

# **HANDLING INSTRUCTION NO 11<sup>1</sup>**

## **CONTROLS, EVALUATIONS AND INSPECTIONS**

### **1. INTRODUCTION**

- (1) This handling instruction describes the security requirements for the control, evaluation and inspection of the means, premises or systems in place for the secure handling of confidential information.
- (2) Controls, evaluations and inspections are notably regulated by Annex I point 9 of the Bureau Decision and Annex II, Security Notice 4, Chapter H points 23 and 24.

### **2. PRINCIPLES**

- (3) Accountability and objectivity are the basic principles for an efficient operation and outcome of any control, evaluation or inspection.
- (4) All procedures shall be based on a risk assessment.
- (5) Control and evaluation procedures shall be conducted to check or determine if confidential information is correctly handled by European Parliament authorised individuals or services. Controls and evaluations can also be carried out within an on-going inspection.
- (6) An inspection is conducted by the European Parliament's Directorate General for Security and Safety to look into, supervise and report upon whether the handling of EUCI in the European Parliament is carried out in conformity with the applicable laws, rules and regulations.

#### **2.1. Control and evaluations**

- (7) Control and evaluation are carried out by the following services:
  - (a) For EUCI SECRET UE/ EU SECRET and above or equivalent, control and evaluation shall be carried out by the Directorate General for Security and Safety within an ongoing inspection procedure as laid down in paragraph 6 of these handling instructions.
  - (b) For EUCI CONFIDENTIEL UE/ EU CONFIDENTIAL UE or equivalent control and evaluation shall be carried out by the Directorate General for Security and Safety within an on-going inspection procedure as laid down in paragraph 6. However, when CONFIDENTIEL UE/EU CONFIDENTIAL or equivalent information is discussed in an in camera meeting , the CIU may, on its own initiative, carry out a control and evaluation procedure to check and determine whether the handling

---

<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”).

instruction for an in camera meeting where this level of classified information is examined is correctly applied. The CIU may request the assistance of the Directorate General for Security and Safety;

- (c) For EUCI RESTREINT UE/EU RESTRICTED or equivalent, the CIU may, on its own initiative, carry out a control and evaluation of logbooks, storage or in camera meetings run by the secretariat of the parliamentary body/office holder or service to ensure that the register of EUCI RESTREINT UE/EU RESTRICTED or equivalent held by the secretariat of the parliamentary office/body is securely instituted and functioning.
- (d) For 'other confidential information' control and evaluation is not mandatory. It may be submitted to control and evaluation if deemed necessary by the Secretary General or Director-General responsible for the secretariat of the parliamentary body/office holder or service holding such information.

## **2.2. Inspections**

- (8) Inspections shall be carried out by the Directorate General for Security and Safety in line with the expected level of the security arrangements for the protection of EUCI.
- (9) As part of an agreed process, the Security Authorities and services of the Council and the Commission may carry out peer evaluations initiated by either side.

## **3. PRACTICE**

### **3.1. Control and evaluations**

#### **3.1.1. CONFIDENTIEL UE/EU CONFIDENTIAL *information discussed in an in camera meeting***

- (10) CONFIDENTIEL UE/EU CONFIDENTIAL information should be consulted in the Secure Area (SA).
- (11) Notwithstanding paragraph (10), CONFIDENTIEL UE/EU CONFIDENTIAL information may be discussed in an in camera meeting in line with the provisions set out in Article 11(3) of the Bureau Decision and handling instruction No 4, point 3.2.2.
- (12) The CIU may control and evaluate how the in camera meeting is organised and held using the conformity list attached in Annex I.
- (13) At the end of the check the CIU shall issue a report. The report shall contain the:
  - (a) name of the secretariat of the parliamentary body/office holder or service;
  - (b) date of the meeting;
  - (c) participants list;
  - (d) conformity list (Annex I);
  - (e) final evaluation, which should refer to:

- i. the status of conformity or
- ii. where appropriate, the changes needed to comply with the rules applying to the handling of CONFIDENTIEL UE/EU CONFIDENTIAL classified information;

(f) Date of the control and signature of the controller.

3.1.2. RESTREINT UE/EU RESTRICTED *information discussed in an in camera meeting*

(14) The CIU may control and evaluate how the in camera meeting is organised and held, using the conformity list attached in Annex II.

(15) When such a control and evaluation takes place, the secretariat of the parliamentary body/office holder or service shall be informed in advance.

