# EUROPEAN EXTERNAL ACTION SERVICE

## Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 15 June 2011 on the security rules for the European External Action Service

(2011/C 304/05)

THE HIGH REPRESENTATIVE,

Having regard to Council Decision 2010/427/EU establishing the organisation and functioning of the European External Action Service ('EEAS'), in particular Article 10 thereof,

Having regard to the opinion of the Committee referred to in Article 10(1) of the abovementioned Council Decision,

Whereas:

(1) The EEAS, as a functionally autonomous body of the European Union, should have security rules as referred to in Article 10(1) of Council Decision 2010/427/EU.

(2) The High Representative should decide on security rules for the EEAS covering all aspects of security so that the EEAS can manage effectively the risks to its staff, physical assets and information, and fulfil its duty of care responsibilities in this regard.

(3) The security rules for the EEAS should help achieve a more coherent comprehensive general framework within the European Union for protecting classified information, building on the Council security rules and the Commission security provisions.

(4) In particular, a level of protection should be afforded to EEAS staff, physical assets and information, which is in line with best practice in the Council, the European Commission, the Member States and, as appropriate, international organisations.

(5) The basic principles and minimum standards for protecting classified information applied in the EEAS should be equivalent to those applied in the Council and the European Commission.

(6) It is necessary to establish the organisation of security in the EEAS and the allocation of security tasks within the EEAS structures.

(7) The High Representative should take all appropriate measures necessary to implement these rules with the support of the Member States, the General Secretariat of the Council and the European Commission.

(8) The High Representative should draw on relevant expertise in the Member States, the General Secretariat of the Council and the European Commission as necessary, including through appropriate security structure,

HAS ADOPTED THIS DECISION:

*Article 1*

**Purpose and scope**

1. This Decision lays down the rules for the safety and security of the European External Action Service (hereinafter 'EEAS security rules'). It establishes the general regulatory framework for managing effectively the risks to staff, physical assets and information, and for fulfilling its duty of care responsibilities in this regard.

2. The EEAS security rules shall apply to all EEAS staff (i.e. officials and other servants, seconded national experts and local agents) and to all staff in Union Delegations, regardless of their administrative status or origin (hereinafter 'staff').

3. The High Representative shall take any measures necessary in order to implement these rules in the EEAS and build up the necessary capacity covering all aspects of security with the support of the relevant services of the Member States, the General Secretariat of the Council and the Commission.

4. From the entry into force of the present Decision, transitional arrangements may be used, as necessary, through service-level agreements with the relevant services of the General Secretariat of the Council and the Commission.

5. The High Representative shall keep these security rules under review. The High Representative shall ensure overall consistency in the application of this Decision.

6. Where necessary, the High Representative, on recommendation by the Committee referred to in Article 9(6), shall approve security policies setting out measures for implementing this Decision. That Committee may agree at its level security guidelines to supplement or support this Decision.

7. In implementing paragraph 6, the Committee shall take full account of security policies and guidelines in force in the Council and the European Commission, in order to maintain consistency between the respective security measures in the EEAS, the Council and the Commission.

*Article 2*

**Security risk management**

1. In order to determine its protective security needs, the EEAS shall apply a comprehensive security risk assessment methodology in consultation with the Security Office of the General Secretariat of the Council and the Security Directorate of the European Commission. The Committee referred to in Article 9(6) shall be consulted on its application in the EEAS.

2. Risk to staff, physical assets and information shall be managed as a process. This process shall be aimed at determining known security risks, at defining security measures to reduce such risks to an acceptable level and at applying measures in line with the concept of defence in depth. The effectiveness of such measures shall be continuously evaluated.

3. The roles, responsibilities and tasks laid down in this Decision are without prejudice to the responsibility of each EEAS staff member to exercise common sense and good judgement with regard to their own safety and security, as well as the requirement for them to comply with all applicable security rules, regulations, procedures and instructions.

4. The EEAS shall take all reasonable measures to ensure the safety and security of staff, physical assets and information and to prevent reasonably foreseeable damage thereto pursuant to Article 1(3).

5. Security measures in the EEAS for protecting classified information throughout its life cycle shall be commensurate in particular with its security classification, the form and volume of the information or material, the location and construction of facilities housing classified information and the threat, including the locally assessed threat, of malicious and/or criminal activities, including espionage, sabotage and terrorism.

