IV

(Notices)

NOTICES FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

EUROPEAN EXTERNAL ACTION SERVICE

DECISION OF THE HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

of 19 April 2013

on the security rules for the European External Action Service

(2013/C 190/01)

THE HIGH REPRESENTATIVE,

Having regard to Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the European External Action Service [1] ("EEAS"),

Having regard to the opinion of the Committee referred to in Article 9(6) of the Decision of the High Representative of 15 June 2011 on the security rules for the European External Action Service [2],

Having regard to the opinion of the Committee referred to in Article 10(1) of Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the EEAS,

Whereas:

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

(2) The High Representative of the Union for Foreign Affairs and Security Policy (hereinafter "High Representative" or "HR") should decide on security rules for the EEAS covering all aspects of security regarding the functioning of the EEAS, so that it can manage effectively the risks to staff placed under its responsibility, to its physical assets, information, and visitors, and fulfil its duty of care responsibilities in this regard;

(3) In particular, a level of protection should be afforded to staff placed under the responsibility of the EEAS, to EEAS physical assets, including communication and information systems, information, and visitors, which is in line with the best practice in the Council, the Commission, the Member States and, as appropriate, in international organisations;

(4) The security rules for the EEAS should help achieve a more coherent comprehensive general framework within the EU for protecting EU Classified Information (hereinafter referred to as "EUCI"), building on, and maintaining as much coherence as possible with, the Council of the European Union (hereinafter referred to as "the Council") security rules and the European Commission security provisions;

(5) The EEAS, the Council and the Commission are committed to applying equivalent security standards for protecting EUCI;

(6) This Decision is taken without prejudice to Articles 15 and 16 of the Treaty on the Functioning of the European Union (TFEU) and to instruments implementing them;

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

[1] OJ L 201, 3.8.2010, p. 30.
[2] OJ C 304, 15.10.2011, p. 5.

(8) The High Representative should draw on relevant expertise in the Member States, in the General Secretariat of the Council and in the Commission as necessary;

(9) 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 Commission,

HAS ADOPTED THIS DECISION:

Article 1

Purpose and scope

This Decision lays down the security rules for the European External Action Service (hereinafter "EEAS security rules").

Pursuant to Article 10(1) of Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the European External Action Service, it shall apply to the EEAS staff and all staff in Union Delegations, regardless of their administrative status or origin, and it shall establish the general regulatory framework for managing effectively the risks to staff placed under the responsibility of the EEAS as referred to in Article 2, to EEAS premises, physical assets, information, and visitors.

Article 2

Definitions

For the purpose of this decision, the following definitions shall apply:

(a) "EEAS staff" means EEAS officials and other servants, including personnel from the diplomatic services of the Member States appointed as temporary agents, seconded national experts, as defined in Article 6 of Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the European External Action Service.

(b) "Staff placed under the responsibility of the EEAS" means the EEAS staff and all staff in Union Delegations, regardless of their administrative status or origin, as well as, in the context of this decision, the High Representative and, as appropriate, other staff resident in EEAS Headquarters premises.

(c) "Dependants" means the members of the family of the staff placed under the responsibility of the EEAS in Union Delegations forming part of their respective household as notified to the Ministry for Foreign Affairs of the receiving State.

(d) "EEAS premises" means all EEAS establishments, including buildings, offices, rooms and other areas, as well as areas housing communication and information systems (including those handling EUCI), where the EEAS conducts permanent or temporary activities.

(e) "EEAS security interests" means the Staff placed under the responsibility of the EEAS, EEAS premises, dependants, physical assets, including communication and information systems, information, and visitors.

(f) "EUCI" means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.

Other definitions are listed in the relevant Annexes and in Appendix A.

Article 3

Duty of care

1. The EEAS security rules shall aim at fulfilling the duty of care responsibilities of the EEAS.

2. The EEAS duty of care comprises due diligence in taking all reasonable steps to implement security measures to prevent reasonably foreseeable harm to EEAS security interests.

It encompasses both security and safety components, including those resulting from emergency situations or crises, whatever their nature.

