Working Instructions

Rules on Handling EIOPA Information and Documents

Document History

Status	Date	Update
Original	09/03/2015	Initial version

Document Sign-Off[1]

Initiation	Quality Check	Endorsement
Initiator	**Governance & Organization Coordinator**	**Executive Director**
Date	Date	Date

[1] *Delegations may apply*

Table of Contents

Working Instructions **1**

Rules on Handling EIOPA Information and Documents **1**

Document History 1

Document Sign-Off 1

1. Purpose and Scope 3
2. Definitions 3
3. Description 5

Creation and receipt of information and documents and assigning the confidentiality levels 6

Markings 7

Downgrading and declassification 9

Distribution and transmission of information and documents 10

Handling and storage requirements 12

Printouts, copies and other usage considerations 14

Destruction and disposal 15

4. Roles and Responsibilities 15

Annex 1 - List of the approved confidentiality levels, markings and their significance

Annex 2 - Example of assigning confidentiality levels, markings and handling instructions on documents

Annex 3 – Sample Business Impact Assessment Questionnaire

1. Purpose and Scope

1.1 This document sets up the basic administrative measures for controlling EIOPA's information and documents throughout their life-cycle in order to help prevent or minimise the risks and the consequences of unauthorised access or disclosure, deliberate or accidental misuse, loss or compromise of such information.

1.2 The Rules on Handling EIOPA Information and Documents sets up provisions for implementing the Chapter *Information and Documents*, paragraphs 3.4 to 3.9, of the EIOPA Security Policy.

1.3 This document sets up the minimum security requirements for handling EIOPA's sensitive and non-sensitive information and documents. It provides also practical advice and recommends increased security for cases where there are higher risks involved and where the security measures have to be strengthened.

1.4 The rules set up by this document are applicable to:

(a) all EIOPA statutory staff, hereafter referred to as "EIOPA Staff" or "EIOPA Staff member"[2] ; and

(b) contractors, subcontractors and their employees[3]; and

(c) all other persons, working with EIOPA Staff or receiving access to EIOPA information.

2. Definitions

For the purposes of the present Working Instructions, the following definitions apply:

Information	Data in a form that allows it to be communicated recorded or processed.
Sensitive Information	EIOPA Restricted Use and EIOPA Confidential Use Information, as the unauthorised disclosure of such information would be prejudicial to EIOPA, the EU or one or more of its Member States or other parties.

[2] *The "EIOPA Staff member" includes: individuals covered by the Staff Regulations and CEOS, as well as Seconded National Experts*
[3] *For the purpose of this document, interim employees and consultants*

Compromise of sensitive or classified information	Denotes a situation when, due to a breach of security or adverse activity, the sensitive or classified information has lost its confidentiality, integrity or availability.
Document	Any letter, note, minute, report, memorandum, signal/message, sketch, photograph, slide, film, map, chart, plan, notebook, stencil, carbon, typewriter or printer ribbon, tape, cassette, computer disk, CD-ROM, or other physical medium on which information has been recorded.
Sensitive Document	A document containing sensitive information.
Handling	All possible actions, to which information may be subject throughout its life-cycle. It comprises of its creation, processing, carriage, downgrading, declassification and destruction. In relation to Communication and Information Systems it also comprises of its collection, display, transmission and storage.
Originator[4]	The duly authorised author of information or document. Heads of departments and units, and the team coordinators may authorize their staff to originate EIOPA sensitive information.
Holder	A duly authorised person with an established need-to-know having the custody of a particular document or information and having the responsibility to protect it according to the approved security rules.
Third Parties	European Union Institutions, Bodies and Agencies, Member States, Third States, International Organisations or other entities.

[4] *According to the definition, the originator is the author of the document, but for continuance reasons the originator may be considered to be the originating service (a Department, Unit, Team, function or similar service). This is due to the fact the EIOPA Organigram is a living description, which might change.*

3. Description

3.1 EIOPA's information and documents must be assured protection throughout their lifecycle by a set of administrative measures in order to help deter, detect and recover from deliberate or accidental compromise or loss of such information.

3.2 The security classifications must be followed and applied in accordance with the Decision of the Management Board of EIOPA concerning the Protection of Information Systems and Information[5].