*Article 3*

**The protection of information**

1. The High Representative shall, after consulting the Committee referred to in Article 10(1) of Council Decision 2010/427/EU establishing the organisation and functioning of the EEAS, decide on rules for protecting classified information equivalent to those set out in the Council Decision 2011/292/EU on the security rules for protecting EU classified information [1] (hereinafter 'EUCI'). Pending the adoption of these rules, the EEAS shall apply *mutatis mutandis* the above-mentioned security rules of the Council. The High Representative shall take all necessary measures to implement those rules in the EEAS pursuant to Article 1(3).

2. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the EEAS, the EEAS shall protect that information in accordance with the requirements applicable to EUCI at the equivalent level, as set out in the applicable rules pursuant to Article 3(1).

3. With regard to the protection of sensitive unclassified information, the security measures within the EEAS shall be commensurate with its sensitivity and/or the impact of its unauthorised disclosure on EU interests.

*Article 4*

**Physical security**

1. Appropriate physical security measures, including access control arrangements, shall be put in place for all premises, buildings, offices, rooms and other areas in the EEAS, as well as areas housing communication and information systems handling classified information. Such measures shall be taken into account in the design and planning of buildings.

2. Where necessary, physical security measures for the protection of staff and their dependants shall be put in place.

3. The measures referred to in paragraphs 1 and 2 shall be commensurate with the assessed risk to staff and visitors, physical assets and information.

4. Areas in the EEAS, in which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, or its equivalent, is stored, shall be established as secured areas in accordance with the rules pursuant to Article 3(1) and shall be approved by the competent security authority within the EEAS.

*Article 5*

**Personnel security clearance**

1. Access to classified information and personnel security clearance procedures shall be governed by the requirements laid down in the rules pursuant to Article 3(1).

2. All staff whose duties may require them to have access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, or its equivalent, shall be security-cleared to the

[1] Council Decision 2011/292/EU of 31 March 2011 on the security rules for protecting EU classified information (OJ L 141, 27.5.2011, p. 17).

relevant level before being granted access to such classified information. However, local agents shall not be granted access to EUCI except and in accordance with the conditions laid down in the rules pursuant to Article 3(1).

3. The personnel security clearance procedures for EEAS staff shall be laid down in the rules pursuant to Article 3(1). These procedures shall provide a level of assurance equivalent to that provided for in the procedures applied in the European Commission and the General Secretariat of the Council.

*Article 6*

**Security of communication and information systems**

1. The EEAS shall protect information handled in communication and information systems (hereinafter 'CIS') against threats to confidentiality, integrity, availability, authenticity and non-repudiation.

2. All CIS handling classified information shall undergo an accreditation process. The EEAS shall apply a system for managing security accreditation in consultation with the General Secretariat of the Council and the European Commission.

3. Where the protection of EUCI is provided by cryptographic products, such products shall be approved by the EEAS Crypto Approval Authority on a recommendation by the Committee referred to in Article 10(1) of Council Decision 2010/427/EU establishing the organisation and functioning of the EEAS, in accordance with Article 10 of Council Decision 2011/292/EU on the security rules for protecting EU classified information.

4. The High Representative shall, to the extent necessary, establish the following information assurance functions, pursuant to Article 3(1):

(a) an information assurance authority;

(b) a TEMPEST authority;

(c) a crypto approval authority;

(d) a crypto distribution authority.

5. For each system, the High Representative shall establish the following functions, pursuant to Article 3(1):

(a) a security accreditation authority;

(b) an information assurance operational authority.

*Article 7*

**Security awareness and training**

1. The High Representative shall ensure that appropriate security awareness and training programmes are drawn up and implemented in the EEAS, and that staff and, where appropriate, their dependants, receive the necessary awareness briefings and training commensurate with the risks in their place of residence.

2. Before being granted access to classified information and at regular intervals thereafter, staff shall be briefed on and acknowledge their responsibilities to protect EUCI in accordance with the rules pursuant to Article 3(1).

*Article 8*

**Security breaches and compromise of classified information**

1. Any breach or suspected breach of security shall be reported immediately to the EEAS Security Directorate, which shall inform the relevant authorities of the Commission, the General Secretariat of the Council or the Member States as necessary.

2. Where it is known or where there are reasonable grounds to suspect that classified information has been compromised or lost, the EEAS Security Directorate shall inform the Security Directorate of the European Commission, the General Secretariat of the Council or the Member State as appropriate and take all relevant measures in accordance with the rules pursuant to Article 3(1).

3. Any member of staff who is responsible for a breach of the security rules laid down in this Decision may be liable to disciplinary action in accordance with the applicable rules and regulations. Any individual who is responsible for compromising or losing classified information shall be liable to disciplinary and/or legal action in accordance with the applicable laws, rules and regulations.