3. Taking into account the duty of care responsibility of Member States, EU institutions or bodies and other parties with staff in Union Delegations and/or in Union Delegation premises, or such responsibility incumbent upon the EEAS when Union Delegations are hosted in above mentioned other parties' premises, the EEAS shall enter into administrative arrangements with each of the above entities that shall address the respective roles and responsibilities, tasks and cooperation mechanisms.

Article 4

Physical and infrastructure security

1. The EEAS shall put in place all appropriate physical security measures (whether permanent or temporary), including access control arrangements, in all EEAS premises, for the protection of EEAS security interests. Such measures shall be taken into account in the design and the planning of new premises or before leasing existing premises.

2. In third countries, the EEAS shall also put in place any appropriate additional physical security measures, permanent or temporary, for the protection of its security interests.

To this end, special obligations or restrictions can be imposed on staff placed under the responsibility of the EEAS and on dependants, for security reasons, for a specific period and in specific areas.

3. The measures referred to in paragraphs 1 and 2 shall be commensurate with the assessed risk.

Article 5

The protection of classified information

1. The protection of EUCI shall be governed by the requirements laid down in this decision, and in particular in Annex A. The holder of any item of EUCI shall be responsible for protecting it accordingly.

2. EEAS shall ensure that access to classified information is only granted to individuals who meet the conditions set out in Article 5 of Annex A.

3. The conditions under which local agents may have access to EUCI shall also be laid down by the High Representative, in accordance with the rules for protecting EUCI laid down in Annex A to this decision.

4. The EEAS Security Directorate manages a database on the security clearance status of all Staff placed under the responsibility of the EEAS and of EEAS contractors.

5. 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 Annex A to this decision.

6. Areas in the EEAS, in which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, or classified at an equivalent level, is stored, shall be established as secured areas in accordance with the rules pursuant to Annex A to this decision, and shall be approved by the EEAS security authority.

7. Procedures for performing High Representative responsibilities in the framework of agreements or administrative arrangements for the exchange of EUCI with third States or international organisations are described in Annexes A and AVI of this Decision.

Article 6

Security incidents and emergencies

1. In order to ensure a timely and effective response to security incidents, the EEAS shall establish a process for reporting such incidents and emergencies, which shall be operational twenty-four hours a day, seven days a week and cover any kind of security incidents or threats to the EEAS security interests (e.g. accidents, conflict, malicious acts, criminal acts, kidnap and hostage situations, medical emergencies, communication and information systems incidents, cyber attacks, etc.).

2. Emergency liaison channels shall be established between the EEAS Headquarters, the Union Delegations, the Council, the Commission, the EU Special Representatives and Member States, to support them in managing security incidents involving personnel and their consequences, including contingency planning.

3. This security incident management shall include, inter alia:

— procedures for effectively supporting the decision-making process in relation to a security incident involving personnel, including decisions relating to the extraction or the suspension of a mission; and

— a policy and procedures for personnel recovery - e.g. in the case of missing personnel or kidnap and hostage situations - taking into account the particular responsibilities of the Member States, of the EU Institutions and of the EEAS in this regard. The need for specific capabilities, within the management of such operations in this regard, shall be considered taking into account the resources that could be provided by the Member States.

4. The EEAS shall put in place appropriate administrative arrangements for reporting security incidents in Union Delegations. When appropriate, the Member States, the Commission, any other relevant authority, as well as the relevant Security Committees shall be informed.

5. The incident management processes should be regularly exercised and reviewed

Article 7

Security of communication and information systems

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

2. Rules, a security policy and a security programme for protecting all CIS owned or operated by EEAS shall be approved by the EEAS security authority as defined in Article 12, Section I, paragraph 1.

3. The rules, the policy and the programme shall be in conformity and their implementation closely coordinated with those of the Council and the Commission, and, where appropriate, with the security policies applied by the Member States.

4. 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 Commission.

5. Where the protection of EUCI handled by the EEAS is provided by cryptographic products, such products shall be approved by the EEAS Crypto Approval Authority on a recommendation by the Council Security Committee.

6. The EEAS security authority shall, to the extent necessary, establish the following information assurance functions:

(a) an information assurance authority;

(b) a TEMPEST authority;

(c) a crypto approval authority;

(d) a crypto distribution authority.

