

Industry Security Notice

Number 2010 / 01

Subject: Handling MOD Personal Data

Introduction:

1. This Industry Security Notice reiterates policy and clarifies guidance on the Protective Marking, Impact Levels, encryption and handling rules for MOD personal information, particularly when held in 'bulk' form with a number of individual personal records accumulated together. As such it relates to elements of Principle 7 of the Data Protection Act 98 but readers should remember the importance and necessity of compliance with all 8 Principles of DPA 98.¹
2. Owing to the impact on reputation and the potential for harm and distress from compromise, the protective measures required for personal information (Impact Levels 0 - 2), particularly when aggregated, are more stringent than for non-personal information of the same Impact Level. Additionally, the basis by which the so-called "Handle As" or implied Impact Level is determined – and thereby the necessary protective measures defined - is based on the number of personal records, (rather than by the volume of the media concerned which is used for aggregated non-personal information).
3. This policy and guidance is to be applied by MOD industry partners. Future contracts involving significant quantities of Personal Data will be issued with a Personal Data Handling Letter.²
4. Policy and guidance on the Aggregation of Non-Personal Data and the impact on IT systems and Data Warehouses is set out in Annex B of DIAN 16, and reproduced here as Annex E.

Policy Changes

5. The threshold at which accumulated data is considered bulk personal data is increased from 250 to 1000.

¹ Personal Data' in this context is information of a personal nature as defined in HMG Information Assurance Standard No 2 or DPA98.

² Template PDAL can be found at Annex D

6. The requirement to handle all bulk personal data as IL5 is replaced by a graduated approach of increasing Impact Levels as volumes of data increase.
7. The frequency with which media holding personal data need be mustered is reduced from monthly to quarterly.

Issue:

Protective Marking and Impact Levels for Personal Information

8. Annex A sets out when individual personal information records should be considered to have a Protective Marking of PROTECT-PERSONAL DATA (P-PD) (IL 2). This may be because the records contain sensitive personal information as defined by DPA 98 or include information which, if compromised, might lead to identity theft or cause harm or distress.
9. Some individual records may need to be Protectively Marked higher than PROTECT and afforded a higher Impact Level than IL2 due to the sensitive nature of their content or context, e.g. if they relate to individuals in protected roles such as Special Forces and could be used to identify them as such.
10. Annex A also gives guidance on when a collection of personal information is to be treated as (“handled as”) IL2 because the impact of its compromise would cause significant reputational or other damage, even if each record individually would not attract a P-PD marking. One example is a collection of more than 1000 records containing information typically found on business cards (name, address, telephone numbers, email address).
11. Annex B illustrates the aggregation effect of increasing volumes of personal data at each Protective Marking, and also the effect on Impact Level resulting from the use of encryption.
12. The minimum Impact Levels to be used to determine the handling rules for aggregated personal data are provided at Annex B, covering data in both encrypted and unencrypted forms. These guidelines apply to personal records held on removable media, on paper and on servers in physical transit. The policy and guidance for personal data held on servers at rest is set out in Annex B of DIAN 16.
13. Particular data sets may attract a higher Impact Level than the minimum guide level because of the particular nature of the records and the reputational damage to the Department or damage to the individuals concerned if the information were to be compromised.

Encryption Requirements

14. All removable electronic media (including portable computers) containing IL1 or above data (whether individually Protectively Marked or by aggregation) must be encrypted. The level of encryption to be applied is determined by the highest Protective Marking of an individual record contained on the removable media.

15. DIAN 15 Lite, reproduced here as Annex F, lists the approved and acceptable encryption products for information at Protective Markings of Restricted and above and the preferred set of products for use within MOD.³ Approved encryption products reduce the Impact Level of the aggregated data. Acceptable encryption products do not reduce the Impact Level but do temper the rise in Impact Level as the volume of data increases.

