the actual or potential award of an Honour before the announcement of the award;
Investigation ≠	concerning investigations into disciplinary or criminal matters;
LocSen (locally sensitive)	concerning locally sensitive information which should not be seen by locally engaged staff or other local nationals;
Management	concerning policy and planning affecting the interests of

	groups of staff;
Medical †	medical reports and records and material relating to them;
Personal †	material only to be seen by the person to whom it is addressed (see section 6) ;
Policy	concerning proposals for new or changed government policy before publication;
Staff †	containing references to names or identifiable staff or personal confidences entrusted by staff to management; and
Visits	concerning details of visits by, for example, royalty, ministers or very senior staff.

† Descriptors associated with **PROTECT**

≠ Descriptors that may be used with **RESTRICTED** or **PROTECT**

If descriptors are used, they will generally sit alongside a protective marking to indicate the nature of the material's sensitivity, e.g.

PROTECT – STAFF or **RESTRICTED - INVESTIGATION** etc

They do not, in themselves, mean having to apply additional security measures or handling procedures. It is the protective marking that determines the level of protection. It is not necessary to use a descriptor each time a paper receives a protective marking. The only exception to this is **PROTECT** which should always be accompanied by a “descriptor”.

6. THE DESCRIPTOR ‘PERSONAL’

The exception here is the descriptor **PERSONAL**. This requires that the information is only made available first of all to the person it is addressed to. It is also possible that you might use the descriptor **PERSONAL** on its own where material is not sensitive enough to warrant any security measures, but where it is important that only the addressee has access.

Apart from **PERSONAL**, descriptors can describe only in the broadest terms the sort of people who should or should not be given access to an asset. You will still need to consider the 'need to know' principle and to ensure that information is spread no more widely than it has to be, even within the group described.

If you use a descriptor in addition to a protective marking, then it should follow the marking, e.g. PROTECT-APPOINTMENTS.

Protected documents must carry their marking printed or stamped **clearly** in the centre of the top and bottom of every page. The cover of a file or folder

containing protected documents should be stamped according to the highest marking of the documents it contains. For advice on inserting headers and footers electronically on documents, please refer to the DEL Intranet – DEL IT Network, Sensitive and Confidential Documents Policy. The link is:-

http://delintlm/DEL_INTRANET/Documents/S_Corporate%20Services/S_Corporate%20Information%20Systems/IT%20Security/Sensitive%20and%20Confidential%20documents%20Version%201%20December%202006.doc

A record should be kept of the movement of all protected material.

7. HANDLING PROTECTIVELY MARKED MATERIAL

All documents marked **CONFIDENTIAL** or above, including waste, must be locked away in appropriate security containers when not in use or whenever a room is left unattended.

Rooms must be checked by the occupants at the close of work to ensure that all protected documents, including waste, have been put away in security containers. Documents marked **RESTRICTED** or **PROTECT** may be stored in ordinary office furniture, provided they are locked away when not in use.

Security keys and the keys of furniture holding **RESTRICTED** or **PROTECT** material should never be taken out of the office or "hidden" in drawers or desks. At close of work these keys should be checked and locked away in combination lock key boxes.

Codes of combination locks should be memorised and not written in diaries or notebooks. If they must be written down then they should be kept on the owner's person.

The settings of combination locks must be changed at least every 6 months or earlier if ownership of the security furniture changes, or staff having knowledge of the combinations are transferred. Settings should be made up of numbers chosen at random; they should not be based on telephone numbers or room numbers or on dates which might have apparent significance, e.g., the officer's own birthday.

The loss of security keys or the suspected compromise of a combination setting must be reported immediately to Personnel (Services) Branch on 90 2(57864).

Office Managers should ensure that their staff know who has the responsibility for securing cabinets and offices.

8. PROTECTIVELY MARKED DOCUMENTS OUTSIDE THE OFFICE

If protected documents have to be taken outside the office, then the carrying officer is solely responsible for ensuring that this has been properly recorded in the branch.

In such circumstances staff should only remove protected material if authorised by:-

- (a) Permanent Secretary in the case of Top Secret.
- (b) Grade 5 in the case of Secret.
- (c) Grade 7 in the case of Confidential.

Staff must ensure that protected documents are not left in an unattended motor vehicle. They must not be read or left unattended in a public place. Protected documents must remain in the possession of the carrying officer **at all times**. This also applies to unprotected but otherwise sensitive material.