7. For each system, the EEAS security authority shall establish the following functions:

(a) a security accreditation authority;

(b) an information assurance operational authority.

8. Provisions for implementing this Article as regards the protection of EUCI are set out in Annex A and A IV.

Article 8

Security breaches and compromise of classified information

1. A breach of security occurs as the result of an act or omission by an individual which is contrary to the security rules laid down in this Decision and/or to the security policies or guidelines setting out any measures necessary for its implementation, as approved in accordance with article 20(1).

2. A compromise of classified information occurs when it has wholly or in part been disclosed to unauthorised persons or entities.

3. Any breach or suspected breach of security, and any compromise or suspected compromise of classified information shall be reported immediately to the EEAS Security Directorate, which shall take appropriate measures as set out in Annex A.

4. Any individual who is responsible for a breach of the security rules laid down in this Decision, or for compromising classified information, may be liable to disciplinary and/or legal action, in accordance with the applicable laws, rules and regulations, as set out in Article 11(3) of Annex A.

Article 9

Investigation of security incidents, breaches and/or compromises and corrective actions

1. The EEAS Security Directorate assisted by experts from Member States and/or from other EU institutions as appropriate, and upon authorisation from the Chief Operating Officer as necessary, shall:

(a) conduct investigations or verifications, as appropriate:

(i) where it is known or where there are reasonable grounds to assume that classified information relevant to EEAS has been compromised or lost;

(ii) on any actual or suspected breach of security or other security incidents or threats to the EEAS security interests;

(b) implement any necessary corrective actions resulting from investigations, when and as appropriate.

2. Investigators shall have access to all information necessary for the conduct of such investigations and shall receive the full support of all EEAS services in this regard.

Investigators may take appropriate actions to safeguard the trail of evidence in a manner that is proportionate to the seriousness of the matter under investigation.

3. Where access to information relates to personal data, including those contained in communication and information systems, such access shall be in accordance with Regulation (EC) 45/2001.

4. Where it is necessary to establish an investigative database that will contain personal data, the European Data Protection Supervisor (EDPS) shall be notified in accordance with the aforementioned regulation.

Article 10

Security risk management

1. In order to determine its protective security needs, the EEAS shall develop, in close cooperation with the Security Directorate of the Commission and, where appropriate, with the Security Office of the General Secretariat of the Council, a comprehensive security risk assessment methodology.

2. Risks to EEAS security interests 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, and the level of risk, shall be continuously evaluated.

3. The roles, responsibilities and tasks laid down in this Decision are without prejudice to the responsibility of each member of staff placed under the responsibility of the EEAS; in particular EU staff on mission in third countries must exercise common sense and good judgement with regard to their own safety and security, and comply with all applicable security rules, regulations, procedures and instructions.

4. The EEAS shall take all reasonable measures to ensure its security interests are protected, and to prevent reasonably foreseeable damage thereto.

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

Article 11

Security awareness and training

1. The EEAS security authority shall ensure that appropriate security awareness and training programmes are drawn up and implemented, and that Staff placed under the responsibility of the EEAS as well as, where appropriate, their dependants, receive the necessary awareness briefings and training commensurate with the risks in their place of work or residence.

2. Before being granted access to EUCI 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 5.

Article 12

Organisation of security in the EEAS

Section 1

General provisions

1. The Chief Operating Officer (COO) shall be the security authority of the EEAS. In that capacity, the COO shall ensure that:

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

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

(c) access to classified information is only granted to individuals who meet the conditions set out in Article 5 of Annex A;

(d) a registry system is established which shall ensure that information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is handled in accordance with this decision within EEAS, and when released to EU Member States, EU Institutions, bodies or agencies or other authorised recipients. A separate record shall be kept of all EUCI 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 15 are undertaken;

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

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

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

(i) appropriate physical and organisational measures are in place for the protection of the EEAS security interests.

In this regard, in consultation with the Executive Secretary General, the COO:

— sets the security category of the Delegations, in consultation with the Commission,

— decides, after consulting the HR, when Delegation staff should be evacuated if the security situation requires it,

— decides on the measures to be applied for the protection of dependants, when appropriate, taking into account arrangements with EU institutions as referred to in article 3(3);

— approves the crypto communication policy, in particular the programme of installation of cryptographic products and mechanism.

