EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate HR.DS - Security
Informatics Security

Brussels, 21/06/2011
HR.DS5/GV/ac ARES (2011) 663475
SEC20.10.05/04 - Standards

European Commission

Information System Security Policy

C(2006) 3602

STANDARD ON SANITISATION OF MEDIA

ADOPTED BY MRS. IRENE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON 21/06/2011

Version 07/03/2010

TABLE OF CONTENTS

1. ADOPTION PROCEDURE 3

2. INTRODUCTION 3

3. OBJECTIVES 3

4. SCOPE 4

5. BACKGROUND INFORMATION 4

6. IMPORTANT DEFINITIONS 5

7. SECURE DISPOSAL OR RE-USE OF EQUIPMENT 7

7.1. Risks 7

7.2. General rules 7

7.3. Purging 8

7.4. Destruction 8

7.5. Specific to media storing EU Classified information 9

7.6. Overwriting 9

7.7. Documentation 10

8. CLASSIFICATION LEVEL OF MEDIA AND SANITISATION DECISION 10

9. DECISION TABLES FOR SANITISATION TECHNIQUES AND METHODS 12

9.1. Decision tables for sanitisation techniques and methods for media 12

9.2. Decision table for secure disposal of paper documents 12

9.3. Table 1 — Sanitisation techniques for media (not paper) 13

9.4. Table 2 — Sanitisation methods for media (not paper) 14

9.4.1. Notes on "Table 2 — Sanitisation methods for media" 15

9.5. Table 3 — Secure disposal of paper documents 16

10. ROLES AND RESPONSIBILITIES 17

11. REFERENCES 17

1. ADOPTION PROCEDURE

This Security Standard is adopted in accordance with Article 10(3) of Commission Decision C(2006) 3602 concerning the security of information systems used by the European Commission, adopted on 16 August 2006.

It is drawn up under the responsibility of the Security Directorate pursuant to Article 9(1)(b) and takes into account the items listed in Article 10(2) of Commission Decision C(2006)3602, in particular internationally recognised norms and standards applicable in the field of information systems security.

Under Article 10(3) of Commission Decision C(2006) 3602, the implementing rules may be supplemented by measures of a technical, physical, procedural or organisational nature proposed by the Director of the Security Directorate and adopted by the Director-General of the Directorate-General Human Resources and Security in consultation with departments that have a legitimate interest. These supplementary measures are called 'security standards' where their application is mandatory, or 'security guidelines' where their application is optional or where they provide guidance on security standards implementation.

2. INTRODUCTION

To protect the confidentiality of sensitive[1] or EU classified information, all documents, media and devices containing such information must be properly sanitised when they reach the end of their lifetime.

Sanitisation is the process of erasing or destroying electronic data from information technology resources and associated storage media (hard drives, diskettes, tapes, CD-ROMs, DVDs, etc) in a manner that gives reasonable assurance that the information cannot be recovered. Sanitisation includes the removal of data from the storage device, as well the removal of all labels, markings, and activity logs.

Data that has been improperly or unsuccessfully removed from media could be re-created by attackers or by unauthorised individuals.

Consequently, the process of sanitisation is particularly critical when sensitive media are transferred, become obsolete or no longer required by an information system. The recovery or reconstruction of data from the residual magnetic, optical or electrical representation on the media must be prevented.

3. OBJECTIVES

This standard provides detailed instructions for the deletion of sensitive/EUCI data and/or for the destruction and disposal of the media used to store this data. Disposal of paper documents is also covered.

---

[1] In the rest of the document "sensitive" indicates information that is classified as LIMITED HIGH or higher.

4. SCOPE

This standard applies to:

– EUCI and media used for its storage.

– Data classified as "LIMITED HIGH" and "LIMITED BASIC" (see art 3.4 of the Implementing Rules of C(2006)3602) and media used for its storage.

Media classified as Public are also in scope, but there is no requirement for their sanitisation.

In addition, secure disposal of paper documents is covered in line with EUCI requirements.