9. DESTRUCTION OF PROTECTIVELY MARKED MATERIAL

You must separate protected from unprotected waste paper. Protected waste, graded above the **RESTRICTED** marking, must be held securely in appropriate containers and then sent for pulping. **RESTRICTED** or **PROTECT** papers may be shredded. Pending its disposal the waste retains its protective marking and must be stored appropriately.

10. SENDING PROTECTED AND PRIVACY MARKED DOCUMENTS

A complete guide to the procedures for sending hard copies of classified documents is attached at Appendix (i).

Commercial courier or storage companies should not be used for the handling or storage of protected material, privacy marked material or documents of a sensitive nature irrespective of whether or not they are actually classified.

Staff are reminded that fax machines must not be used for the transmission of any material graded higher than **RESTRICTED**. When faxing a protected document on an unsecured fax machine it is essential that the sender notifies the recipient in advance. Staff should not send any material graded higher than **RESTRICTED** via the Department's IT network, but should send such documents in hard copy as described in Appendix (i).

Documents with **PROTECT** heading may be sent to parties outside the NICS, if so it would be appropriate to send handling instructions to the recipient. A sample of handling instructions is attached at Appendix (ii).

11. STORING PROTECTED AND PRIVACY MARKED DOCUMENTS

All protected material must be kept secure. **RESTRICTED** and **PROTECT** documents may be locked in ordinary office furniture. **CONFIDENTIAL**, **SECRET** and **TOP SECRET** must be locked in an approved special security cabinets of metal construction with either combination locks or special metal bar and key locks. Personnel (Services) Branch can arrange for you to be supplied with such cabinets on request. It must be clearly understood that ordinary metal cabinets are **NOT** security cabinets.

All protected material must be locked up when not in active use. It is your personal responsibility to make sure that protected material is not left on your desk where it can be seen or handled by unauthorised persons. **It is particularly important that all desks are cleared and all papers locked up properly at night.** Personnel (Services) Branch will carry out regular security checks to ensure that classified material is not left unprotected. Further information on the clear desk policy and related issues is available in the Departmental Security Guidelines on the DEL Intranet.

Protected material committed to electronic media must be subject to the same restriction of access as protected documents. The media upon which the protected material is held, (e.g. floppy disk) must be capable of being stored as for documents, that is, in an appropriate security container. Passwords to restrict access to protected material must be issued on the 'need to know' policy and treated as requiring protection.

12. REGRADING OR DECLASSIFYING OF PROTECTED MATERIAL

Whenever possible the officer who was the originator of the protected document, regardless of any subsequent change of post or promotion, should be asked about the need for it to retain its protective grading. Due to the passage of time this will often not be possible. In any such case the officer currently in the "originator's" post should be asked to review the grading. Any decision the current postholder makes must be put in writing.

Staff must ensure that any protected material which is circulated for information is not retained or copied by an individual officer unless specified or permitted to do so but is returned to the point of origin or destroyed. Failure to comply with this particular instruction is a frequent cause of security breaches.

13. ADVICE AND GUIDANCE

Departmental Security

Further information on security issues is available in the Departmental Security Guidelines on the DEL Intranet. If you are unclear about any part of this circular or feel that you could benefit from further advice, contact Norman McCracken on 90 (257861) or Maureen Doonan, Personnel (Services) Branch on 90 2(57866).

IT System

For more detailed guidance on security standards for Information Technology Systems, please contact Roisin McKay, Information Technology Security Officer (ITSO), CIS on 90 2(57926).

Please also refer to the DEL IT Network, Sensitive and Confidential Documents Policy document available on the DEL Intranet. The link is:-

http://delintlm/DEL_INTRANET/Documents/S_Corporate%20Services/S_Corporate%20Information%20Systems/IT%20Security/Sensitive%20and%20Confidential%20documents%20Version%201%20December%202006.doc

Management of Official Records and TRIM

If you wish to receive further advice on the management of official records including the use of TRIM, please refer to the Guidelines on the Management of Official Records which is held on the DEL Intranet or speak to Helen Lindsay, Information Management 90 2(57442).

