EBA DC 197

1 September 2017

Decision of the Executive Director on the EBA Information Classification Policy

The Executive Director

HAVING REGARD to Regulation (EC) No. 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority)[1], (hereinafter referred to as "the EBA" or "the Authority"), and in particular Articles 70, 71 and 72 thereto,

HAVING REGARD to the Decision EBA/DC/138 of 29 October 2015 adopting the Commission's Information Security Policy;

HAVING REGARD to the Regulation (EU) 2015/496 amending Regulation (EEC, Euratom) No 354/83 as regards the deposit of historical archives of the institutions at the European University Institute;[2]

Whereas:

1. The EBA has responsibility for protecting the confidentiality of its information, and for ensuring that staff and stakeholders are made aware of their obligations in this regard;

2. It is important to define and implement a classification scheme for information held by the EBA, including measures for storing and transmitting this information.

After consulting the EBA Staff Committee,

HAS DECIDED AS FOLLOWS:

Article 1

[1] 1 OJ L 331/12, 15.12.2010, p. 12
[2] OJ L 79, 25.3.2015, p. 1–5.

The document entitled "EBA Information Classification Policy" annexed to this Decision is hereby adopted.

Article 2

This Decision shall enter into force on the day following its adoption.

Adam Farkas
Executive Director

Done in London, 1 September 2017

Annex I

EBA Information Classification Policy

Contents

Table of Contents

Introduction 4

1. Scope 5

2. Definitions 5

3. Responsibilities 5

(i) Information Security Officer (ISO) 5

(ii) Local Security Officer (LSO) and the Local Informatics Security Officer (LISO) 5

(iii) The Information Technology (IT) Unit 5

(iv) EBA Staff and non-staff individuals participating in the EBA's work 6

4. Classifying information 6

5. Classifications 6

(i) EU classified information (EUCI) 6

(ii) EBA classified information (EBACI) 7

EBACI classification levels: 8

a) PUBLIC 8

b) EBA Regular Use 8

c) EBA Restricted Use 8

d) EBA Confidential Use 8

6. Electronic transmission/distribution of EBACI 9

6. Additional Markings 10

(i) Annex 1 – Additional Markings - Labels 11

(ii) Annex 2 – EU Unclassified Information and EBA Classified Information 13

(iii) Annex 3 – EU and EBA Classified Information - Levels 14

(iv) Annex 4 – EU and EBA Classified Information - Description 15

(v) Annex 5 – How to share and protect EBACI 16

Introduction

It is necessary to define a classification scheme for information handled at the EBA that is not EU Classified Information[3] but is confidential.

This document outlines the EBA policy on classifying information and covers the different categories by which information can be classified.

Where confidentiality is concerned, care and experience are needed in the selection of information and material to be protected and the assessment of the degree of protection it requires.In order to ensure the smooth flow of information, steps must be taken to avoid both over-classification and under-classification.

By adhering to this policy, the EBA will reduce the risk of a security and confidentiality breach, fraud or information theft; increase staff's awareness of protecting sensitive information; help demonstrate compliance with data protection requirements; and create a culture of staff responsibility in relation to handling and care of personal and EBA's activities-related information.

The security classification system is the instrument for giving effect to these principles.

The provisions in this policy are aligned with:

- Regulation (EU) No 1093/2010 establishing the European Banking Authority (EBA founding regulation), specifically Article 70 – Obligation of professional secrecy, Articles 71 – Data protection, and Article 72 – Access to documents, which require the EBA to apply:
    - Regulation (EC) No 45/2001 on the protection of personal data; and
    - Regulation (EC) No 1049/2001 regarding public access to documents;
- EBA/DC/138 of 29 October 2015 adopting the Commission's Information Security Policy;
- Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information; and
- Regulation (EU) 2015/496 amending Regulation (EEC, Euratom) No 354/83 as regards the deposit of historical archives of the institutions at the European University Institute.

[3] The definition of EU Classified information is provided in Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53–88).

1. Scope

This policy covers all documents as defined in the EBA Document Management Policy[4], whether in paper and/or electronic format. This policy applies to:

- Everyone working at the EBA, irrespective of their administrative position or status, i.e. temporary agents, contract agents, seconded national experts, on-site consultants, temporary workers (interim staff) and trainees; and
- Everyone participating in the EBA's work, as specified in the Decision of the European Banking Authority EBA BS 2017 184 adopting Rules of Procedure on Professional Secrecy for Non-Staff, and repealing the Decision of the Management Board of 12 January 2011 on Professional Secrecy (EBA DC 004).