Approval Requirements

16. The approval of the relevant Information Asset Owner must be obtained before protected personal data is placed on removable media, even if encrypted. This approval must be documented sufficiently to establish an audit trail of responsibility. If IL2 or above data (whether individually Protectively Marked or by aggregation) have to be put onto unencrypted removable media then a Risk Balance Case (RBC) should be raised to the SIRO (Senior Information Risk Owner) for approval, using the 'fast-track' process.⁴ Additional mitigation measures to those set out in Annex C may need to be agreed with Accreditors and CIO as part of the RBC process.

Other Access and Handling Requirements for Personal Data

17. Guidance is provided on the access and handling rules for personal data in Annex C, broken down by:

- a. Minimum personnel security level for routine access to the data;
- b. Level of physical protection required for its storage;
- c. Postal/courier transmission;
- d. Accounting and mustering.

Action by Industry:

18. Industry should fully comply with this Industry Security Notice, where full compliance is not possible the issue should be brought to the attention of the relevant MOD accreditor or CIO.

Validity / Expiry Date:

19. With immediate effect and until further notice.

MOD Point of Contact Details:

20. Daniel Selman, CIO-IHAT Del Ast Hd, CIO, Main Building, London, SW1A 2HB
020 7218 1353 CIO-IHATDelAstHd@mod.uk

³ DIAN 15 Lite, "Encryption of CIS Media"

⁴ There is a blanket exemption from this requirement to submit a RBC for the transfer of IL2 data on to back-up tapes if those tapes are handled in accordance with the guidance set out in the tables in Annexes B and C

Definition of Protected Personal Data

1. Personal data whose release or loss could cause harm or distress to individuals needs to be protected. Such information should be considered to have a Protective Marking of at least 'PROTECT – PERSONAL DATA' and handled, as a minimum, as Impact Level 2. A higher Protective Marking, for example RESTRICTED – PERSONAL DATA, may be used where justified by content or context, for example particularly sensitive information relating to individuals in the Special Forces which could be used to identify them as such.
2. Where information is only being shared with the individual to whom it refers, the originator of the information will decide whether a Protective Marking is applicable but it should still be handled at the relevant Impact Level.
3. Aggregation does not alter the Protective Marking of the collection – it remains that of the highest Protective Marking of any individual record in the collection – but the Impact Level may be raised to mitigate the increased impact of compromise. Annex B gives the indicative Impact Level for accumulated data and Annex C outlines the appropriate handling measures required at each Impact Level.
4. Information Asset Owners must determine which of the data they hold falls into the category of Protected Personal Data; this may be over above the conclusions of any Privacy Impact Assessment. This must include as a minimum all data falling into either Category A or B in the following table.

Category A: Any information that links one or more identifiable living person with information about them whose release is likely to cause harm or distress.⁵

5. This Category sets the minimum Protective Marking of each individual record and hence of any collection of records as PROTECT – PERSONAL DATA (P-PD). Note this is not an exhaustive list, TLB/TF PSyAs (Principal Security Advisers) and supplier SIROs, in conjunction with the relevant IAOs, should determine whether other information they hold should be treated in the same way.

⁵ DPA 98 is limited to living persons. MOD holds significant records relating to individuals who are deceased, but whose compromise might cause harm or distress to relatives and reputational damage to the department. An impact assessment should be made of the consequences of loss and the data protected accordingly.

1. One or more of the pieces of information which can be used along with public domain information to identify an individual	combined with	2. Information about that individual whose release is likely to cause harm or distress
Name / address (home or business or both) / postcode / email / telephone numbers / driving licence number / date of birth [Note that driving licence number is included in this list because it directly yields date of birth and first part of surname]		Sensitive personal data as defined by s2 of the Data Protection Act, including records relating to the criminal justice system, and group membership DNA or finger prints / bank, financial or credit card details / mother's maiden name / National Insurance number / tax, benefit or pension records / health records / employment record / school attendance or records / material relating to social services including child protection and housing.