5. BACKGROUND INFORMATION

The Commission provisions on security of the Commission decision 2001/844/EC, ECSC, Euratom do not provide detailed instructions for the destruction of EU classified data but the following security notices lay down the main rules.

- Security Notice 2 – paragraph 2.11 – (only for RESTREINT UE)

  Destruction of RESTREINT UE documents

  (1) They must never be disposed of in normal office waste bin/bags without having been shredded. The standard shredder used in the Commission is acceptable for this purpose.

  (2) The shredded document may be disposed of in normal office waste bin/bags.

  (3) Computer storage media should be given to the Registry Control Officer or Local Security Officer for destruction and disposal.

  (4) If so wished, the Director General/Head of Service may delegate performance of this task to the Local Security Officer or other named individual.

- Security Notice 4 – paragraph 2.10 – (only for CONFIDENTIEL UE) and Security Notice 4A (only for SECRET UE).

  Destruction of CONFIDENTIEL UE and SECRET UE documents

  (1) They must never be disposed of in normal office waste bin/bags.

  (2) They may only be destroyed by the Registry Control Officer in the registry where they are registered; using one of the processes indicated in paragraph (3).

(3) All documents and computer media must be destroyed by burning, pulping, shredding or otherwise reducing into an unrecognisable and non reconstitutable form.

(4) Where a shredder is used, it shall have been approved for the purpose by the Commission Security Directorate.

(5) Destruction shall only be carried out within the security area by the Registry Control Officer, acting under the supervision of the Local Security Officer.

(6) The destroyed document shall de disposed of by the Registry Control Officer.

(7) CONFIDENTIEL UE and SECRET UE documents that are destroyed shall be recorded on signed destruction certificates to be retained by the Registry, together with the distribution forms, for at least three years.

6. IMPORTANT DEFINITIONS

Declassification: an administrative decision/action, based on a consideration of risk by the owner, whereby the classification of a properly sanitised storage device or the information itself is downgraded to UNCLASSIFIED.

Recycling: end state for IS storage devices processed in such a way as to make them ready for reuse, adapt them to a new use, or to reclaim constituent materials of value.

Data remanence: residual physical representation of data that has been erased in some way. After storage media are erased there may be some physical characteristics that allow data to be reconstructed.

Coercive force: a negative or reverse magnetic force applied for the purpose of reducing magnetic flux, used as a method of sanitising magnetic media.

Keyboard attack – an attack that consists in extracting information from data storage media by executing software utilities, keystrokes, or other system resources executed from a keyboard. For example, disk and file recovery utilities and memory scavenging procedures can be used to carry out keyboard attacks. A countermeasure to keyboard attack is: to overwrite or remove data storage media, thereby making information unavailable to users employing normal system capabilities. An alternative name for "keyboard attack" is "operating system recovery". A keyboard attack can be performed without specialist equipment, unlike a Laboratory attack.

Laboratory attack – involves using non-standard systems or signal processing equipment by specially trained personnel to conduct data recovery on media (possibly disassembled) outside their normal operating environment. Laboratory attacks can sometimes recover data that cannot be recovered with a keyboard attack

Classification level of a storage medium –is the maximum confidentiality level of the information/data that may be stored and protected on this medium by all the security measures approved in the security plan(s)[2] by the system owner(s) and implemented by the system provider. These measures are the result of the information classification and risk management to ensure the adequate level of protection for the business context of the information system(s) using or sharing the storage medium, i.e. business purposes, security context (e.g. usage of logical access control) or organisation units[3] related to the media information. It is used as a reference for the decision about the level of sanitisation.

Techniques and methods of media sanitisation

- **Disposal** – act of discarding media with no other sanitisation considerations. This is often used to dispose of media that contain only non-sensitive information. On the other hand, "**secure disposal**" means some form of sanitisation or even destruction before actual disposal.

- **Clearing** – method of media sanitisation that consists in erasing data so that it cannot be retrieved by keyboard commands. Clearing protects information from a robust keyboard attack but not from a laboratory attack so that it must not allow information to be retrieved by data, disk or file recovery utilities. Deletion of items using simple erase commands of the operating systems is not sufficient for clearing. Overwriting with random data is the most common and acceptable method used; however, overwriting is not possible for media that are damaged (partially or totally) or not writeable (read only media).