2. Definitions

The applicable definitions are those contained in the EBA Document Management Policy.

3. Responsibilities

(i) Information Security Officer (ISO)

The **ISO** is responsible for developing a comprehensive information security framework, including developing policies and procedures and delivering training on information security.

(ii) Local Security Officer (LSO) and the Local Informatics Security Officer (LISO)

The **LSO** and **LISO** have an advisory and monitoring role in supporting staff to comply with the requirements of the policy. The LSO is responsible for ensuring that there are adequate means of protection for paper-based classified documents and the LISO is responsible for ensuring that safeguards for the protection of electronic information are in place.

(iii) The Information Technology (IT) Unit

[4] For a definition of 'document', see the EBA Document Management policy

The IT Unit supports the implementation of security requirements for EBA Classified Information, by identifying suitable IT solutions and providing users with the technical means to ensure security of electronic information.

(iv) EBA Staff and non-staff individuals participating in the EBA's work

It is the responsibility of **all staff members** and of **all non-staff individuals participating in the EBA's work** to comply with the EBA Information Classification policy, to adhere to the obligation of integrity and discretion, including protecting information in their custody from unauthorised access and improper use.

4. Classifying information

Everyone working at the EBA and/or participating in the EBA's work, as defined in 1. Scope, must classify information they have authored, using information classification levels set out in this policy.

Where documents are grouped, the classification level to be applied to the whole must be as high as the highest classification of its parts. A group of documents (a file) may however be given a higher classification than its constituent documents.

Classifications must be assigned only when necessary and for as long as necessary. The classification must be clearly indicated and must be maintained only as long as the information requires protection.

5. Classifications

(i) EU classified information (EUCI)

EUCI is information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States. Commission Decision (EU, Euratom) 2015/444[5] lays down the basic principles and minimum standards of security for protecting EUCI and the EBA complies with it when handling EUCI.

EUCI is classified into four levels which are (from highest to lowest): EU TOP SECRET, EU SECRET, EU CONFIDENTIAL and EU RESTRICTED.

[5] Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53)

The EBA expects to handle EUCI very rarely, and then only EUCI classified as EU RESTRICTED (i.e. at the lowest level). See Annex 3 for a description of what constitutes EU RESTRICTED information. If the need to handle other EUCI classifications arises, this policy will be reviewed and updated.
EUCI must be clearly marked with its classification level. When the EBA receives EUCI, it is responsible for protecting it, and it must keep its original security classification.
The security measures for protecting EUCI throughout its life-cycle must be commensurate in particular with its security classification, the form and the volume of the information or material, the location and construction of facilities housing EUCI and the locally assessed threat of malicious and/or criminal activities, including espionage, sabotage and terrorism.
Staff who handle EUCI must familiarise themselves with the requirements of Commission Decision (EU, Euratom) 2015/444.

EUCI will not be stored in the EBA's Document Management System.

(ii) EBA classified information (EBACI)

EBACI is information or material designated by an EBA security classification. The unauthorised disclosure of EBACI may cause varying degrees of prejudice to the EBA, the EU, one or more of its member states or other parties.

EBACI corresponds to the LIMITED and PUBLIC levels of EU unclassified information described in the EBA Decision EBA/DC/138 of 29 October 2015, adopting Commission Decision C(2006) 3602 on the security of information. For an explanation of different levels of EU unclassified information and their relationship to EBACI, see Annex 2.

EBACI classification levels:

a) PUBLIC

PUBLIC EBACI is information meant for public distribution, for example documents published on the EBA external website. The disclosure of this information would not damage the interests of the EBA, the European Union, Member States or other parties.

Staff must seek approval from their hierarchy prior to making EBA documents public.

b) EBA Regular Use

Unauthorised disclosure of information classified as EBA Regular Use would not be prejudicial to the EBA. Typically, EBA Regular Use documents are internal, non-sensitive documents. EBA Regular Use information is available to all EBA staff and to third parties that have a legitimate 'need-to-know', including standing committees, sub-groups, and task forces.