Category B: Any COLLECTION of information about large numbers of identifiable individuals, other than information sourced from the public domain

6. This could be a database containing 1000 or more entries, or an electronic folder or drive containing records about 1000 or more individuals, or a paper-based system containing entries about 1000 or more individuals, containing facts derived from, or equivalent to, the types of information in the left-hand column of the Category A Table above⁶. Information on smaller numbers of individuals may justify equal protection because of the nature of the individuals, source of the information, or extent of information. The effect of such aggregation on Impact Levels is shown in Annex B along with the reducing effects of encryption.

⁶ This information about a single individual would neither attract a Protect-Personal Data protective marking or be considered IL2.

Guidelines on Associating Impact Levels with Aggregations of Personal Data

1. These guidelines apply to personal records held on removable media, on paper and on servers in transit. Where personal records are held on servers in a data centre reference should be made to the policy and guidance in DIAN 16.

Highest Protective Marking of individual record	Level of encryption	Number of records	Minimum 'Handle As' Impact Level
Not Protectively Marked (NPM)	Approved or Acceptable products ⁷	any	IL0
Not Protectively Marked (NPM)	Unencrypted	<1000	IL0
Not Protectively Marked (NPM)	Unencrypted	≥1000	IL2
PROTECT- PERSONAL DATA	Approved products	Any	IL0
PROTECT- PERSONAL DATA	Acceptable products	Any	IL2
PROTECT- PERSONAL DATA	Unencrypted	<1000	IL2
PROTECT- PERSONAL DATA	Unencrypted	1000 to 9999	IL3
PROTECT- PERSONAL DATA	Unencrypted	10,000 to 99,999	IL4
PROTECT- PERSONAL DATA	Unencrypted	≥100,000 ⁸	IL5
RESTRICTED-PERSONAL DATA	Approved product	Any	IL0
RESTRICTED-PERSONAL DATA	Acceptable product	Any	IL3
RESTRICTED-PERSONAL DATA	Unencrypted	<1000	IL3
RESTRICTED-PERSONAL DATA	Unencrypted	1,000 to 99,999	IL4
RESTRICTED-PERSONAL DATA	Unencrypted	≥100,000	IL5

⁷ Approved and Acceptable encryption products are defined and listed in DIAN 15

⁸ IS6 requires such volumes of records to be subject to Penetration Testing

Handling/Access Rules for Personal Data

Minimum 'Handle As' Impact Level⁹	Format information held in	Personnel security	Physical security	Postal/courier transmission¹⁰	Accounting / mustering¹¹
0 - 3 ¹²	Electronic media	BPSS	Lock and Key	Follow procedure for SECRET	Quarterly
0 - 3 ¹³	Paper	BPSS	Lock and Key	Follow procedure for RESTRICTED	N/A
4	Any	BPSS	Class 3 Lock and Class 3 Container	Follow procedure for SECRET	Quarterly
5	Any	SC	Class 3 Lock and Class 3 Container	Follow procedure for SECRET	Quarterly

⁹ From Annex B

¹⁰ Where an encrypted device is involved the encryption key and any passwords should be transmitted separately

¹¹ This applies only to electronic media

¹² Where both the original information and 'handle as' impact level are IL0 these measures do not have to be applied.

¹³ Where both the original information and 'handle as' impact level are IL0 these measures do not have to be applied.

Personal Data Aspects Letter for Contracts involving the handling of Protected Personal Data

Messrs

For the personal attention of:

(Name of company Data Controller)

Dear Sir

TENDER NO / CONTRACT NO (to be inserted by the Contracts staff)

On behalf of the Secretary of State for Defence, I hereby give you notice that the Privacy Impact Assessment conducted has identified that this contract involves the requirement to handle MOD personal data. This data is subject to the provisions of the Data Protection Act 1998,¹⁴ the Data Handling Review,¹⁵ and Security Policy Framework.¹⁶ Your attention is also drawn to the specific aspects of personal data handling set out in Industry Security Notice 2010/01 which must be fully implemented.