- **Purging** – method of media sanitisation that consists in erasing data so it is unlikely that a laboratory attack can recover the data. Possible methods of purging are degaussing and the firmware "Secure Erase" command (for supported drives only). If purging media is not a reasonable sanitisation method, it is recommended that the media be destroyed.

- **Destruction** – Destruction of media is the ultimate form of sanitisation. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverising, shredding, and melting.

- **Overwriting** – overwriting media is an acceptable method for clearing media and for purging in some cases. Overwriting cannot be used for media that are damaged or that are not suitable for overwriting (read only media).

- **Degaussing** – degaussing (or demagnetising) is a purging method that exposes the magnetic media to a strong magnetic field (coercive force) from a permanent magnet or electromagnetic coil to render any previously stored data unreadable

[2] Plural in case of media storing information from different information systems or under the accountability of different system owners.

[3] Organisation entity or set or organisation entities in the scope and boundaries of the information systems related to the storage media as defined in the security plan.

and unintelligible, and to ensure that it cannot be recovered by technology known to exist. Degaussing may be an effective method for purging damaged media, for purging media with exceptionally large storage capacities or for quickly purging diskettes. Degaussing cannot be used to purge nonmagnetic media, such as optical media (e.g. CD or DVD). However, degaussing of any drive assembly may permanently damage the drive because the firmware data that manages the device is also destroyed.

7. SECURE DISPOSAL OR RE-USE OF EQUIPMENT

Policy objective 4.2.4 – Secure disposal or re-use of equipment – All items of equipment containing storage media, either must be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or sending back for repair, or must be securely destroyed.

Policy objective 5.7.2 – Disposal of media – Media must be disposed of securely and safely when no longer required, using formal procedures.

7.1. Risks

- Information can be compromised through careless disposal or re-use of equipment.
- Sensitive information could be disclosed through careless disposal of media. Removable media include tapes, disks, flash disks, removable hard drives, CDs, DVDs and printed media.

7.2. General rules

(1) During its lifecycle the storage media of an information system can be reused, released or destroyed. In addition, stored or processed EU classified or sensitive information may be downgraded or declassified. Thus procedures must be developed for proper sanitisation of media to make sure the information is always protected according to its classification:

(a) Media containing sensitive information must be sanitised using techniques to make the original information non-retrievable rather than using the standard delete or format function.

(b) A check for successful sanitisation must be done before the devices or media leave ("déclassement") the Commission.

(2) At the start of information system development, as soon as the initial security plan is developed, media sanitisation controls (methods and techniques) and any related contractual agreements[4] must be identified, developed and documented to be deployed later.

[4] In case the sanitisation is outsourced to an external company.

(3) In keeping with sound practices, EC information resources must be conserved and media must be reused whenever possible.

(4) Individuals involved in sanitising computer equipment must check all components and peripherals for removable media to be sanitised, i.e. cleared, purged, destroyed and/or disposed (e.g. remove the computer case to check for additional removable media).

(5) Procedures must be in place to identify the items that might require secure disposal:

(a) It may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items.

(b) Many companies offer collection and disposal services for papers, equipment and media; care must be taken in selecting a suitable contractor with adequate controls and experience.

(c) Disposal of sensitive items must be logged where possible in order to maintain an audit trail.

7.3. Purging

(6) Purging media must be done in accordance with the methods for the specific media (see table 2 — sanitisation methods). Note: routines that only remove pointers and leave data intact (i.e. standard delete or format commands) are not acceptable methods of purging media.

(7) The success of purging must be assured:

(a) Either by using tools or material that have been certified for purging in accordance to requirements.

(b) Or by obtaining a formal certificate from an external company contractually engaged for the purpose of data purging.

(c) Or by reviewing the media for data retention in other cases. For example, if an overwrite routine is used to purge an information system hard disk, dump random short sectors, blocks, or memory contents and verify that only the last character written is all that can be read.