Any documents that are not specifically classified are considered to be EBA Regular Use.

Annex 5 details requirements for storage, distribution and disposal of EBA Regular Use information.

c) EBA Restricted Use

Unauthorised disclosure of EBA Restricted Use documents would be prejudicial to the the EBA, the EU, one or more of the Member States or other parties, but not to an extent serious enough to merit classification as EBA Confidential Use.

All staff members may classify data as EBA Restricted Use, as appropriate. Annex 4 provides further advice on potential consequences of disclosing EBA Restricted Use information.

Annex 5 details requirements for storage, distribution and disposal of EBA Restricted Use information.

d) EBA Confidential Use

Unauthorised disclosure of EBA Confidential Use documents would be significantly prejudicial to the EBA, the European Union, one or more of its member states or other parties, but not to an extent serious enough to merit classification as EUCI.

All staff members may classify data as EBA Confidential Use as appropriate. Annex 4 provides further advice on potential consequences of disclosing EBA Confidential Use information.

Annex 5 details requirements for storage, distribution and disposal of EBA Confidential Use information.

6. Electronic transmission/distribution of EBACI

EBA Restricted Use and EBA Confidential Use information belongs to one of these categories:

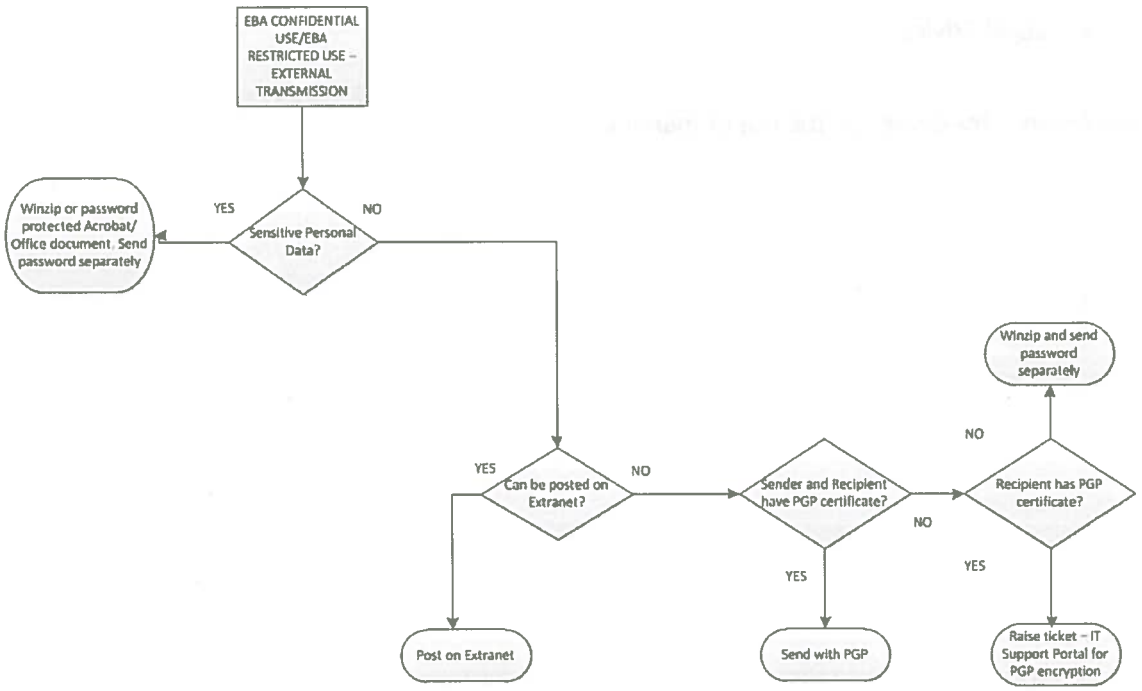
Market sensitive information: Includes information concerning institutions, e.g. related to stress tests, impact assessment, Basel related policy papers with QIS data/ study's with sensitive information.

Sensitive personal data: Includes Staff matters sent to external lawyers, or recruitment assessments to other ESAs when participating on their recruitment panels, or replying to complaints from Union citizens.

Legal advice/legal matters, which are classified as EBA Restricted Use or EBA Confidential Use may contain either personal data or market sensitive information.