3.3 For all documents not defined as "EU classified information", the levels of confidentiality of information in EIOPA are as follows:

- "PUBLIC" shall apply to information the public disclosure of which would not be prejudicial to EIOPA. This includes information released by EIOPA for wide-spread public disclosure;

- "EIOPA REGULAR USE" shall apply to information that is not intended for public disclosure, but the unauthorised disclosure of which would not be prejudicial to EIOPA;

- "EIOPA RESTRICTED USE" shall apply to information the unauthorised disclosure of which would be prejudicial to EIOPA, the EU or one or more of its Member States or other parties, but not to an extent serious enough to merit EU classification as laid down in paragraph 16.1 of the provisions of Commission Decision 2001/844/EC, ECSC, Euratom;

- "EIOPA CONFIDENTIAL USE" shall apply to information the unauthorised disclosure of which would be significantly prejudicial to EIOPA, the EU or one or more of its Member States or other parties, but not to an extent serious enough to merit EU classification as laid down in paragraph 16.1 of the provisions of the provisions of Commission Decision 2001/844/EC, ECSC, Euratom.

3.4 It is the responsibility of the originator of the information to initially determine and, later on, review the confidentiality levels.

3.5 The holder of any item of information or document is responsible for protecting it, by preserving its confidentiality, integrity and availability,

[5] *EIOPA-MB-14/034, dated 10 June 2014*

in accordance with the provisions of the EIOPA Security Policy and of this document.

3.6 For creating, receiving, handling, processing, storing and transmitting sensitive information and documents, only EIOPA property or approved IT equipment, media, infrastructure and software must be used. Personal tools, equipment, non-work emails must not be used in relation with sensitive information.

Creation and receipt of information and documents and assigning the confidentiality[6] levels

3.7 The confidentiality levels indicate the degree of sensitivity of EIOPA information and are applied in order to alert recipients to the need to ensure protection in proportion to the degree of prejudice that would occur from unauthorised access or disclosure, or loss.

3.8 The main confidentiality levels of EIOPA originated information are:

- PUBLIC
- EIOPA Regular Use
- EIOPA Restricted Use
- EIOPA Confidential Use

3.9 Assigning a confidentiality level to information implies that it will be handled according to certain rules, which, on the one hand, confer a degree of protection on it but, on the other, imply a number of constraints. Care must be taken in order to avoid over-classification and under-classification[7].

3.10 The originator is responsible for deciding on the confidentiality level to be assigned to information or document before its creation, in consultation with the relevant Team Coordinators or the EIOPA Security Officer. Protection must be ensured also to draft versions, early versions, and data collections under development.

3.11 When assessing a particular piece of information, the main criteria to be used is the degree of prejudice that could be caused by affecting one or more of the attributes of confidentiality, integrity and availability.

---

[6] *In the case information does not merit EUCI classification*

[7] *The terms "over-classification" and, similarly, "under-classification" are used to illustrate the potential negative consequences of wrongly or carelessly assigning a lower or higher confidentiality level to information.*

3.12 For ensuring a consistent and objective classification process and for reducing the risks of over- and under-classification, the main methodologies to be used when deciding on the confidentiality level to be assigned to the EIOPA information are:

(a) The analogy with the classification already done (an information valuation has already been made for similar information used in a similar scope: similar stakeholders, similar boundaries etc.);

(b) Using the definitions of the confidentiality or EU classified information (EUCI) levels (identify the worst case impact potentially caused by all kinds of threats and vulnerabilities without taking into account any existing or potential security countermeasures); and

(c) Step by step Business Impact Assessment (see Annex 3 for an example of a BIA Questionnaire), consisting in determining the possible business impacts resulting from various incidents when affecting the confidentiality.

3.13 It is advisable to attribute different confidentiality levels to individual pages, paragraphs, sections, annexes, attachments, enclosures of a given document. The confidentiality level of the document as a whole will be at least that of its most highly sensitive component.

3.14 Information originated or received from third parties must be handled and protected based on the equivalence of the confidentiality levels, in line with the instructions received or in line with the existing security arrangements. In the case none of these exist, the information must be assessed and protected in the same manner as the EIOPA originated information.

Markings

3.15 EIOPA's sensitive documents[8] (i.e. documents containing EIOPA Restricted Use and EIOPA Confidential Use information) must be always marked at the time of the creation by the authorised person, by following the instructions received from the originator.

[8] *Including any output containing sensitive information from IT systems (such as printed reports, messages, presentations, screen display etc.)*

3.16 The confidentiality levels must be visibly affixed on the sensitive documents on the upper-right of the first page, by using Verdana, 12 or any other font indicated by the current corporate templates.

3.17 There is no specific marking requirement for EIOPA Regular Use and PUBLIC documents. However, those documents should be preferably marked according to the same rules applicable to sensitive documents.