7.4. Destruction

(8) Methods for destroying media include shredding, smelting, incinerating, disintegrating, applying acid solutions, etc., to ensure that data cannot be retrieved by any currently known methods. All methods for destruction and the possible usage of metal destruction facility must be approved by the System owner.

(9) Damaged storage media[5] with a classification level of LIMITED HIGH and higher must be physically destroyed rather than sent for repair or discarded unless

[5] Including media that failed to be successfully or completely cleared or purged.

contractual agreements give assurance that the supplier performs the required level of sanitisation.

(10) Media with a classification level of LIMITED HIGH and higher must be purged before submitting them to destruction. In case purging is not possible, the media must be protected in line with their classification level until they are completely destroyed.

(11) If sensitive media are securely transported to an external company for secure disposal, a signed report must be delivered certifying their destruction.

7.5. Specific to media storing EU Classified information

(12) For the specific sanitising actions concerning media with a classification level "TRES SECRET UE/EU TOP SECRET", HR.DS must be contacted for guidance. Consequently, the rules that follow in this section 7.5 on "EU Classified" are not applicable to "TRES SECRET UE/EU TOP SECRET" media.

(13) Media with a classification level "EU classified" that will be released from the EU classified environment must be purged. EU classified media or formerly EU classified media must not be used in unclassified environments without being purged.

(14) When the destruction of media with a classification level "EU classified" is required the selected destruction technique must give assurance that it precludes recovery of any of the information they contained.

(15) Purged computer equipment must be affixed with a signed label verifying that the equipment has been purged. At minimum, labels must:

- Describe the equipment.
- Provide a statement indicating that the equipment has been purged in accordance with requirements of this standard.
- Record the date, the printed name and the signature of the certifier.

7.6. Overwriting

(16) Overwriting is an acceptable method for clearing or purging many types of storage media. The overwriting may be implemented by a commercial service, or locally developed or acquired computer program or routine that must be certified to comply with the following:

(a) The read and write device hardware is functioning properly before proceeding with the overwriting procedure.

(b) Overwrite programs must write to every addressable location on the storage media. In case of magnetic disks, for example, the program must write to active and inactive file space, bad sectors and tracks, the space between the end of file, or the end of a block or sector, file allocation tables, directories, block maps, etc.

(c) The overwrite program must perform the clearing and purging as described for the storage medium type.

(17) Overwritten media must be checked to verify that the overwriting process has been successfully completed.

(18) Before using storage media for the first time, it is advisable to overwrite the media with an unclassified data pattern to help prevent recovery of data stored later.

(19) Table 2 on methods for sanitising must be consulted for the requirements for overwriting based on storage media type and the sanitising technique (clearing or purging). It also gives the required number of passes of overwriting depending on the data classification.

7.7. Documentation

(20) It is critical that a record of sanitisation of sensitive media (LIMITED HIGH and above) is maintained to document what media were sanitised, and the final disposition of the media.

8. CLASSIFICATION LEVEL OF MEDIA AND SANITISATION DECISION

As defined in the section on definitions, the classification level of a storage medium is the maximum confidentiality classification of the information that may be stored on this medium as a result of all the security measures approved in the security plan(s)[6] by the system owner(s) and implemented by the system provider. These measures are the result of the information classification and risk management to ensure the adequate level of protection for the business context of the information system(s) using or sharing the medium, i.e. business purposes, security context (e.g. usage of logical access control) or organisation units related to the medium information.

(21) In line with this definition, a storage medium must be sanitised in accordance with its classification level and the reason for sanitisation.

(22) A decision for sanitisation must be considered if the security context of the storage medium has been or will be changed, i.e. it is not possible to keep the complete set or a part of the security measures required by the system owner(s) for the protection of the medium and related information system(s).

(23) In case of a storage medium shared (logically and/or time-shared) by different types of information, with different access levels and/or under the accountability of different system owners, the (aggregated) classification level of the medium must be understood and approved by all the system owners via service level agreements with the service providers who must ensure a secure segregation via logical access control or equivalent security measures. These security measures

[6] Plural in case of a medium storing information from different information systems or under the accountability of different system owners.

are included in the (aggregated) security context of the storage medium approved by the system owners.

