

## Document security in ND Division 3

**BSS/IMT/013**

<b>Date issued:</b> 2007-08-16	<b>OG Status:</b> Fully open
<b>Review date:</b> 2010-08-16	<b>Author Unit/Section:</b> ND 3AD

[Purpose & Scope](#)  
[Policy](#)  
[Responsibilities](#)  
[Definitions](#)  
[Procedures](#)  
[Associated Documents](#)

## **1 Purpose & Scope**

1.1 The purpose of this job guide is to explain the document security regulations applicable within Division 3 and to provide information on what will happen in a situation of non-compliance. The documentation/material referred to in this procedure, refers to information which bears a protectively marked classification and any information which is not in the Public Domain.

## **2 Policy**

2.1 Protectively marked files / documents bearing security markings “Restricted” (or above) must be treated in an appropriate manner consistent with HSE and government guidelines on the receipt, handling, storage and destruction of such material. This also applies to electronic information.

2.2 Due care must also be taken when handling information about ND staff.

2.3 All files marked confidential (and above) which relate to AWE / MOD related work or sites will be held in appropriate storage furniture and / or stored in the Division 3 enclave.

2.4 Periodic checks will be undertaken to ensure that staff adhere to the arrangements on handling and storage of protectively marked material. Any breaches in security relating to document handling will result in action in accordance with HSE guidance.

## **3 Responsibilities**

3.1 It is the responsibility of the file holder/document user to ensure that whilst sensitive or protectively marked files/documents are in their possession they should be stored securely in accordance with HR Guidance and Procedures - Conduct.

3.2 It is the responsibility of designated ND staff to carry out periodic checks of areas in Building 4S.2 and 3.2 to ensure no sensitive / protectively marked documentation is left out / can be accessed.

## **4 Definitions**

4.1 See **BSS/IMT/Annex 1** - Glossary of Definitions.

## **5 Procedures**

5.1 All sensitive/protectively marked material must be locked away securely when not in use. Staff should not leave material visibly displayed on their computer screen when they are away from their desk. In addition, work should not be left on the desk unattended, even for a short time and certainly not overnight.

5.2 Staff who regularly receive protectively marked or sensitive material and are going to be away from the office for some time should arrange for all post to be directed to the Divisional Support Office or, arrange for a colleague to empty their in-tray and store the contents adequately. Similarly, staff leaving the office early, who have missed the last collection, should not put any sensitive post in their out-tray. This will need to be locked away until next morning ensuring the keys being put away in a secure place.

5.3 Designated ND3 staff will carry out periodic 'sweeps' of offices to ensure that the document security regulations are being adhered to. This will involve checking areas within Division 3 to verify that the work is appropriately locked away.

5.4 Any sensitive/protectively marked material which is found during a 'sweep' will be confiscated and replaced with a note explaining why, and that retrieval of the material must be requested via the individual's line manager. A mail message will be sent to the individual's line manager explaining the situation and giving details of the material confiscated.

5.5 All sensitive/protectively marked material which is found will be stored in a safe in the secure enclave in Redgrave Court until retrieval is arranged.

5.6 Individuals **must** contact their line manager to arrange for retrieval of the confiscated material. The line manager will then contact the Enclave Liaison Manager (ELO) to arrange return.

5.7 The ELO will make a note of the incident, recording especially the nature / classification of the information contained in the material.

5.8 The ELO will produce a report to HSE security at the end of each quarter giving details of security breaches. Repeated security breaches by an individual may result in disciplinary proceedings - HR Guidance and Procedures - Conduct refers.

## **6 Associated Documents**

6.1 HR Guidance and Procedures - Conduct.