3.18 All documents which have no marking are considered to be EIOPA Regular Use.

3.19 Additional markings to designate the field of activity to which it relates, identify the originator, limit distribution, restrict use or indicate releasability may be used on the first page. Additional text or footnotes may be used for setting up particular handling instructions. Only the approved confidentiality levels markings must be used. Annex 1 lists possible additional markings and their applicability. An example on the affixing the confidentiality levels and the usage of the markings is contained in Annex 2.

3.20 The originator of the document should be identified whenever it is possible on the first page of the sensitive documents.

3.21 The attachments, annexes, enclosures of a sensitive document must be listed in the main document, along with the confidentiality level. The main document will be assigned and marked with the highest confidentiality level of all the parts. However, the originator should specify the confidentiality level of the main document when detached from the annexes. For example: EIOPA Restricted Use – without attachments EIOPA Regular Use.

3.22 The filenames of the electronically created sensitive documents must indicate the documents confidentiality levels.

3.23 The emails containing sensitive information or sensitive attachments should be encrypted and marked according to the following rules:

(a) The subject line must contain the confidentiality level;

(b) Special care is needed as the subject line itself must not contain or disclose any sensitive information;

(c) The message body must be marked in the same way as the sensitive documents. The rules listed under paragraph 3.21 that are relevant to attachments must also be respected; and

(d) Each of the attachments must be clearly identified within the message body along with its confidentiality level.

3.24 As a general rule, no confidentiality marking will be affixed on the documents received from third parties that already carry a classification or confidentiality level.

3.25 All sensitive documents should contain a page number at the bottom of each page, along with the total number of pages of the document.

3.26 CDs, DVDs, USB sticks and other computer storage media must be labelled with the highest confidentiality level of the information contained. The labelling may be removed only when the media was properly destroyed or sanitised.

Downgrading and declassification

3.27 Downgrading means a reduction in the level of confidentiality (for example, from EIOPA Confidential Use to EIOPA Restricted Use).

3.28 Declassification means the removal of the previous confidentiality level and assigning it as PUBLIC (for example, from EIOPA Restricted Use to PUBLIC).

3.29 As a principle, the downgrading and declassification of EIOPA information is subject to the prior consent of the originator (originating service). The originator may indicate a specific event or a given date when a document can be automatically downgraded or declassified, by using a specific marking or by adding a footnote with specific instructions.

3.30 Downgrading and declassification may be decided on an ad hoc basis, for example following a request for access to public information, governed by Regulation (EC) No 1049/2001 on public access to documents and EIOPA implementing rules (EIOPA-MB-11/051).

3.31 It is strongly advised that the information and documents are periodically reviewed by the originator (originating service), at least every five years, in order to decide whether the information requires the same level of protection.

3.32 When a document no longer needs protection, the markings and the handling instructions must be removed from the document.

Distribution and transmission of information and documents

3.33 Initial distribution of sensitive information and documents may be carried out by the originator following the need-to-know principle and optimally by setting up a distribution list (for example, a list of staff, roles, teams, units etc. requiring access to the information or document).

3.34 Further distribution may be carried out by the holder following the need-to-know principle, provided that the originator has not imposed restrictions on such further distribution. In certain circumstances established by the originator, written approval might be required.

3.35 When distributing or transmitting sensitive information and documents to internal recipients or to third parties, adequate steps must be taken in order to ensure that information cannot fall into any unauthorised person's hands.

3.36 EIOPA Regular Use information may be distributed or transmitted to third parties on a need-to-know basis.

Distribution and Transmission within EIOPA premises

3.37 The distribution of sensitive information within EIOPA premises must be carried out preferably electronically, by approved IT means (such as document management systems, folders with limited access based on the need-to-know principle etc.), as the number of copies or printed materials must be kept to a minimum.

3.38 The sensitive information and documents must not be sent by email unless encrypted. In the case the encryption tools are not available, the hyperlink of the document (for example, hyperlink to a sensitive document stored with limited access rights on the I: drive) may be used instead.

3.39 Printed versions or copies of sensitive documents may be transmitted within EIOPA premises to the intended recipients or their team/unit assistants. Documents must be covered in order to prevent observation of the content (suggested, in a sealed opaque envelope and bearing the name of the addressee). Envelopes with the marking 'Personal' must be opened only by the intended recipient.

3.40 Non-encrypted USB sticks and other computer storage media (such as CD-ROMs, DVDs) may also be used for the in-house transmission of sensitive information, by following the rules set under paragraph 3.26.