Will you please confirm that:

- a. This definition of the personal data aspects of the above contract has been brought to the attention of the person directly responsible for the protection of data in this contract.
- b. The definition is fully understood.
- c. Measures can, and will, be taken to protect the personal data.
- d. Any problems in meeting these requirements will be notified to MOD immediately.

Yours faithfully

Copy to:

CIO-Advisor

¹⁴ http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

¹⁵ http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

¹⁶ <http://www.cabinetoffice.gov.uk/spf.aspx>

IT Systems and Data Warehouses

Key Principles

1. Designers of IT Systems and Data Warehouses need to take account of the aggregation effect for similar reasons to the more traditional document archive, i.e. the potential catastrophic impact to the organization should there be a compromise to the confidentiality, integrity or availability of the data.

2. During an IS1 Risk Assessment, the Business Impact of compromise of the aggregated information rather than the individual items should be considered, and controls considered case-by-case and an assessment made to determine whether enhanced controls would be appropriate.

3. The following steps are illustrative and should be conducted as part of the standard risk assessment, mitigation and accreditation processes in accordance with IS1 and IS2.

Step 1: Consider Business Impacts and Threats as Part of an IS1 Analysis

Business Impacts

4. The aggregation effect will invariably increase the Business Impact Levels of compromise of Confidentiality, Integrity and Availability via accumulation and/or association.

Threats

5. IS1 analysis uses the Threat and Business Impact levels to produce a Risk Level. Aggregation of low Business Impact Level data, particularly via the association of disparate elements of information, may attract a higher level of threat. For example, while individually all of the commercial emails on a military project may have a low level of interest to a threat source, when accessible from one folder they may provide a detailed picture of the project and hence be very attractive to a Foreign Intelligence Service, commercial competitor or investigative journalist.

Step 2: Review the Business Case.

6. Assess whether there is a valid business requirement to aggregate all the data in one place. Assess whether the information management measures are appropriate – e.g. whether information is being retained for unnecessarily excessive periods or on subjects unrelated to the business function.

Step 3: Draw up Mitigation Plans in Accordance with IS1 and IS2

7. In drawing up the plans consider using a mix of personnel, physical, procedural and technical measures.

8. Some controls, notably link encryption, assume that if the control were to be defeated then a large amount of information would be compromised; the design of the control already takes aggregation into account. However, not all controls are designed this way and may not account for aggregation, or do so only partially. The principle to apply is whether, if the control were to be defeated, an attacker would compromise only one item of data or compromise an aggregate of data.

Personnel Measures

9. Additional personnel security controls can be applied to mitigate risks arising from aggregation. For example, if the individual items are protectively marked no higher than RESTRICTED, the minimum personal security clearance would be no higher than BPSS, but if the result of aggregation indicates an Impact Level for the database of IL5 then clearing appropriate staff to Security Check would help mitigate the risk.

10. Personnel with special privileges, such as System Managers and System Administrators, are in a unique position of responsibility; where they have responsibility for systems processing information which has a high implied Impact Level (or is highly critical to the business) then clearing such staff to Developed Vetting would help mitigate the risk.

Physical Measures

11. Simple physical controls may mitigate the risk e.g., placing strong door and locks on the server rooms where the database resides with appropriately limited access to keys and/or combinations.

Procedural Measures

12. Assess whether procedural measures can mitigate the risk e.g. monitoring and ensuring staff: follow Security Operating Procedures with regard to the use of laptops containing aggregated databases and removable media; introduce a "two man rule" for critical activities; improve the Business Continuity Plan (e.g. increase back-ups), or provide more configuration control.

Technical Measures

13. Technical measures may help mitigate the risk, e.g. implementing a technical barrier – such as a Firewall – to protect an IL3 database, assessed as IL5 by aggregation. Enforcing Mandatory Access Controls may prove effective in restricting access to all the information on a database to a specific set of authorised users.

14. Extensive system accounting and audit can provide an early indication of unauthorized attempts to access, modify, delete or export data. This is of particular relevance when dealing with either information at the higher Protective Markings or Personal Data.