(16) At the end of the check the CIU shall issue a report. The report shall contain the:

(a) name of the secretariat of the parliamentary body/office holder or service;

(b) date of the meeting;

(c) participants list;

(d) conformity list (Annex II);

(e) final evaluation, which would only refer to:

- i. the status of conformity;
- ii. where appropriate, the changes needed to comply with the rules applying to the handling of RESTREINT UE/EU RESTRICTED classified information;

(f) Date of the control and signature of the controller.

3.1.3. RESTREINT UE/EU RESTRICTED *held outside the CIU*

(17) The CIU may control and evaluate the registration status, logbooks and storage of EUCI held by any parliamentary body/office holder or service. On such occasions the secretariat of the parliamentary body/office holder or service shall be informed before the control and evaluation takes place.

(18) The CIU shall also proceed with checks on each occasion when there is a change in the post-holder and in any case at least annually for documents which have not yet been transmitted to CIU archives.

(19) Checks shall be carried out using the conformity list attached in Annex III. They shall focus:

- (a) on the number and status of documents held in storage against the records maintained by the secretariat of the parliamentary body/office holder or service as well as the adequacy of their storage conditions;
  - (b) on the number of solemn declarations against the record of consultation;
  - (c) when appropriate, on receipts issued and received;
  - (d) on destruction certificates maintained;
  - (e) on the correct registration of documents and the availability and correct use of the register.
- (20) At the end of the check the CIU shall issue a report. The report shall contain the:
- (a) name of the secretariat of the parliamentary body/office holder or service;
  - (b) conformity list (Annex III);
  - (c) final evaluation, which should refer to:
    - i. the status of conformity or
    - ii. where appropriate, the changes needed to comply with the rules applying to the handling of RESTREINT UE/EU RESTRICTED classified information;
  - (d) date of the control and signature of the controller.

#### 3.1.4. *'Other confidential information'*

- (21) Should a control and evaluation of 'other confidential information' be decided:
- (a) all staff of the secretariat of the parliamentary body/office holder or service holding the relevant 'other confidential information' shall be informed and
  - (b) a conformity list shall be established.
- (22) The control and evaluation shall be exercised on the basis of the model of the conformity list in Annex IV. This list may be completed by further checks as deemed necessary. In this case, the secretariat of the parliamentary body/office holder or service holding the relevant 'other confidential information' shall be informed of the content of the checks.

## 3.2. INSPECTIONS

### 3.2.1. *Periodic internal inspections*

- (23) The periodic internal inspections of security arrangements for the protection of classified information shall be carried out by the European Parliament's Directorate General for Security and Safety, which may request the assistance of the Information Assurance Authority, DG ITEC and of the Commission or Council security authorities in carrying out this task.

- (24) The periodic internal inspections may be general in scope and thus the entire Information Security Management System (ISMS) may be subject to a general inspection. Alternatively they may be partial in scope, when particular parts of the ISMS are subject to an inspection.
- (25) Partial internal inspections may cover:
- (a) the physical security arrangements of the Secure Area using the conformity list in Annex V and checklist of items, zones and systems submitted to a physical inspection of the Secure Area in Annex VI;
  - (b) the physical security arrangements for Secure Reading Rooms;
  - (c) the Archive(s) of EUCI;
  - (d) the storage of EUCI;
  - (e) the transport of EUCI;
  - (f) the packaging of EUCI;
  - (g) the certified material or tools;
  - (h) other aspects considered appropriate for the protection of the confidentiality of EUCI.
- (26) The periodicity of inspections depends on its scope and under the following conditions:
- (a) general inspections shall take place every 2 years;
  - (b) when the ISMS as a whole is ready to be used. In this case the Security Authorities of the Council and the Commission shall be invited to nominate their security team to be associated with the inspection;
  - (c) on a decision of the Security Authority (SA), in particular in response to an event of relevant importance, a crisis, or as a result of a recommendation issued from an investigation (see handling instruction No 8) or from a partial internal inspection.
- (27) The Directorate General for Security and Safety shall ensure that partial inspections take place:
- (a) before any new zone, area, means, tool, facility or systems for the secure handling of EUCI is ready for use and certified;
  - (b) at least once a year, if the inspection concerns the Secure Area;
  - (c) on a request of the SA or on a recommendation of the CIU;
- (28) in line with a timeframe to be defined within the scope of the risk management strategy.

- (29) At the end of the inspection, the Directorate General for Security and Safety shall issue a report. The report shall contain:
- (a) the date(s) of the inspection;
  - (b) details of the inspection team (include institutions, where services from the Commission or the Council have been associated);
  - (c) an identification of the type of inspection (general or partial). If partial, to identify the scope of the partial inspection;
  - (d) the level of EUCI (if all levels were inspected, just mention EUCI);
  - (e) a copy of the conformity certificate or the fact that a new one may be issued;
  - (f) conclusions and recommendations.
  - (g) The date of the control and signature of the controller.
- (30) Any report issued from an inspection shall be sent to the SA, who shall take a decision on any follow up where appropriate.
- (31) The SA may inform the SA of the Council and the Commission about the results of the inspections, where Council and Commission services were not associated in the inspection procedure.