3.41 If considered necessary, it is possible to increase the security of information by using encrypted computer storage media, especially for large quantities of sensitive information and documents.

Transmission outside EIOPA premises[9]

3.42 The originator and the holder of the sensitive information must assess the risks related to sharing information with the third parties. EIOPA management consent is required for transmitting or exchanging sensitive information.

3.43 The external recipients must be instructed to ensure the protection of EIOPA's sensitive information and documents. Preferably, similar security rules for protecting information must be in place. The principle applicable is the mutual trust, which can be reinforced by security arrangements on the mutual protection of the exchanged sensitive or classified information.

3.44 As a general rule, EIOPA's sensitive information and documents must be exchanged or transmitted outside EIOPA premises by electronic means protected by approved cryptographic products. Files may also be uploaded and shared on a need-to-know basis on a collaboration platform with strong authentication and encryption (for example, Extranet).

3.45 When electronic transmission is not possible, postal services may be used instead. When sending printed documents or computer storage media containing sensitive information to external parties, courier services ensuring hand delivery against signature must be used. Encrypted computer storage media should be the preferred choice.

3.46 Hand carriage of sensitive documents may be used. The package must prevent the unauthorised access to information. Sensitive documents must not be opened en route or read in public places. Documents must not be left unattended unless properly stored. The rules set out under paragraph 3.58 are also applicable.

3.47 As sensitive information and documents are distributed based on the need-to-know principle only to selected recipients, fax transmission is not advisable, unless there is a clear guarantee that documents will reach only the intended recipient.

---

[9] *A record of the transmissions of the EIOPA Confidential Use documents sent to external recipients should be maintained, as soon as the technical means will become available.*

Handling and storage requirements

3.48 The sensitive information and documents must be generally handled and stored by the EIOPA staff and other authorised users within EIOPA premises, in administrative[10] or secure[11] areas, in such a way to prevent unauthorised disclosure, alteration, removal or deletion.

3.49 Only in the interest of service, sensitive information and documents may be also temporarily handled or stored outside EIOPA premises, provided that the holder complies with the security requirements particular to those circumstances.

3.50 The holder has the responsibility of protecting the entrusted sensitive information, by preserving its confidentiality, integrity and availability. The holder may modify or alter the content of a document only after originator's written consent.

3.51 Sensitive information should be preferably handled and stored in electronic format:

(a) By using the dedicated EIOPA IT Systems[12] (document management platforms, repositories, network storage folders etc.) with access control restrictions, based on the need-to-know principle or other approved technical solutions communicated by the IT & Corporate Support Unit;

(b) By using encryption solutions for sensitive information at rest, which is not stored on EIOPA IT Systems[13] (on mobile devices, USB sticks, computer portable media, local drive etc.);

(c) In exceptional circumstances, only when encryption is not available, by using approved non-encrypted USB sticks and computer portable media. However, the media shall be visibly marked with the highest overall confidentiality level and stored in the same manner as the paper documents (i.e. when not used, stored in locked cabinets or locked offices).

---

[10] *A physical area where officials and other staff regularly work.*

[11] *A physical area where servers and other technical equipment are located. Secure zones are subject to higher levels of physical protection than Administrative zones.*

[12] *The security requirements of the EIOPA IT Systems and specifications on how the information is protected within the systems (for preserving the confidentiality, integrity and availability of information) are defined in the System Security Plans. See also paragraph 3.17 of the EIOPA Security Policy.*

[13] *Due care should be applied that the key or password used for the encryption is kept separately from the media.*

3.52 For avoiding the accidental or deliberate modification, alteration or deletion of information and documents, supplementary action may be taken, such as password protecting the documents, exporting as non-editable PDF, limited and/or read-only access to files and folders.

3.53 The mobile devices with no operational encryption services must not be used for storing sensitive information (for example, sensitive documents must not be saved on non-encrypted local drives of laptops).

3.54 When not in use and especially after working hours, all printed versions of sensitive documents and computer storage media containing sensitive information (especially those unencrypted or not sanitised) must be stored securely in locked cabinets or locked offices[14]. Metallic cupboards would represent a preferable and more secure solution especially for the regular basis storage of large quantities of EIOPA Confidential Use documents.