DIAN 15 INDUSTRY LITE version for ISN 2010-01

Ministry of Defence

Defence Security Division

Information Security



DOCUMENT TYPE:	DEFENCE INFORMATION ASSURANCE NOTICE	
DOCUMENT NUMBER:	DIAN 15 Industry Lite Version	
DOCUMENT TITLE:	Encryption of CIS Media	
AUTHOR:	DefSy InfoSy 1	
VERSION:	6	
DATE:	26 August 2010	
DOCUMENT HISTORY:	Versions 1.0 to 5 MOD INTERNAL USER INFO ONLY	20 Jun 08 11 Aug 08
	Version 6: APPLICABLE TO INDUSTRY ONLY DIAN 15 INDUSTRY LITE version for ISN 2010-01	26 Aug 10
CHANGES FORECAST:	As new methods of encryption are identified and approved	

© Crown Copyright 2009. All Rights Reserved

INTRODUCTION

1. **Objectives of DIAN.** Defence Information Assurance Notices LITE (DIAN Lite) are issued by MOD DefSy InfoSy to give guidance or provide standards on specific technical aspects of Communications and Information Systems (CIS) security.
2. **Readership.** Information contained within DIAN 15 Lite is intended primarily for Industry IT-CIS Security or Specialist Staff, and Industry staff with responsibility for the handling or protection of MOD data or information on removable media.
3. **Points of Contact.** Any questions relating to this DIAN Lite should be addressed to:
DefSy InfoSy 1
MOD Main Building Floor 1.I.25
Horseguards Avenue, LONDON, SW1A 2HB
Tel: 020 7218 3994, Fax: 020 7218 9078, Email: DBR-DefSy-InfoSy1@mod.uk

ABOUT THIS DIAN Lite

4. **Implementation of Policy.** This DIAN Lite provides guidance on the methods of encryption, which may be used to fulfil the requirements of Industry Security Notice (ISN) 2010-01 for the encryption of media (floppy disks, CD/DVD, USB Sticks, SD/XD cards, PC (PCMCIA) Cards and External Hard Drives), used for external storage, archival or data transfer purposes of Personal Data. This DIAN Lite does not provide guidance on the encryption of laptops, internal hard disk drives or removable hard disk drives.
5. **Scope of Implementations.** This DIAN identifies methods of encryption, which may be selected by IT System Owners. System Owners are advised to consult with their own IT Security or Specialist staffs and if necessary with the Contracting Authority IT Security Staff before selecting products and implementation methods.
 - a. Where media are required to be distributed, care will need to be taken that the recipients are able to decrypt the media. Some methods of encryption provide “self-extractor” or “readers” to enable recipients to decrypt information without the application that encrypted it.
 - b. The MOD’s Chief Information Officer (CIO) is overseeing the adoption of MOD-wide corporate implementation of encryption methods that are deemed to satisfy MOD-wide business requirements or that would otherwise benefit the MOD. These are :
 - (1) **SDMS AES LOCK Encrypted USB Stick:** for regular personal data transfer and storage up to and including SECRET.
 - (2) **BeCrypt Media Client Baseline:** for the encryption of files on CD/DVD up to and including SECRET. It may also be used to encrypt files on USB memory sticks and USB connected hard disk drives up to and including RESTRICTED.
 - (3) **Stonewood Eclipt Freedom:** for regular bulk data transfer and temporary storage up to and including TOP SECRET.
 - (4) **WinZip Version 10 (or later):** for the encryption of floppy disks at RESTRICTED and below.

The use of these corporate solutions is not mandatory. However, since they will have been chosen to enable interoperability across the MOD IT estate it can be expected that most MOD IT workstations will be configured, so that the corporate solution USB sticks

and external hard drives will be usable and so that CD/DVDs encrypted in the corporate solution will be widely readable.

c. Implicitly, all the methods of encryption identified in this DIAN Lite are supported only by Microsoft Windows Operating Systems. System Owners wishing to encrypt CIS media on computers using other Operating Systems should consult the Author.