### 3.2.2. *Peer evaluations*

- (32) Peer evaluations shall be part of an agreed process between the relevant Security Authorities and may involve the relevant services of both parties. The components and reporting shall be fixed by an agreed process.
- (33) Peer evaluations of the security arrangements for the protection of classified information exchanged under the interinstitutional agreements with the Council and the Commission may be carried out by the Security Authorities and services of the Commission or Council as part of an agreed process initiated by either side.

## Annexes - Examples

- # I : Control and evaluation - conformity list - CONFIDENTIEL UE/EU  
CONFIDENTIAL information discussed in a meeting in camera
- # II : Control and evaluation - conformity list - RESTREINT UE/EU RESTRICTED  
information discussed in an in camera meeting
- # II : Control and evaluation - conformity list - RESTREINT UE/EU RESTRICTED  
information held outside the CIU
- # IV : Control and evaluation - conformity list - 'Other confidential information'
- # V : Control and evaluation - conformity list - Inspection of the secure area

## Conformity list

## CONFIDENTIEL UE/EU CONFIDENTIAL information

## discussed in an in camera meeting

Security requirements are laid down in handling instruction No 4 and reproduced on page 2 of this annex.

Check of	C <sup>2</sup>	NC <sup>3</sup>	Recommendations where appropriate
<b>The meeting is held <i>in camera</i></b>			
<b>Control of access</b> (the persons designated to participate in the meeting have the appropriate level of <b>security clearance</b> and/or <b>sign the solemn declaration</b> provided)			
<b>Solemn declaration collected</b>			
<b>No electronic communication devices</b> are taken into the room			
<b>Minutes</b> of the meeting make no mention of the content of the discussion of the information considered under the confidential procedure			
<b>Copies of documents are sealed</b> when delivered to the addressee			
<b>Briefing</b>  - the classification/marketing status of the documents (oral and written)  - not to remove the documents from the meeting room			
<b>No additional stock</b> of documents may be held in meeting rooms			
<b>Collection and verification of all copies of the documents</b> at the end of the meeting by authorised staff from parliamentary body/office holder or service responsible for the meeting			
<b>Conditions of temporary storage</b> (where appropriate)			

Date:

Signature: \_\_\_\_\_

<sup>2</sup> C = in Conformity

<sup>3</sup> NC = Not in conformity



**Consultation of information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or equivalent in an in-camera meeting**

Handling instruction No 4, point 3.2.2

- (39) Information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or equivalent may be consulted in an in-camera meeting as provided for in Article 11(3) of the Bureau Decision at the request of a parliamentary committee chair, the Conference of Presidents or the Bureau. The procedure for the temporary deposit of the information with the relevant parliamentary body is set out in handling instruction No 3.
- (40) The secretariat of the parliamentary body/office holder or service responsible for the meeting shall:
- (a) ensure that the persons designated to participate in the meeting have the appropriate authorisation, as set down in handling instruction No 12, and sign the solemn declaration on the protection of EUCI annexed hereto (Annex I);
  - (b) collect the above-mentioned completed declarations;
  - (c) ensure electronic communication devices are not taken into the room;
  - (d) ensure that all copies are provided by the CIU in accordance with the procedure set out in handling instruction No 3;
  - (e) ensure that no additional stock of documents is produced or held in the meeting rooms;
  - (f) ensure that the minutes of the meeting make no reference to the title or content of discussion on the information considered under the confidential procedure;
  - (g) ensure that classified information provided orally in the European Parliament is subject to the same level of protection as the equivalent classified information in written form;
  - (h) ensure that at the commencement of the meeting, the chair makes clear to the persons designated to participate in the meeting the classification/marketing status of the documents;
  - (i) ensure that participants are duly warned not to remove the documents from the meeting room and that participants return the documents to the person responsible for management of the meeting as set out in handling instruction No 3.

- (30) In Parliament, information classified as CONFIDENTIEL UE/EU CONFIDENTIAL and above or equivalent shall be registered and managed exclusively by the CIU. In accordance with the exceptions laid down in point 3.2.2 of Annex II to the Framework Agreement and in Article 6(5) of the Inter-Institutional Agreement between Parliament and the Council, information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or equivalent originating from the European Commission or the Council may be provided by the CIU to the secretariat of a parliamentary body/office holder or service as a temporary deposit for use at an in camera meeting, in accordance with Article 11(3) and (4) of the Bureau Decision. Further, other institutions may, under their own responsibility, provide for classified information to be used at an in camera parliamentary meeting on the basis of an established practice or following specific arrangements with the parliamentary body/office holder or service concerned.
- (31) The secretariat of the parliamentary body/office-holder or service responsible for the in camera meeting shall ensure compliance with Article 11(2) and (3) of the Bureau Decision and shall ensure that persons designated to participate in the meeting comply with Article 3 (4) and (7) of the Bureau Decision.
- (32) Information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or equivalent temporarily deposited with the secretariat of the parliamentary body/office holder or service for an in camera meeting may under no circumstances be registered by any parliamentary body/office holder or service.
- (33) When information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or equivalent is provided to the secretariat of a parliamentary body/office holder or service for an in camera meeting, the following procedure shall apply:
- (a) the CIU shall provide numbered copies of the information for each MEP in a sealed envelope;
  - (b) the CIU shall complete a confirmation of a temporary deposit for an in camera meeting, annexed hereto (Annex IV), comprising a general summary of the temporary deposit together with a comprehensive list of MEPs and their allocated copy number. The sealed envelopes shall be personally delivered to the secretariat of the parliamentary body/office holder or service at which time the secretariat shall sign the general summary in the acknowledgement of receipt and retain the comprehensive list;
  - (c) the CIU shall record this temporary deposit;
  - (d) the above mentioned sealed envelopes shall be distributed by the secretariat of the parliamentary body/office holder or service to MEPs on commencement of the meeting. MEPs shall sign the comprehensive list in the acknowledgement of receipt against their allocated copy number. The secretariat shall insert the time of delivery of each sealed envelope on the comprehensive list;

- (e) at the end of the meeting, the secretariat of the parliamentary body/office holder or service shall recover the copies of the information for each MEP in the unsealed envelopes. MEPs shall sign the comprehensive list on return against their allocated copy number. The secretariat shall insert the time of receipt of each copy of the information for each MEP on the comprehensive list. The secretariat shall return those copies of the information for each MEP together with the updated comprehensive list to the CIU without delay. The secretariat and the CIU shall co-sign the comprehensive list confirming return of the copies of the information for each MEP;
- (f) the CIU shall record the return of this information. The CIU shall destroy the copies of the information for each MEP and the unsealed envelopes without delay in an appropriate level accredited shredder (see rules on destruction in Chapter 4 of handling instruction no 3). The CIU shall store the confirmation of a temporary deposit for an in camera meeting comprising the general summary of the temporary deposit together with the comprehensive list of MEPs and their allocated copy number for a duration of five years.

ANNEX II

**CONTROL AND EVALUATION**

**Conformity list**

**RESTREINT UE/EU RESTRICTED information discussed in a meeting in camera**

Security requirements are laid down in handling instruction No 4

and reproduced on page 2 of this annex.

<b>Check of</b>	<b>C<sup>4</sup></b>	<b>NC<sup>5</sup></b>	<b>Recommendations when appropriate</b>
<b>The meeting is held <i>in camera</i></b>			
<b>Control of access</b> (only the persons designated and authorised to participate in the meeting are allowed to enter the meeting room, including the officials from the secretariat)			
<b>Copies of documents</b> (if the document is copied and several copies are to be distributed, they shall bear a copy number on every page . Each copy shall also bear on the first page the total number of copies and of pages.)			
<b>No electronic communication devices</b> are taken into the room			
<b>Minutes</b> of the meeting make no mention of the content of the discussion of the information considered under the confidential procedure			
<b>Briefing /Solemn declaration</b> (confidential information provided orally to recipients in the European Parliament is subject to the equivalent level of protection as that applied to confidential information in written form)			
<b>No additional stock</b> of documents may be held in meeting rooms			
<b>Collection and verification of all copies of the documents</b> at the end of the meeting by an authorised staff from parliamentary body/office holder responsible for the meeting			

**Date:**

**Signature:** \_\_\_\_\_

<sup>4</sup> C = in Conformity

<sup>5</sup> NC = Not in conformity

**Consultation of information classified as RESTREINT EU/EU RESTRICTED in an in camera parliamentary meeting**

(Handling instruction No 4, point 3.2.4)

- (46) Information classified as RESTREINT EU/EU RESTRICTED may be consulted in an in camera meeting held at the request of a parliamentary committee chair, the Conference of Presidents or the Bureau.
- (47) In the event that the information to be consulted during an in camera meeting is held by the CIU, the procedure for the temporary deposit of the information with the relevant parliamentary body set out in handling instruction No 3 shall apply.
- (48) Unless additional security requirements are requested, the secretariat of the parliamentary body/office holder or service responsible for the meeting shall:
  - (a) ensure that only persons designated by the chair of the committee or body to participate are permitted to enter the meeting room and, further, ensure that all those persons sign the solemn declaration on the protection of EUCI annexed hereto (Annex I to handling instruction No 4);
  - (b) ensure all copies of documents are numbered, distributed on commencement of the meeting, recovered and accounted for at the end of the meeting and, further, ensure that no notes, copies or photographs of the documents are made;
  - (c) ensure that the minutes of the meeting make no reference to the content of discussion on the information considered and only make reference to the relevant decision, if appropriate;
  - (d) ensure that confidential information provided orally in the European Parliament is subject to the same level of protection as the equivalent confidential information in written form;
  - (e) ensure that no additional stock of documents are produced or held in meeting rooms;
  - (f) distribute only the requisite number of copies of documents to participants and interpreters;
  - (g) ensure that at the commencement of the meeting, the chair makes clear to the persons designated to participate in the meeting the classification/marketing status of the documents;
  - (h) ensure that participants are duly warned not to remove documents from the meeting room;
  - (i) ensure that no electronic communication devices or other electronic devices are allowed in the meeting room.

ANNEX III

**CONTROL AND EVALUATION**

**Conformity list**

**RESTREINT UE/EU RESTRICTED held outside the CIU**

<b>Check of</b>	<b>C<sup>6</sup></b>	<b>NC<sup>7</sup></b>	<b>Recommendations when appropriate</b>
Number and status of documents held in storage			
Storage conditions			
Number of solemn declarations against the record of consultation			
Destruction certificates			
Correct use and record			

**Date:**

**Signature:**

---

<sup>6</sup> C = in Conformity

<sup>7</sup> NC = Not in Conformity

ANNEX IV

**CONTROL AND EVALUATION**

**Conformity list**

**'Other confidential information'**

This list may be complemented. The items inserted are nonetheless recommended in case such a procedure takes place.

<b>Check of</b>	<b>C<sup>8</sup></b>	<b>NC<sup>9</sup></b>	<b>Recommendations when appropriate</b>
Number and status of documents held in storage			
Store conditions			
Correct use and record			

---

<sup>8</sup> C = in Conformity

<sup>9</sup> NC = Not in conformity

ANNEX V

**CONTROL AND EVALUATION**  
**CONFORMITY LIST (Sample)**  
**INSPECTION OF THE SECURE AREA**

(To be printed on Directorate General for Security and Safety headed paper)

INSPECTED ZONE OR SYSTEM	SECURITY REQUIREMENT OR CONTROL	C <sup>10</sup>	PC <sup>11</sup>	NC <sup>12</sup>	OBSERVATION OR RECOMMENDATION
Ex: video surveillance and monitoring system (VSMS=CCTV)	A video surveillance and monitoring system (VSMS) is installed and operating				
	The entire area or all possible entries and exits are under the VSMS surveillance				
	The VSMS is an autonomous and closed system:				
	- Access to control functions of the system is only possible within the zone				
	- Access to real-time images is only possible within the zone				
	- Access to recorded images is only possible within the zone				
	The VSMS has sufficient (e.g.: 24 hours) recording storage capabilities				
	The VSMS is connected to a no-break power supply or as an autonomous power supply (UPS) with sufficient (e.g.: 8 hours) electrical power autonomy				

**Date:**

**Signature:** \_\_\_\_\_

---

<sup>10</sup> C = Compliant  
<sup>11</sup> PC = Partially Compliant  
<sup>12</sup> NC = Non-Compliant



## ANNEX VI

### LIST OF ITEMS, ZONES AND SYSTEMS

#### SUBMITTED TO A PHYSICAL INSPECTION OF THE SECURED AREA

- SAS (Security access screening room / Système d'accès sécurisé)
- All rooms (meeting room, consultation/reading room, archives, registry room, crypto and communication room)
- Walls
- Windows
- Doors
- Access control systems
  - o badges and badge control
  - o biometry
  - o Pin-code terminal
  - o Doors contacts
  - o Urgency trigger
  - o BCR
  - o BCZR
  - o Power supply and batteries
- Intrusion detection systems
- Keys and Keys combinations
- CCTV Monitoring System /Système de Surveillance CCTV
- Remote Control System /Système de Telegestion
- Two-Way Warning System
- Extinguishers
- Lockers and safes
- Stand-alone reproductive machinery (copiers, printers, etc)
- Stand-alone PCs
- Shredders

Any item, zone or system not listed present in the secured area must be inspected, listed and reported.