Please also refer to Guidelines on the Management of Official Records available on the DEL Intranet. The link is:-

[http://delintlm/DEL_INTRANET/Documents/S_Corporate%20Services/S_Information%20Management/Departmental%20Records%20Unit/Guidelines%20on%20the%20Management%20of%20Official%20Records%20\(Revised%20Mar%202005\).doc](http://delintlm/DEL_INTRANET/Documents/S_Corporate%20Services/S_Information%20Management/Departmental%20Records%20Unit/Guidelines%20on%20the%20Management%20of%20Official%20Records%20(Revised%20Mar%202005).doc)

HOW TO SEND PROTECTIVELY MARKED MATERIAL

Classification	Destination	Envelopes			Transmission
TOP SECRET		Single	Double	Marking	Approved Messenger/Courier Service only
	Different departments within NI	No	Yes New envelopes	a. Inner envelope to be marked TOP SECRET and inscribed 'TO BE OPENED only by (full address) or in their absence (1) by the person designated to open TOP SECRET documents on their behalf or (2) return to sender. b. Outer envelope should show no classification marking but be fully addressed.	Yes Document receipts advisable.
	Between two buildings within one department	No	Yes New envelopes	As for double envelopes above.	Yes Timed and signed package at each handover.
	Single department within one building	No	Yes New envelopes	As for double envelopes above.	Yes Document/packet receipts advisable.

Classification	Destination	Envelopes			Transmission
SECRET		Single	Double	Marking	Approved Messenger/Courier Service only
	Different departments within NI	No	Yes New envelopes	a. Inner envelope to be marked SECRET and inscribed 'TO BE OPENED only by (full address) or in their absence (1) by the person designated to open SECRET documents on their behalf or (2) return to sender. b. Outer envelope should show no	Yes Document/packet receipts advisable.

				classification marking but be fully addressed.	
	Between two buildings within one department	No	Yes New envelopes	As for double envelopes above.	Yes Document/packet receipts optional.
	Single department within one building	No	Yes New envelopes	As for double envelopes above.	Yes Document/packet receipts optional.

Classification	Destination	Envelopes			Transmission	
		Single	Double	Marking	Approved Messenger Courier Service only	Royal Mail
CONFIDENTIAL						
	Different departments within NI	No	Yes	a. Inner envelope to be marked CONFIDENTIAL and be fully addressed. b. Outer envelope should show no classification marking and be addressed as for inner envelope.	Yes	Yes
	Between two buildings within one department	No	Yes	a. Inner envelope to be marked CONFIDENTIAL and be fully addressed. b. Outer envelope should show no classification marking and be addressed as for inner envelope.	Yes	Yes
	Single department within one building	No	Yes	a. Inner envelope to be marked CONFIDENTIAL and be fully addressed. b. Outer envelope should show no classification marking and be addressed as for inner envelope.	Yes	N/A

Classification	Destination	Envelopes			Transmission	
		Single	Double	Marking	Approved Messenger Courier Service only	Royal Mail
RESTRICTED/PROTECT						
	Different departments within NI	Yes	No	Show no protective marking but be fully addressed.	Yes (Also mark envelope "for addressee only")	Yes

	Between two buildings within one department	Yes	No	Show no protective marking but be fully addressed.	Yes (Also mark envelope "for addressee only")	Yes
	Single department within one building	Yes	No	Show no protective marking but be fully addressed.	Yes (Also mark envelope "for addressee only")	N/A

Classification	Destination	Envelopes			Transmission	
		Single	Double	Marking	Approved Messenger Courier Service only	Royal Mail
RESTRICTED/ PROTECT STAFF or RESTRICTED/ PROTECT MANAGEMENT or RESTRICTED/ PROTECT PERSONAL		Single	Double	Marking	Approved Messenger Courier Service only	Royal Mail
	Different departments within NI	No	Yes	a. Inner envelope should show the appropriate PRIVACY MARK. b. Outer envelope should show no marking but be fully addressed.	Yes	Yes
	Between two buildings within one department	Yes	No	Envelope should show the appropriate PRIVACY MARK.	Yes	No
	Single department within one building	Yes	No	Envelope should show the appropriate PRIVACY MARK.	Yes	N/A

FOOTNOTE TO BE ATTACHED TO MATERIAL WITH PROTECT SECURITY MARKINGS TO PARTIES OUTSIDE NICS

PROTECT

Please note that the attached material has been given the protective marking **PROTECT**. **PROTECT** is a non-National Security marking.

How to handle material with PROTECT marking?

- Handle, use and transmit with care;
- Take basic precautions against accidental compromise, opportunist or deliberate attack;
- Dispose of sensibly by destroying in a manner to make reconstruction unlikely.