6. Limitations.

a. **Mass Storage Media.** This DIAN Lite offers guidance on the encryption of some types of Mass Storage media, such as SD/XD cards and PC (PCMCIA) Cards. It should be noted that the guidance applies only where the medium appears to the Operating System of the computer as a Mass Storage device or as a Removable Disk drive. System Owners should arrange for a test that the encryption method recognizes such media as able to receive encrypted data before making a commitment to the encrypted use of the media: feedback to the Author will be appreciated.

b. **Magnetic Storage Tapes and Magneto-Optical Drives.** This DIAN Lite does not specify any encryption methods for encrypting magnetic storage tapes or magneto-optical drives. Where there is a requirement to encrypt these media, IT System Owners should investigate the suitability and availability of commercially available encryption methods. Encryption products with a FIPS 140 or equivalent certificate will be acceptable, provided that the encrypted media are stored, handled and distributed in accordance with the Protective Marking of the original information. Further advice should be sought from the Author.

All MOD Industry Contracted Companies to whom this DIAN Lite applies are reminded that any inability to comply with the requirements of ISN 2010-01 and this DIAN Lite requires them to immediately notify the Contracting Authority of the non compliance.

DEFINITIONS

7. Levels of Encryption. In this DIAN Lite, levels of encryption are defined as:

a. **Approved.** “Approved encryption” products have been evaluated by CESG (the National Technical Authority) as meeting criteria for the encryption of Protectively Marked information at specified levels and the subsequent reduction of Protective Marking by a defined number of levels for storage, handling and distribution. ***Methods of Approved encryption are shown at Tables 1- 4 and should be used in preference to the Acceptable methods.***

b. **Acceptable to MOD.** “Encryption acceptable to MOD” has been assessed by MOD as meeting minimal criteria, so that MOD may comply with UK Government policy that removable media are encrypted. **Note that: “Acceptable encryption” does not change the Protective Marking of information.** Methods of encryption, which are acceptable to MOD, are shown at Tables 5 - 7. Where business requirements and restraints on the configuration of IT systems prevent the use of the **Approved** encryption methods, these **Acceptable** encryption methods may be used instead.

8. **Protective Marking.** The Protective Marking shown at Column (c) of all Tables should be assumed to be the result of assessing the cumulative Protective Marking of separate items

of sensitive information in accordance with MOD Information Security Policy. This is most likely to affect information marked PROTECT PERSONAL DATA.

GUIDANCE

9. Encryption of Floppy Disks.

- a. Approved encryption for floppy disks is listed in Table 1.
- b. Acceptable encryption for floppy disks is listed in Table 5.

10. Encryption of Mass Storage Media - USB Sticks, SD/XD cards and PC (PCMCIA) Cards.

- a. Approved methods of encryption for Mass Storage media - USB Sticks, SD/XD cards and PC (PCMCIA) Cards - are listed in Table 2.
- b. Acceptable methods of encryption for USB sticks only are listed in Table 6.
- c. It should be noted that these methods are only for USB sticks with solid state flash memory: hard drives with USB interfaces are covered under External Hard Drives.

11. Encryption of CD/DVD.

- a. **Approved** encryption for CDs and DVDs are listed in Table 3.
- b. **Acceptable** encryption for CDs and DVDs are listed in Table 7.

12. **Encryption of External Hard Drives.** **Approved** methods of encryption for external hard drives are listed in Table 4. There are no **Acceptable** of encryption for external hard drives. It should be noted that removable hard drives are required to be encrypted in accordance with security policy for Portable CIS.

13. Other Methods of Encryption.

- a. **Approved.** The list of Approved encryption methods at Tables 1 -4 is intended to be complete. Omissions should be notified to the Author as soon as convenient.
- b. **Acceptable.** The list of encryption methods Acceptable to MOD at Tables 5 – 7 may not be complete. The Author will welcome suggestions for assessment, especially where IT System Owners have already made plans to use a method, which is not listed there. After assessment, special permission may be granted for continued use or the method may be included in further versions of this DIAN.