Any information classified as EBA Restricted Use or EBA Confidential Use, if transmitted to external recipients, must be protected. If posted on the EBA extranet, EBA Restricted Use or EBA Confidential Use does not need to be encrypted or password protected. Competent authorities have access to the EBA Extranet on the understanding that the information contained in the system should be treated on a professional secrecy basis and must not be made public. However, documents classified as EBA Restricted Use or EBA Confidential Use must be encrypted or password-protected if sent via email, with few exceptions (see Annex 5).

Figure 1



6. Additional Markings

EBACI documents must be clearly marked with their classification level. They may also contain **additional markings** to provide instructions on the handling of a document. A marking is not the same as an information classification level, and may not be used in place of one.
More than one marking may be used. Markings may be applied to EBA Regular Use, EBA Restricted Use and EBA Confidential Use documents, but not to PUBLIC documents.

When used, markings should be applied to the first page of the document and may be applied to subsequent pages. If a document is being sent by internal mail then the marking should also be added to the outside of an envelope to avoid it being opened in error (unless otherwise indicated in the handling instructions).

The following markings may be used:

- [Team] use
- Personal Data
- Staff Matter
- Highly Market Sensitive
- Medical Secret
- Legal Advice

See Annex 1 for details on the use of markings.

(i) Annex 1 – Additional Markings - Labels

Marking	Distribution and Handling instructions	Who can apply the marking	Examples
[Team] use	Only for use within internal teams or committees (e.g. unit, department, team, project team, EBA management, crisis management group) • Distribution on need to know basis to a named group. Further distribution only with agreement of EBA staff document owner • Not for publication All recipients should be aware of the strict application of the 'need to know'	All staff	Documents for internal crisis management group Resolution plans Stress test results analysis (pre-publication)
Personal Data	Must be applied to documents containing personal data that shall only be communicated on a need to know basis pursuant to data protection legislation and that do not fall under the scope of another approved marking. Should be used for any document containing personal data not covered by another marking Must also be marked 'EBA Confidential Use' or 'EBA Restricted Use'	All staff	Lists of contact details of members of EBA groups Fire Warden PEEPS lists HR documents containing staff information (not covered by another marking such as 'Medical secret')
Staff matter	To be used only for documents related to staff matters and managed by HR staff and management concerned, and to be opened by the addressee(s). The provisions of data protection legislation regarding the confidentiality of such information must be respected Must also be marked EBA Confidential Use or EBA Restricted Use, as appropriate	HR and management	Documents relating to a staff complaint, an administrative inquiry, or proposals for internal staff transfers

Marking	Distribution and Handling instructions	Who can apply the marking	Examples
Highly market sensitive	Marking to be applied on documents which contain information which is **highly** market sensitive information or concerns adverse developments which may **seriously** jeopardise orderly functioning/integrity of financial markets or financial system • Marking may only be initiated on instruction at the level of Head of Department or above • Where e-mail is used to transmit related information covered by the obligation of professional secrecy, this must be encrypted • Distribution only on a strict need to know basis – the originator should be consulted before transmission of the document outside the original list of recipients.	All staff	Draft stress test data/analysis Resolution plans
Medical secret	For documents covered by medical confidentiality rules Must also be marked EBA Confidential Use The provisions of Regulation (EC) 45/2001 apply	HR, EBA Medical Service	
Legal advice	Legal advice given by the Legal Unit to be considered as advice for the addressee(s) to treat the document as a document which should be known or kept by the addressee(s). • EBA document protected pursuant to Article 4 of Regulation (EC) No 1049/2001 on access to documents • Not for publication Circulation outside EBA staff should be discussed and agreed with the Legal Unit	Legal Unit	

(ii) Annex 2 – EU Unclassified Information and EBA Classified Information

EU unclassified information and EBA Classified information is categorised as LIMITED and PUBLIC, has three characteristics: confidentiality, integrity and availability.

- Confidentiality refers to the level of access to information based on the 'need-to-know' principle.
- Integrity refers to the resulting harm ensuing from potential for loss, alteration or corruption of information.
- Availability refers to the maximum total harm ensuing from loss of information.

LIMITED information can be further split into HIGH and BASIC levels, and there are three levels each for Integrity and Availability: MODERATE, CRITICAL and STRATEGIC.