3.55 Printed documents, copies, draft versions containing sensitive information:

(a) must not be left unattended in the office, unless properly stored or all doors and windows are locked, and they cannot be read from outside;

(b) must not be left on a desk, table, or in any other freely accessible place, in such a way that non-authorised EIOPA staff or external parties, e.g. visitors, cleaners, maintenance personnel, etc., might be able to read or remove them; and

(c) must not be read nor left unattended in public places where they might be seen by non-authorised persons, e.g. trains, planes, restaurants etc.

3.56 When not attended and after working hours, the offices where regularly large quantities of sensitive information and documents are handled and stored should remain locked. These offices may be subject to other supplementary physical security controls.

3.57 Outside the EIOPA premises and only in the interest of service (for example, when handling sensitive information for teleworking, meetings and mission purposes), the sensitive documents will be preferably accessed and handled remotely, by using only EIOPA approved mobile

[14] *Please ensure you have keys for the cupboards and doors. This can be obtained from the Corporate Support Unit*

devices and IT solutions (with operating encryption and secure VPN solutions).

3.58 Printed versions of sensitive documents may be taken outside the premises, respecting the following rules:

(a) where applicable, the prior hierarchical approval is required;

(b) the holder understands and follows the security responsibilities;

(c) documents must be placed in a locked container or furniture when not attended or in use;

(d) documents must not be read or opened in public places;

(e) in order to protect from unauthorised access, documents must neither be shown to, nor discussed with, persons who do not have a justified need-to-know; and

(f) during carriage, the documents must not leave the possession of the holder at any times.

Printouts, copies and other usage considerations

3.59 Printing, scanning and creating copies of sensitive documents is not advisable unless necessary for exceptional working reasons. The security measures applicable to the original document must also be applied to the copies produced.

3.60 Any operation must be performed in such a way to prevent unauthorised access to the documents, by using local printers or password-protected printers. The devices must be checked afterwards as no originals or copies are left unsecure.

3.61 The newly created documents containing extracts from one or more sensitive documents must be protected in the same manner as the source document with the highest confidentiality level, until properly reviewed by the originator and assigned with a confidentiality level, based on the actual content. (For example, when collating information from various sources, one being assigned with EIOPA Confidential Use level, the draft document must be protected also according to that level, until it is reviewed)

3.62 Sensitive documents may be distributed in a limited number during meetings, only in accordance with the need-to-know principle.

3.63 Unless otherwise instructed, the participants must not take any sensitive document at the end of the meeting. All the distributed copies must be collected by the meeting organiser. Whenever possible, for tracking purposes, minutes of the meetings should indicate the copies of the sensitive documents remaining in the custody of the participants.

Destruction and disposal

3.64 To prevent the unnecessary accumulation of sensitive documents, drafts and unnecessary copies, those regarded by the originator or holder as out of date or surplus in number must be destroyed as soon as practicable.

3.65 EIOPA Confidential Use documents must be destroyed in shredders capable of reducing the document to a non-reconstitutable form.

3.66 EIOPA Restricted Use and EIOPA Regular Use documents may be disposed alternatively in containers designated for collection and secure disposal.

3.67 Non-reusable computer storage media (such as CD-ROMs, DVDs) must be physically destroyed (for example, by using proper shredders) as the information must not be retrievable from the media.

3.68 For the encrypted information stored electronically on various types of media or communication and information systems, file deletion would be sufficient.

3.69 The sensitive information stored non-encrypted on re-usable computer storage media (USB sticks, hard drives etc.) must be destroyed with approved methods (secure wiping utility, degauss etc.). Simple file deletion or formatting is not sufficient as the information might be very easily retrieved.

4. Roles and Responsibilities

4.1 It is the responsibility of the **EIOPA Staff** and other parties referred under paragraph 1.4 to comply with the security provisions and especially the handling of sensitive information and documents requirements set up by the working instructions.

4.2 Two particular roles have are particularly important:

(a) The **originator**[15] of EIOPA's information, having the responsibility of assigning and reviewing the confidentiality levels of information, proportional with the degree of prejudice the unauthorised access or disclosure, or loss could produce; and

(b) The **holder**[16] of the information (the authorised person having the custody of information), having the primary responsibility of taking the appropriate measures for protecting the information entrusted to him/her, by preserving its confidentiality, integrity and availability.

4.3 The **Local Security Officer** and the **Local Informatics Security Officer** have an advisory and monitoring role in supporting staff to comply with the requirements set up by the working instructions. Instructions and training are necessary for implementing the provisions of this document.

4.4 The **IT & Corporate Support Unit** supports the efforts of implementing the security requirements by identifying the suitable IT and physical security solutions and providing the originators and the holders of the information and documents with the technical means to ensure the security of information.