INSTRUCTIONS FOR USE OF PRODUCTS

14. MOD Approved Products. Instructions for the following products are provided in the Vendors' User Instructions.

- a. BeCrypt DISK Protect Baseline - both Password Only and Token Authentication variants.
- b. BeCrypt DISK Protect Enhanced.
- c. BeCrypt Media Client Baseline.
- d. Stonewood Ecrypt Freedom Enhanced, Baseline and Baseline Plus.
- e. Check Point Media Encryption.

15. AES LOCK Encrypted USB Sticks. Instructions for the use of the Secure Data Media Solutions Ltd (SDMS) AES LOCK Encrypted USB Sticks will be provided by the Vendor's User Instructions.
16. PGP Zip. PGP Zip is part of the PGP Desktop product and is used to create encrypted files or "zipped archives" for transfer onto CIS media. It can use both passwords and Public Key Cryptography (PKC) for encryption; the PKC option is preferred. PGP Zip is under evaluation by CESG if and when **Approval** is given an addendum DIAN Lite-Memo will be published.
17. External Hard Drives. Because external hard drives are to be Protectively Marked in accordance with the highest or the cumulative Protective Marking of unencrypted information. They may be stored handled and distributed in accordance with the Protective Marking of Information after Encryption shown in Column (d) of Table 4 at Annex A. Exceptionally, Eclipt Freedom external hard drives storing encrypted RESTRICTED and PROTECT information require no Protective Marking.

Tables:

Tables 1, 2, 3 and 4 – Approved Methods of Encryption for Floppy Disks, Mass Storage Media, CD/DVD and External Hard Drives.

Tables 5, 6 and 7 – Acceptable Methods of Encryption for Floppy Disks, USB Sticks and CD/DVD.

Tables 1, 2, 3 and 4 –Approved methods of encryption for floppy disks, mass storage media, CD/DVD and external hard drives

Table 1: Encryption of Floppy Disks					
Serial	Encryption Product	Highest Protective Marking	Protective Marking of Information after Encryption	Availability	Remarks
(a)	(b)	(c)	(d)	(e)	(f)
1	BeCrypt DISK Protect Baseline	CONFIDENTIAL	One level lower than original information	Through MOD ICS Catalogue or Manufacturer	Requires version 3.1 onwards. At CONFIDENTIAL, the Password Only variant is to be used only for encrypting the floppy disk.
2	BeCrypt DISK Protect Enhanced	TOP SECRET	One level lower than original information	Through MOD ICS Catalogue or Manufacturer	Requires version 3.04 onwards.

Table 2: Encryption of Mass Storage Media - USB Sticks, SD/XD cards and PC (PCMCIA) Cards					
Serial	Encryption Product	Highest Protective Marking	Protective Marking of Information after Encryption	Availability	Remarks
(a)	(b)	(c)	(d)	(e)	(f)
1	BeCrypt DISK Protect Baseline	CONFIDENTIAL	One level lower than original information	Through MOD ICS Catalogue or Manufacturer	Requires version 3.1 onwards. At CONFIDENTIAL, the Password Only variant is to be used only for encrypting the mass storage medium.
2	BeCrypt DISK Protect Enhanced	TOP SECRET	One level lower than original information	Through MOD ICS Catalogue or Manufacturer	Requires version 3.04 onwards
3	BeCrypt Media Client Baseline	RESTRICTED	NPM	Through MOD ICS Catalogue or Manufacturer	

Table 3: Encryption of CDs and DVDs					
Serial	Encryption Product	Highest Protective Marking	Protective Marking of Information after Encryption	Availability	Remarks
(a)	(b)	(c)	(d)	(e)	(f)
4	BeCrypt Media Client Baseline	UK SECRET ¹⁷	RESTRICTED becomes NPM CONFIDENTIAL and SECRET as original information	Through MOD ICS Catalogue or Manufacturer	

¹⁷ If information owned by international organisations, e.g. NATO, is encrypted with UK encryption products, it should not be distributed outside UK without the permission of the appropriate international Security Authority.