(24) A decision for sanitisation must be considered in the following and similar cases.

(a) The storage medium is removed and will not be re-used because it is not operational, at the end of the system life or phased out.

(b) The storage medium will no longer be under EC control: declared surplus, donated or resold outside the Commission.

(c) The storage medium is returned to the manufacturer or leasing company for warranty or repair without contractual agreement.

(d) The storage medium will be reused in a different business context: different business purpose, different organization and security context under the accountability of different system owners. Change of business context must be considered when the medium is to be used in a different organisational unit, for other business purposes and/or in a different security context (i.e. the security measures related to the medium classification or information segregation have been changed).

(e) Maintenance of device or medium performed in such a way that the information on the storage medium can be accessed by people who do not have the right level of clearance or need-to-know, or do not work under formal contractual agreements (with non-disclosure agreements).

(25) In case of media storing unclassified information that are reused for the same business context or for a higher level of access control or need to know, there is no need for sanitisation action unless the system owner decides that the media should be cleared.

(26) In case of media storing EUCI[7] that are reused for the same business context or for a higher level of access control or need to know, the sanitisation action must be Clearing or Purging at the discretion of the system owner.

(27) The confidentiality classification of the information stored on a storage medium must never exceed the classification level of the medium. If the confidentiality classification of the information stored on the storage medium becomes higher than the classification level of the medium (inadvertently or not), it must be sanitised in accordance with the confidentiality level of the information stored in error on the medium: Clearing for LIMITED BASIC or Purging (not destruction) for LIMITED HIGH and higher.

[7] Excluding TRES SECRET UE/EU TOP SECRET for which DS must be contacted for advice.

9. DECISION TABLES FOR SANITISATION TECHNIQUES AND METHODS

9.1. Decision tables for sanitisation techniques and methods for media

The following two tables summarise the minimum controls for the sanitisation of media. The two tables cover the techniques and methods of sanitisation respectively thus:

(1) First "Table 1 — Sanitisation techniques for media" shows the required technique for sanitisation (i.e. clearing, purging or destroying) based on the classification level of the media and the reason for sanitisation.

(2) Then "Table 2 — Sanitisation methods for media" gives the relevant physical method for sanitisation (for example: degaussing, overwriting, incinerating, shredding), based on the technique required in table 1 and the type of media.

9.2. Decision table for secure disposal of paper documents

Table 3 summarises the minimum requirements for secure disposal of paper documents.

9.3. Table 1 — Sanitisation techniques for media (not paper)

REASON FOR SANITISATION	CLASSIFICATION LEVEL OF MEDIA						
	PUBLIC	LIMITED BASIC	LIMITED HIGH	RESTREINT UE	CONFIDENTIEL EU	SECRET EU	TRES SECRET UE / EU TOP SECRET
No reuse: not operational, end of system life, phased out	No sanitising action	Clearing before Disposal	Purging before Disposal	Destruction after Purging (4)	Destruction after Purging (4)	Destruction after Purging (4)	Contact DS
Failed: partly (2) or completely	No sanitising action	No sanitising action before Disposal or Destruction (6)	Destruction after Purging (4)	Destruction after Purging (4)	Destruction after Purging (4)	Destruction after Purging (4)	Contact DS
Reuse in the same business context (i.e. business purpose, organisational units or security context) reuse for the same or higher level of access/control	No sanitising action	No sanitising action	No sanitising action or Clearing (3)	Clearing	Clearing or Purging (not destruction) (1) (5)	Clearing or Purging (not destruction) (1) (5)	Contact DS
Reuse for lower level of access/control or other business context (i.e. business purpose, organisational units or security context)	No sanitising action	Clearing	Purging (not destruction) (1)	Purging (not destruction) (1)	Purging (not destruction) (1)	Purging (not destruction) (1)	Contact DS
Not under EC control anymore: declared surplus, donation or reselling to other organisation, return to manufacturer/leasing company (for warranty, repair…) without contractual agreement	No sanitising action	Clearing	Purging (not destruction) (1)	Purging (not destruction) (1)	Purging (not destruction) (1)	Purging (not destruction) (1)	Contact DS
Maintenance or upgrade either by internal people, or by external people under supervision of internal people or under contractual agreement. Right level of clearance ensured in case of EUCI.	No sanitising action	No sanitising action	No sanitising action	No sanitising action	No sanitising action	No sanitising action	Contact DS
Maintenance or upgrade, either by internal people, or by external people under contractual agreement. Right level of clearance not ensured in case of EUCI	No sanitising action	No sanitising action	No sanitising action or Clearing (3)	Purging (not destruction) (1)	Purging (not destruction) (1)	Purging (not destruction) (1)	Contact DS