4.5 The **Heads of Departments and Units** and the **Team Coordinators** ensure that the handling requirements and mechanisms are properly applied and used by the staff under their coordination.

---

[15] *For continuance reasons the originator may be considered to be the originating service (a Department, Unit, Team, function or similar service). This is due to the fact the EIOPA Organigram is a living description, which might change.*

[16] *The holder has a duty of confidentiality and non-disclosure based on Staff Regulations article 17 or contractual obligations and the signature of a confidentiality agreement.*

Annex 1 – List of the approved confidentiality levels, markings and their significance[17]

Summary of assigning EIOPA confidentiality levels and marking rules:

<table>
<tr><td>PUBLIC</td><td>For example, information which is on the EIOPA website or published material may be distributed without protection. No further authorisation need be sought from the hierarchy as the decision has already been taken to make the information public.</td><td rowspan="2">Generally, no marking is required.

Documents should be preferably marked when possible according to the same rules applicable to sensitive documents.

When no marking is affixed, the document is considered to be classified as EIOPA Regular Use</td></tr>
<tr><td>EIOPA Regular Use</td><td>This type of document might be available on internal websites or be information which might be finalised and/or published only at a later date and is therefore currently an internal document. As such it is protected by the confidentiality clause derived from the Article 17 of the Staff Regulations. Some of this information can be made public later or on request (Public Access to documents).</td></tr>
<tr><td>EIOPA Restricted Use</td><td rowspan="2">Concerns information whose unauthorised disclosure would cause harm to various interested parties (confidential business / commercial information, intellectual property, personal data and so on), but which would not be so sensitive as to cause damage to EU or Member States interests.</td><td rowspan="2">Marking is required and must be affixed on the creation of the document.

On the first page of the document, upper right, by using Verdana 12 or similar sized font.

The originator of the document should be identified on the first page.</td></tr>
<tr><td>EIOPA Confidential Use</td></tr>
</table>

List of examples of possible additional markings:

[17] *To be reviewed and updated periodically*

Internal Use Only	Restricts the distribution to internal recipients within EIOPA.
Department/Unit/Team	Identifies the originator of the document
Personal	The document is intended to be consulted only by the addressee mentioned in the header of the document. Envelopes marked 'Personal' must be opened only by the addressee.
Personal Data	The document contains personal data.
Embargo Until ...	(specific date) intended to indicate time restrictions on release of information to other internal or external (third) parties
Until ...	(specific date or event) The confidentiality level specified on the document must be maintained until the mentioned specific date or the event takes place.
Deadline ...	(specific date) The date by which a document must be finalised within a service.
Releasable To ...	(EU institutions, Member States, third states, international organisations, National Competent Authorities etc.) Marking is used to indicate that the document may be released to a particular organisation or third party.

Annex 2 – Example of assigning confidentiality levels, markings and handling instructions on documents

Frankfurt, 11 December 2014
Financial Stability Team

EIOPA CONFIDENTIAL USE
INTERNAL USE ONLY

EIOPA-12/123

REPORT ON CRISIS SITUATION

<u>Subject:</u> Example of markings

This document is only for use in Financial Stability Team
Distribution on need-to-know basis
Not for publication
Not to be photocopied
All recipients should be aware of the strict application of need-to-know
Not to be distributed externally
Where email is used, this must be encrypted

Annex 3 – Sample Business Impact Assessment Questionnaire

Business Impact Assessment						
CONFIDENTIALITY RATING AND CLASSIFICATION						
Business impact types Business consequences of unintended or unauthorized **disclosure** of information (worst case)	**Business impact levels**					**Comments**
	1	**2**	**3**	**4**	**5**	
	None	**Low**	**Medium**	**High**	**Major**	
EIOPA image or reputation						
EIOPA stakeholder co-operation						
Financial, monetary, economic and commercial interests of financial market participants						
Financial, monetary, economic and commercial interests of the EU or one of its Member States						
Diplomatic relations and commercial or policy negotiation of EU or Member States with others order						
EIOPA business operations, business performance						
Financial impact on EIOPA						
EIOPA personnel safety and well-being						
Legal and compliance with regulatory requirements for EIOPA						
Summary of ratings	**1**	**2**	**3**	**4**	**5**	
The summary of rating would normally be at least as high as the highest rating assessed above						
Mapping from ratings to classification levels	**Public**	**EIOPA Regular Use**	**EIOPA Restricted Use**	**EIOPA Confidential Use**	**EUCI***	
Resulting Confidentiality classification						