*Article 9*

**Organisation of security in the EEAS**

1. The High Representative shall be the security authority of the EEAS. In that capacity, the High Representative shall ensure in particular that:

(a) security measures are coordinated as necessary with the competent authorities of the Member States, the General Secretariat of the Council and the European Commission, and, as appropriate, third States or international organisations, on all security matters relevant for the EEAS' activities, including on the nature of threats to the security of staff, physical assets and information and the means of protection against them;

(b) security aspects are fully taken into account from the outset for all EEAS activities;

(c) EU Personnel Security Clearances are issued to EEAS staff in accordance with Article 5(2) before they may be granted access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, or its equivalent;

(d) a registry system for security purposes is established within the EEAS which shall ensure that classified information is handled in accordance with the rules pursuant to Article 3(1) and that a record is kept of all classified information released by the EEAS to third States and international organisations, and of all classified information received from third States or international organisations;

(e) security inspections referred to in Article 11 are undertaken;

(f) investigations are conducted into any actual or suspected breach of security, including compromise or loss of classified information held by or originating in the EEAS, and that the relevant security authorities are requested to assist in such investigations;

(g) in order to give a timely and effective response to security incidents, appropriate incident and consequence management plans and mechanisms are established;

(h) appropriate measures are taken in the event of failure by staff to comply with this Decision.

2. The High Representative may enter into administrative arrangements as necessary, and in particular with regard to the exchange of classified information with third States or international organisations, without prejudice to Article 218(3) of the Treaty on the Functioning of the European Union. The Committee referred to in Article 9(6) shall be consulted before they are entered into.

3. The Executive Secretary-General shall ensure that appropriate physical and organisational measures are in place for the security and safety of staff and visitors, physical assets and information in all EEAS premises. The Executive Secretary-General shall be assisted in this task by the Chief Operating Officer and the EEAS Security Directorate.

4. The EEAS shall have a Security Directorate responsible for organising all security matters in the EEAS, which shall be at the disposal of, and when necessary may report to, the High Representative in accordance with its mandate. In accordance with Article 10(3) of Council Decision 2010/427/EU establishing the organisation and functioning of the EEAS, the Security Directorate shall be assisted by the competent services of the Member States.

5. The Head of each Union Delegation shall be responsible for implementing all measures relating to the security of the Delegation, and shall manage the security and safety of the Delegation's staff and visitors, physical assets and information. He shall be assisted in these tasks by the EEAS Security Directorate, by Delegation staff exercising dedicated tasks and functions, and by dedicated security staff posted where necessary.

6. A Security Committee is hereby established. The High Representative shall seek the advice of the Security Committee, which shall examine and assess any security matter within the scope of this Decision and make recommendations, as appropriate. The Security Committee shall be composed of relevant security experts representing each Member State, the General Secretariat of the Council and the Security Directorate of the European Commission. It shall be chaired by the High Representative or designated delegate, and shall meet as instructed by the High Representative or at the request of any of its members. The Security Committee shall organise its activities in such a way that it can make recommendations on any specific area of security within the scope of this Decision.

7. The Head of the Security Directorate of the EEAS shall meet regularly, and whenever necessary, to confer on areas of common interest with the Director of Security of the General Secretariat of the Council and the Director of the Security Directorate of the European Commission.

*Article 10*

**Security of CSDP missions and EUSR**

The responsibility of each Head of Mission or EU Special Representative (EUSR) with regard to the security of the mission or team is laid down in the Council Decision establishing the mission or appointing the EUSR. Each Head of Mission or EUSR may be assisted by the EEAS Security Directorate in ensuring that the policy approved by the Council on the security of personnel deployed outside the EU in an operational capacity under Title V, Chapter 2 of the Treaty on European Union is duly implemented. Appropriate liaison mechanisms shall be established to that effect.

*Article 11*

**Security inspections**

1. The High Representative shall ensure that security inspections are undertaken in order to verify compliance with the security rules and regulations for protecting staff, physical assets and information within the EEAS and in missions established under Title V, Chapter 2 of the TEU.

2. The EEAS may draw, as necessary, on expertise in the Member States, the General Secretariat of the Council and the European Commission.

3. The High Representative shall adopt an annual security inspection programme.

*Article 12*

**Business continuity planning**

The EEAS Security Directorate shall assist the Executive Secretary-General in managing the security-related aspects of EEAS business processes as part of the overall Business Continuity Planning of the EEAS.

*Article 13*

**Entry into force**

This Decision shall enter into force on the date of its signature.

Done at Brussels, 15 June 2011.

*The High Representative*

C. ASHTON