

## HANDLING INSTRUCTION NO 2<sup>1</sup>

### CREATION OF CONFIDENTIAL INFORMATION

#### 1. INTRODUCTION

- (1) This handling instruction lays down detailed rules for the creation of confidential information and the attribution of classifications and/or markings. It focuses on the procedural and security conditions under which such information may be created.
- (2) The creation of confidential information is notably regulated by Article 4 of the Bureau Decision and Annexes I (Sections 4 and 8.4) and II (Security Notice 2, Chapters B and D, in particular points 23 and 27) thereto.

#### 2. PRINCIPLES

- (3) The President, the chairs of parliamentary committees, the Secretary-General and persons authorised by the Secretary-General may create confidential information and/or classify information<sup>2</sup>.
- (4) Originators<sup>3</sup> shall determine the confidentiality level of information according to their best judgement based on the level of risks associated with unauthorised disclosure of this information. If possible, the originator shall specify at the date of creation the date, period or event when the content may be downgraded or declassified.
- (5) During the creation of confidential information, such information shall be stored in accordance with handling instruction No 5.
- (6) As soon as the creation of confidential information has been finalised, it shall be registered in accordance with handling instruction No 3.
- (7) The level up to which EUCI<sup>4</sup> may be created and/or classified shall correspond to the function of the originator:

---

<sup>1</sup> Decision of the Bureau of the European Parliament of 15 April 2013 concerning the rules governing the treatment of confidential information by the European Parliament (“the Bureau Decision”).

<sup>2</sup> See Article 4(1) of the Bureau Decision.

<sup>3</sup> “Originator” means the duly authorised author of confidential information (see Article 2(o) of the Bureau Decision).

<sup>4</sup> EU classified information as defined under Article 2(d) of the Bureau Decision.

- up to EU TOP SECRET: the President of the European Parliament, chairs of parliamentary committees, the Secretary-General, the Deputy Secretary-General, the Director general for Security and Safety, the Director and the Head of Unit of the classified information unit ("CIU");
  - up to SECRET UE/EU SECRET: the Jurisconsult, the Directors-General, the Directors and the Internal Auditor;
  - up to CONFIDENTIEL UE/EU CONFIDENTIAL: the Heads of Units;
  - RESTREINT UE/EU RESTRICTED: duly authorised Parliament officials and Parliament employees working for a political group.
- (8) Authorisation to create EUCI may only be granted by the Secretary-General if the official of the European Parliament or Parliament employee working for a political group holds the appropriate level of security clearance. The template for an individual authorisation by the Secretary-General is set out in Annex I to this handling instruction. The names of persons authorised by the Secretary-General to create EUCI shall be recorded on a list drawn up by the CIU.

### **3. PRACTICE**

#### **3.1. Creation of information classified as CONFIDENTIEL UE/EU CONFIDENTIAL and above**

- (9) Before creating information classified as CONFIDENTIEL UE/EU CONFIDENTIAL and above, the originator shall submit an application to the CIU (via e-mail to CIU@europarl.europa.eu), specifying the classification level of the information to be created. Unless the originator is the President of the European Parliament, chair of a parliamentary committee or the Secretary-General, the application shall include a copy of the authorisation from the Security Authority to create and classify confidential information.
- (10) Information classified as CONFIDENTIEL UE/EU CONFIDENTIAL and above may only be created within the Secure Area of the CIU. Access by the originator to the Secure Area shall be in accordance with handling instruction No 7.
- (11) Information classified as CONFIDENTIEL UE/EU CONFIDENTIAL and above shall not be removed by the originator from the Secure Area.
- (12) Information classified as CONFIDENTIEL UE/EU CONFIDENTIAL and above may only be processed (created, edited, copied, stored, printed, deleted, destroyed etc.) on an accredited CIS. Only accredited procedures for these purposes, including environmental procedures, hardware, software, operating procedures etc. may be used.
- (13) As soon as the information is formally drawn up, the originator shall complete an initial declaration, provided by the CIU, attesting to the creation of the information (annexed to handling instruction No 3). The initial declaration shall

list all data pertinent to the correct security registration of the information<sup>5</sup>. The originator shall personally deliver the completed initial declaration to the CIU. At the moment of delivery, the completed initial declaration shall be co-signed by the originator and the CIU staff member.