- MODERATE: shall apply to information and related assets the loss of integrity or availability of which might threaten the internal working of the EBA.
- CRITICAL: shall apply to information and related assets the loss of integrity or availability of which might threaten the position of the EBA with regard to other Institutions, Member States or other parties.
- STRATEGIC: shall apply to information and related assets the loss of integrity or availability of which would be unacceptable to the EBA, other Institutions, Member States or other parties.

EBACI can be classified into four levels: EBA CONFIDENTIAL, EBA RESTRICTED, UNRESTRICTED or PUBLIC. These four levels will comprise the characteristics described for confidentiality (LIMITED, PUBLIC) and integrity or availability (MODERATE, CRITICAL, STRATEGIC) in key combinations:

EBACI level	Confidentiality	Integrity or Availability
EBA Confidential Use	Limited High	Strategic
EBA Restricted Use	Limited High	Critical
EBA Regular Use	Limited Basic	Moderate
PUBLIC	Public	Moderate

(iii) Annex 3 – EU and EBA Classified Information - Levels

EU Classification levels [6]		EBA Classification levels	
EU Top Secret/ EU Secret/ EU Confidential	Information and material the unauthorised disclosure of which could cause exceptionally grave prejudice/seriously harm/harm the essential interests of the European Union or of one or more of the Member States.	**Not applicable**	
EU Restricted	Information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.	**EU Restricted**	Information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.
Commission Decision C (2006) 3602 [7]			
CONFIDENTIALITY: Limited High	'LIMITED': information system or information reserved for a limited number of persons on a need to know basis and whose disclosure to unauthorised persons would be prejudicial to the Commission, other Institutions, Member States or other parties, but not to an extent serious enough to merit Classification.	**EBA Confidential Use**	Information the unauthorised disclosure of which would be significantly prejudicial to the EBA, the EU, or one or more of its member states or other parties, but not to an extent to merit EU classification;
		EBA Restricted Use	Information the unauthorised disclosure of which would be prejudicial to the EBA, the EU, or one or more of its member states or other parties, but not to an extent to merit EU classification;
CONFIDENTIALITY: Limited Basic		**EBA Regular Use**	Information that is not intended for public disclosure, but the unauthorised disclosure of which would not be prejudicial to the EBA, the EU, one or more of its member states or other parties;
CONFIDENTIALITY: Public	'PUBLIC': information system or information whose public disclosure would not damage the interests of the Commission, the other Institutions, the Member States or other parties.	**PUBLIC**	Information whose public disclosure would not damage the interests of the EBA, the EU, one or more of its member states or other parties.

[6] Commission Decision (EU, Euratom) 2015/444
[7] Commission Decision C (2006) 3602

(iv) Annex 4 – EU and EBA Classified Information - Description

EU classification	*Short description*		*Example*
EU RESTRICTED	This classification shall be applied to information and material the unauthorised disclosure of which could be disadvantageous to the interests of the EU or of one or more of its Member States		Information disclosure of which is likely to have a ***material*** financial stability impact for the EU or a Member State
EBA classification	***Short description***	***Summary***	***Example***
EBA Confidential Use	Unauthorised disclosure would be significantly prejudicial to the EBA, the EU, or one or more of its Member States or other parties, but not to an extent to merit EU classification as EU Classified Information (as laid down in paragraph 3.1 of see Commission Decision (EU, Euratom) 2015/444)	Information whose unauthorised disclosure would cause harm to various interested parties because it contains confidential business/ commercial information, intellectual property or personal information.	Likely to have a **HIGH** negative impact on the EBA and would be likely to have one or more of the following consequences: • Partial failure to deliver on statutory tasks or failure to deliver on advisory functions or complete failure to achieve strategic objective • Unwanted adverse market reactions and significant market movements between one day and one week • Financial loss above €1.000.000 up to €10.000.000 • Facilitate improper gain or advantage for individuals or companies • Impede criminal investigation, or facilitate crime Examples: • Resolution plans for significant institutions and information which does not directly identify individual financial institutions but disclosure may affect orderly functioning/integrity of financial markets or financial system, e.g. Crisis Management Team discussions, or non-public bank stress test analysis.
EBA Restricted Use	Unauthorised disclosure would be prejudicial to EBA, the EU, or one or more of its member states or other parties, but not to an extent to merit EU classification.		Likely to have a **MEDIUM** negative impact on the EBA and/or would be likely to have one or more of the following consequences: • Unsatisfactory quality or significant delays in delivery on statutory tasks or partial failure to meet strategic objectives • Temporary market irritation and unwanted significant market movements during one day • Financial loss above €100.000 to €1.000.000 • Cause distress to individuals • Breach statutory/regulatory restrictions on the disclosure of information Examples: Non-public data held on individual financial institutions/groups, e.g. COREP, FINREP data, college documents such as risk assessments. Confidential responses to Consultation Papers (CPs), Confidential requests for Breach of Union Law (BUL) investigations. Procurement tender proposals , Sensitive personal data – e.g. personnel/recruitment files, medical documents, personal dealing notifications, remuneration data of individuals **Note:** In each case, there needs to be an impact assessment, if information is inadvertently made public. If necessary, upgrade or downgrade classification.
EBA Regular Use	Not meant for the public, but its unauthorised disclosure would not be prejudicial to the EBA.	Information that is currently internal (may become public at later date)	Documents intended to become public and drafts of which would not disrupt financial markets or prejudice individual institutions: • EBA work programme; most Consultation Papers, Guidelines, Technical Standards, Press Releases • Agendas and Minutes of BoS, MB and Working Group meetings, including their drafts under development (unless content is sensitive, then classify as Restricted Use/Confidential Use) • Internal policies
PUBLIC	Public disclosure would not damage interests of the EBA, the EU, Member States/ other parties.	Information on the EBA website.	• Documents distributed through the external EBA website or as hard copy publications (e.g. Annual Report) • Public registers

(v) Annex 5 – How to share and protect EBACI

	Distribution					Storage and Disposal			
	Internal		External						
Classification	Email	Post	Fax	Email	Post	Devices	Electronic Storage	Physical Storage	Paper Disposal
EU classification									
EU RESTRICTED	Must be distributed only to staff/role that can access the information/document with indication " EU RESTRICTED " in the title and with a read receipt and delivery receipt, which is verified by the sender	Must be distributed personally, indicated on the outside " EU RESTRICTED ".	Not allowed unless recipient fax number is confirmed	Not allowed unless the email is approved by manager and documented or cryptography and control recommendations are implemented	Courier in double envelopes;	Not allowed	In official EBA applications.	Locked safe	Dispose through a shredder
EBA classification									
EBA Confidential Use	Send eDEN links or links to shared drive folders (on Unit drives or Project drives) via email. In situations of extreme urgency, when sender or recipient doesn't have access to eDEN or shared drives, and it's not feasible to encrypt, attachments and unencrypted messages may be sent.	Sealed envelope inside another envelope and hand-delivered, indication on the outside "EBA Confidential Use "	Not allowed unless recipient fax number is confirmed	Links to the extranet. If it isn't possible to send extranet links, encrypt using PGP, Winzip, or send as password-protected Acrobat/Office file. See decision tree page 8, Figure 1.	Courier in double envelopes	Office PCs or EBA-issued laptops, tablets and phones	eDEN or folder(s) with restricted permissions on shared drive or EBA applications	Locked cupboard	Dispose by secure means provided by the EBA
EBA Restricted Use	Send eDEN links or links to shared drive folders (on Unit drives or Project drives) via email. Attachments and unencrypted messages may exceptionally be sent if sender or recipient doesn't have access to eDEN or shared drives, and it's not feasible to encrypt.	Internal post or hand-delivered Indication on the outside "EBA Restricted Use"	Not allowed unless recipient fax number is confirmed	Links to the extranet. If it isn't possible to send extranet links, encrypt using PGP, Winzip, or send as password-protected Acrobat/Office file. See decision tree page 8, Figure 1.	Registered mail or courier in double envelopes	Office PCs or EBA-issued laptops, tablets and phones	eDEN or folder(s) with restricted permissions on shared drive or EBA applications	Locked cupboard	Dispose by secure means provided by the EBA
EBA Regular Use	For internal circulation within the EBA, ESFS and other contributors to EBA work. Must be stored on EBA infrastructure, may be distributed by email without encryption, but requires manager's approval for external distribution.								
PUBLIC	In the public domain, therefore no special rules on distribution, storage, or disposal.								