(1) Except for elements that cannot be purged but only destroyed (ROM) and replaced.

(2) Problems inhibiting the complete Clearing or Purging of media

(3) Clearing if decided by the system owner

(4) If Purging not possible, destroy with necessary protection in the meantime see section 7.4

(5) Purging (not destruction) if decided by the system owner

(6) No sanitising action before Disposal but destroy only if decided by the system owner

9.4. Table 2 — Sanitisation methods for media (not paper)

	CLEAR	PURGE	DESTROY
Magnetic tapes (reel and cassette format magnetic tapes)	Degaussing (note 0) Alternative: Overwriting random, unclassified data over existing data (note 2)	Degaussing (tape coercivity lower than degausser) (note 1)	Incineration to white ash (note 12), or Disintegrate in high security disintegrator
Magnetic disks (e.g., Hard drives, Sealed Disk Drives, ZIP disks)	Overwriting with an approved product or tool (notes 3 and 4)	Degaussing (disk coercivity lower than degausser one) (see notes 1, 5 & 8) Firmware secure erase (for supported drives only, see note 9) Overwriting with Blancco (notes 6, 10 & 11)	Incineration to white ash (note 12), or Disintegrate in high security disintegrator
Floppy disks, magnetic cards	Overwriting with an approved product or tool (notes 3 and 4)	Degaussing (disk coercitivity lower than degausser one) (note 1) (note 5) Firmware secure erase (for supported drives only, see note 9)	Incineration to white ash (note 12), or Shred
Optical disk CD, DVD	See destruction	See destruction	Use an optical disk grinder, or Incineration to white ash (note 12), or Use optical device shredder or disintegrator to reduce into particles (nominal edge of 5mm and surface 25 mm^2)
Volatile solid state storage devices: e.g. DRAM, SRAM, Volatile FGPA	Remove the power (causes instantaneous sanitization) Overwriting with a known unclassified pattern	Same as clear	Disintegrate, smelt or incinerate (note 12)
Non-Volatile solid state storage devices: EPROM and UVEPROM	Perform ultra-violet erase (see manufacturer's recommendation) but increase the time requirement by a factor of three, then overwrite with a known unclassified pattern	Same as Clear	Disintegrate, smelt or incinerate (note 12)
Non-Volatile solid state storage devices: PROM and ROM	See destruction	See destruction	Smelt, or disintegrate
Smart cards	See destruction	See destruction	Disintegrate, incinerate (note 12) or shred with strip shredder (maximum width 2 millimetres, inserted diagonally at a 45 degree angle), or Cut with scissors at a 45 degree angle diagonally (note 7)
Flash memory e.g. USB keys	Overwriting with a known unclassified pattern (at least one pass)	Overwriting with a known unclassified pattern (at least three passes)	Disintegrate, smelt or incinerate (note 12)

See referred notes on next page.

9.4.1. Notes on "Table 2 — Sanitisation methods for media"

Note 0: any degausser type I (350 Oersted) or type II (700 Oersted) may be used.

Note 1: media coercivity given by manufacturer (should be labelled on the device); the manufacturer indications must be followed.

Note 2: at least one-pass overwriting with unclassified pattern or random data.