- (14) The originator is responsible for ensuring that data required by Annex II, Security Notice 2, paragraph 23 to the Bureau Decision duly appears in the classified information. The relevant registration number shall be affixed by the CIU. If during the drafting process it becomes necessary to re-evaluate the classification level of the information and assign a higher or lower classification level, the originator shall inform the Security Authority thereof. If the originator does not have authorisation for a higher classification, creation of such confidential information requires a new authorisation by the Security Authority.

### **3.2. Creation of information classified as RESTREINT UE/EU RESTRICTED**

- (15) Information classified as RESTREINT UE/EU RESTRICTED may be created either within the CIU premises or in the premises of secretariats of parliamentary bodies/office holders or service.
- (16) When the originator does not have access to a properly accredited CIS, information classified as RESTREINT UE/EU RESTRICTED shall be created within the CIU premises. The originator shall submit an application to the CIU (via e-mail to CIU@europarl.europa.eu), including a copy of the Security Authority authorisation to create and/or to classify information at the said level.
- (17) When created inside the CIU premises, a registration number will be affixed by the CIU as soon as the document is finalised. When created within the premises of a parliamentary body/office holder or service, the registration number will be attributed by the originator in accordance with the numbering used in the internal logbooks of the respective parliamentary body/office holder or service<sup>6</sup>.
- (18) For the creation of information classified as RESTREINT UE/EU RESTRICTED, a uniform system shall be established within an accredited CIS. Once it becomes operational, use of this system shall be mandatory.
- (19) Until an accredited CIS becomes operational, information classified as RESTREINT UE/EU RESTRICTED shall be created under the following conditions:
- (a) the workstation shall be a stand-alone computer;
  - (b) where this is not possible, the workstation shall be physically disconnected from the network by removing the LAN connection cable before starting to work;

---

<sup>5</sup> The requirements under handling instruction No. 3 on registration, notification and destruction of confidential information fully apply.

<sup>6</sup> The requirements under handling instruction No. 3 on registration, notification and destruction of confidential information fully apply.

- (c) auto save functions, such as those present in Microsoft Word etc., shall be deactivated;
  - (d) documents shall be stored on an external accredited drive (USB or CD Rom) and not saved on the hard disk of the workstation;
  - (e) the external drive shall be clearly marked as RESTREINT UE/EU RESTRICTED and only information classified at this level shall be saved to the same media;
  - (f) the external drive shall be put under lock and key and shall not be placed If a parliamentary body/office holder or service does not have such facilities, it may request the use of CIU facilities.
- (20) Once the CIS becomes operational, the information created outside the CIS shall be uploaded into the CIS system and deleted from the external drive.
- (21) The originator shall respect the provisions of Annex II, Security Notice 2, paragraph 23 of the Bureau Decision.
- (22) Confidential information classified as RESTREINT UE/EU RESTRICTED may only be printed on dedicated printers that have been identified as forming part of an accredited CIS system.

### **3.3. Creation of 'other confidential information'**

- (23) All staff assigned to the Directorates general and services mentioned in the table of markings set out in Annex I, column 3 to handling instruction No 1 are hereby authorised to create information bearing these markings.
- (24) The originator shall respect the relevant provisions of Annex II to the Bureau Decision (see Security Notice 2, paragraph 27).
- (25) The text of 'other confidential information' may be attached to GEDA if the respective marking permits this (see handling instruction No 1).

[The Secretary-General]

## **Authorisation to create classified information in the European Parliament**

On the basis of Article 4 of the Bureau Decision of 15 April 2013 establishing the Rules governing the treatment of confidential information by the European Parliament,

The Secretary-General

acting in his/her capacity as the EP Security Authority herewith

authorises Mr/Ms.....

to create classified information in the European Parliament.

---

Name, function and administrative address of the authorised person:

Up to and including the level of confidentiality:

Authorisation is valid until:

Remarks/Instructions:.....  
.....  
.....  
.....  
.....  
.....

Signature of the Security Authority

Name:

Signature + stamp:

Place and date: