HANDLING INSTRUCTION 8[1]

BREACHES OF SECURITY, LOSS OR COMPROMISE OF CONFIDENTIAL INFORMATION AND INVESTIGATIONS

1. INTRODUCTION

(1) A breach of security occurs as a result of an act or omission by an individual which is contrary to the security rules laid down in the Bureau Decision and its handling instructions.

(2) Compromise of confidential information occurs when, as a result of a breach of security, confidential information, has, wholly or in part, been disclosed to unauthorised persons or if the likelihood exists of such an event having occurred.

(3) Any breach or suspected breach of security shall be reported immediately to the Secretary General acting as Security Authority, who shall take all appropriate measures.

(4) In the event of a breach or suspected breach of security involving a Member of the European Parliament, the Secretary General shall act in liaison with the President of Parliament.

(5) A breach of security relating to EU classified information (EUCI) may lead to severe sanctions, including eventual criminal proceedings.

(6) Members of the European Parliament, Parliament officials and other Parliament employees working for political groups required and authorised to handle confidential information shall refrain from careless, negligent or indiscreet behaviour and immediately report any breach of security to the Secretary General, as Security Authority.

2. PRINCIPLES

(7) An individual responsible for a breach of the security rules laid down in the Bureau Decision and its handling instructions may be liable to disciplinary action in accordance with applicable rules and regulations.

(8) An individual responsible for compromising or losing confidential information shall be liable to disciplinary and/or legal action in accordance with the applicable laws, rules and regulations.

(9) With regard to breaches of security in the case of EUCI provided to the European Parliament by the Council or the Commission under the relevant interinstitutional agreement, the Council and the Commission may react along the same lines. In the event that the said information was provided as part of a

[1] 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

Security of Information Agreement between the Council or the Commission with national authorities, third states or international organisations, disciplinary and/or legal action may be initiated by that third party.

3. PRACTICES

(10) Members of the European Parliament, Parliament officials and other Parliament employees working for political groups required to handle classified information shall be thoroughly briefed on security procedures, the dangers of indiscreet conversation and relationships with the media. They shall, where appropriate, sign a declaration attesting to non-disclosure of the contents of confidential information to third persons, full respect for the obligation to protect classified information and acknowledgement of consequences of any failure in this regard. Any access to or use of classified information by a person not having been briefed and having signed the declaration shall be considered a breach of security.

(11) Members of the European Parliament, Parliament officials and other Parliament employees working for political groups or contractors shall immediately report any breach of security, loss or compromise of confidential information coming to their notice to the Secretary General and, further, shall refrain from disclosing this breach to any other person.

(12) When reporting a breach of security, loss or compromise of confidential information, the following shall be submitted in writing without delay:

(a) reference to the information involved, including classification reference and, if possible, copy number, date, origin, subject and scope;

(b) a brief description of the circumstances involved, including the date and time period when the information was exposed to compromise.

(13) The report of a breach of security, loss or compromise of confidential information shall be handled in conformity with the appropriate level of confidentiality.

(14) Where it is known or where there are reasonable grounds to assume that confidential information has been compromised or lost, the Secretary General, as Security Authority shall take appropriate measures in accordance with the relevant laws and regulations to:

(a) inform the originator and/or the depository Institution;

(b) ensure that an investigation to establish the facts is carried out by staff not linked with the breach;

(c) assess potential damage to the interest of the Union;

(d) take appropriate measures to prevent any recurrence; and

(e) notify the appropriate authorities of actions taken.

(15) The Secretary-General may be assisted in these tasks by the Directorate-General for Security and/or the Classified Information Unit (CIU), entrusting them to:

(a) establish the facts;

(b) safeguard evidence;

(c) assess and minimise potential damage;

(d) report on possible measures to prevent recurrence.

(16) The Directorate-General for Security or the CIU shall keep the Secretary General informed at all stages.

(17) The CIU in agreement with the Risk Management Unit of the Directorate-General for Security shall establish security operational procedures.

(18) Members of the European Parliament, Parliament officials or other Parliament employees working for political groups responsible for a breach of the security rules laid down in the Bureau Decision and its handling instructions may be liable to disciplinary action in accordance with the applicable rules and regulations.

(19) Members of the European Parliament, Parliament officials or other Parliament employee working for political groups responsible for compromising or losing confidential information shall be liable to disciplinary and/or legal action in accordance with the applicable laws, rules, and regulations.

(20) Managers shall be fully aware of the identities of their staff engaged in work on classified information or having access to classified information or to the accredited Communication Information System (CIS). Managers shall record and report on any incident or apparent vulnerability with a possible bearing on security.

(21) In the event that any adverse information concerning an individual with access to classified information becomes known, the Directorate for Security shall be informed without delay. When established that such an individual constitutes a security risk, the person shall be duly barred or removed from all assignments linked to classified information.