Note 3: three passes for 'LIMITED HIGH': first all 0's, then all 1's and finally random unclassified data in last round.

Note 4: single pass overwriting of random data for "LIMITED BASIC".

Note 5: if the degaussing method damages disks (hard disks), the media must be destroyed after verification of purging; magnetic media products that have pre recorded magnetic servo pattern must not be degaussed unless the media has to be destroyed; in fact degaussing would erase the factory written servo signals and leave the media unusable.

Note 6: overwriting must be followed by verification, randomly re-reading the overwritten information (see section 7.9).

Note 7: must make sure that the magnetic strip, bar code, micro chip are destroyed and written information made unreadable.

Note 8: strength of degausser in Gauss to be from 2 to 3 times coercivity of the media in Oersted; a choice of a degausser that achieves 90 dB and more than 5000 Gauss gives assurance.

Note 9: valid alternative to degaussing if it is supported by the device.

Note 10: for "CONFIDENTIEL UE" and "SECRET UE": seven passes with unclassified data and use random data in last round.

Note 11: three passes for "LIMITED HIGH" and "RESTREINT UE" - first all 0's, then all 1's and finally random unclassified data.

Note 12: incineration using licensed incinerator.

9.5. Table 3 — Secure disposal of paper documents

PUBLIC	No requirement
LIMITED BASIC	Recommended to be shredded with straight cut shredder 4mm The shredded document may be disposed of in normal office waste bin/bags
LIMITED HIGH	To be shredded with shredder DIN 32757 Level 3: straight cut 1.9 or cross cut 4 x 80 mm - max surface 320 mm² The shredded document may be disposed of in normal office waste bin/bags
RESTREINT UE	To be shredded with shredder DIN 32757 Level 4: straight cut 1.9 or cross cut 2 x 15 mm - max surface 30 mm² The shredded document may be disposed of in normal office waste bin/bags
CONFIDENTIEL EU	To be shredded with shredder DIN 32757 Level 5: straight cut 1.9 or cross cut 0,8 x 13 mm - max surface 10 mm² The shredded document may never be disposed of in normal office waste bin/bags This shredding must be done in the secure zone before leaving this zone for destruction (burning)
SECRET EU	To be shredded with shredder DIN 32757 Level 5: straight cut 1.9 or cross cut 0,8 x 13 mm - max surface 10 mm² The shredded document may never be disposed of in normal office waste bin/bags This shredding must be done in the secure zone before leaving this zone for destruction (burning)
TRES SECRET UE / EU TOP SECRET	Contact DS - DS will decide on the best method on a case by case basis.

10. ROLES AND RESPONSIBILITIES

System Owner: accountable for the security of their information systems, including the storage media during their whole lifecycle, i.e. classification level of their media, compliance with the sanitisation requirements of this standard, and any contractual agreements with the sanitisation company.

LISO and/or LSO and/or RCO: responsible for preparing for secure disposal or sanitisation and any possible secure storage of media waiting to be sanitised.

Security Directorate: provide instructions on all special cases upon DG's request.

11. REFERENCES

Commission Decision C(2006) 3602 of 16/8/2006

Implementing rules for Commission Decision C(2006) 3602 of 16.8.2006.

International standard ISO/IEC 27001 – Second edition 2005-06-15

International standard ISO/IEC 17799 – Second edition 2005-06-15

Security Notice 01: The use and application of security designators and markings (See Security Directorate website)

Security Notice 02 CREATION, HANDLING AND STORAGE OF RESTREINT UE INFORMATION (Revision 07, 3/12/2009)

Security Notice 04 CREATION, HANDLING AND STORAGE OF CONFIDENTIEL UE INFORMATION (Revision 01, 9/3/2005)

Security Notice 4A CREATION, HANDLING AND STORAGE OF SECRET UE INFORMATION (Revision 01, 9/3/2005)

Commission Decision of 24 November 2001 (2001/844/EC, ECSC, Euratom)

Commission Decision of 3 February 2005 amending Decision 2001/844/EC, ECSC, Euratom.