Table 4: Encryption of External Hard Drives					
Serial	Encryption Product	Highest Protective Marking	Protective Marking of Information after Encryption	Availability	Remarks
(a)	(b)	(c)	(d)	(e)	(f)
5	BeCrypt DISK Protect Baseline	CONFIDENTIAL	One level lower than original information	Through MOD ICS Catalogue or Manufacturer	Requires version 3.1 onwards. At CONFIDENTIAL, the Password Only variant is to be used only on the external hard drive.
6	BeCrypt DISK Protect Enhanced	TOP SECRET	One level lower than original information	Through MOD ICS Catalogue or Manufacturer	Requires version 3.04 onwards
7	BeCrypt Media Client Baseline	RESTRICTED	NPM	Through MOD ICS Catalogue or Manufacturer	
8	Stonewood Eclipt Freedom Baseline	RESTRICTED	NPM	Through MOD ICS Catalogue or Manufacturer	
9	Stonewood Eclipt Freedom Baseline Plus	CONFIDENTIAL	CONFIDENTIAL becomes RESTRICTED Others become NPM	Through MOD ICS Catalogue or Manufacturer	
10	Stonewood Eclipt Freedom Enhanced	TOP SECRET	Two levels lower than original information	Through MOD ICS Catalogue or Manufacturer	

Tables 5, 6 and 7 – Acceptable methods of encryption for floppy disks, USB sticks and CD/DVD

Table 5: Encryption of Floppy Disks					
Serial	Encryption Product	Highest Protective Marking	Protective Marking of Information after Encryption	Availability	Remarks
(a)	(b)	(c)	(d)	(e)	(f)
11	Check Point Media Encryption	RESTRICTED	As original information	Through MOD ICS Catalogue or Manufacturer	Formerly called Reflex DiskNet Pro and Check Point Media Encryption and Point Protection (MEPP).
12	WinZip 10 onwards	RESTRICTED	As original information	Through MOD ICS Catalogue or Manufacturer	Should be used only if Serial 1 is not suitable or available. Instructions for use are available from DBR-DefSy-InfoSy 1.

Table 6: Encryption of USB Sticks					
Serial	Encryption Product	Highest Protective Marking	Protective Marking of Information after Encryption	Availability	Remarks
(a)	(b)	(c)	(d)	(e)	(f)
13	Check Point Media Encryption	RESTRICTED	As original information	Through MOD ICS Catalogue or Manufacturer	Formerly called Reflex DiskNet Pro and Check Point Media Encryption and Point Protection (MEPP).
14	Lumension Security Sanctuary Device Control	RESTRICTED	As original information	Through MOD ICS Catalogue or Manufacturer	Requires version 4.3.2 onwards.
15	SDMS AES LOCK Encrypted USB Stick	SECRET	As original information	Through MOD ICS Catalogue or Manufacturer	

Table 7: Encryption of CDs and DVDs					
Serial	Encryption Product	Highest Protective Marking	Protective Marking of Information after Encryption	Availability	Remarks
(a)	(b)	(c)	(d)	(e)	(f)
16	Checkpoint Media Encryption	RESTRICTED	As original information	Through MOD ICS Catalogue or Manufacturer	Formerly called Reflex DiskNet Pro and Check Point Media Encryption and Point Protection (MEPP)
17	PGP Zip using Public Key Cryptography (PKC) for Key Management	RESTRICTED	As original information	Commercially available From manufacturer	Follow CESG guidance on use.
18	Lumension Security Sanctuary Device Control	RESTRICTED	As original information	Through MOD ICS Catalogue or manufacturer	Requires version 4.3.2 onwards.