2. The COO shall be assisted in this task by the Managing Director for Administration and Finance, by the Head of EEAS Security Directorate, and, as appropriate, by the Managing Director for the Crisis Response and Operational Coordinator.

3. The COO as EEAS security authority may delegate tasks in this regard, as appropriate.

4. Each Head of department/division shall be responsible for implementing rules on protecting EUCI within his department/division.

Whilst remaining responsible as mentioned above, each Head of department/division shall designate staff for a Departmental Security Coordinator function, whose resources shall be proportionate to the amount of EUCI handled by that department/division.

Departmental Security Coordinators shall, when and as appropriate, assist and support their Head of department/division in performing tasks related to security, such as:

(a) developing any additional security requirements appropriate to the specific needs of the department/division;

(b) giving periodic security briefings to the members of their department/division;

(c) ensuring the need-to-know principle is respected in their department/division;

(d) maintaining up-to-date a list of safe codes and keys;

(e) maintaining security procedures and security measures;

(f) reporting any breaches of security and/or compromise of EUCI both to their Director and to the Security Directorate;

(g) debriefing staff who cease to be employed by the EEAS;

(h) providing regular reports through their hierarchy on department/division's security matters;

(i) liaising with the EEAS Security Directorate on security issues.

Any activity or issue that might have an impact on security shall be notified to the EEAS Security Directorate in a timely manner.

5. Each Head of Union Delegation shall be responsible for implementing all measures relating to the security of the Union Delegation.

Section 2

The EEAS Security Directorate

1. The EEAS shall have a Security Directorate. It shall:

(a) manage, coordinate, supervise and/or implement all security measures in all premises under the responsibility of the EEAS, at Headquarters, within the EU and in third States;

(b) ensure coherence and consistency with this decision and with implementing provisions of any activity which may have an impact on protecting EEAS security interests;

(c) be the principal adviser of the HR, of the Executive Secretary-General and of the COO on all matters related to security;

(d) be assisted by the competent services of the Member States, in accordance with Article 10(3) of Council Decision 2010/427/EU establishing the organisation and functioning of the EEAS, the Security Directorate

(e) support the activities of the EEAS Security Accreditation Authority by carrying out physical security assessments of the General Security Environment (GSE) / Local Security Environment (LSE) of communication and information systems handling EUCI, and of premises to be authorised for handling and storing EUCI.

2. The Head of the EEAS Security Directorate shall be responsible for:

(a) ensuring the overall protection of the EEAS security interests;

(b) drafting, reviewing and updating of the security rules, as well as co-ordinating security measures with the competent authorities of the Member States and, as appropriate, the competent authorities of third States and international organizations linked to the EU by security agreements and/or arrangements;

(c) supporting the EEAS Security Committee proceedings, as set out in Article 14(1) of this Decision;

(d) liaising with any partners or authorities other than those under (b) above on security matters, where appropriate;

(e) prioritizing and making proposals for the management of the budget for security in Headquarters and in Union Delegations.

3. The Head of the EEAS Security Directorate shall:

(a) ensure that security breaches and compromises are recorded and investigations are launched and undertaken where and when necessary;

(b) meet regularly, and whenever necessary, to discuss 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 Commission.

4. The EEAS Security Directorate shall establish contact and maintain close cooperation with:

— the departments in charge of security in the Ministries of Foreign Affairs of the Member States;

— the National Security Authorities (NSAs) and/or the other competent security authorities of Member States, to elicit their assistance in regard to the information it needs to assess such dangers and threats as may face the EEAS, its staff, its activities, its assets and resources and its classified information at its usual place of business;

— the competent security authorities of the Member States or Host States on the territory of which the EEAS may exercise its activity, regarding any matter relating to the protection of its staff, its activity, its assets and resources, and its classified information while on their territory;

— the Security Office of the General Secretariat of the Council and the Security Directorate of the Directorate General for Human Resources and Security of the Commission, and, where appropriate the security departments of the other EU institutions, bodies and agencies;

— the security departments of third States or international organisations, with a view to any useful co-ordination, and

— the Member States' NSAs, regarding any matter relating to the protection of EUCI.

Section 3

Union Delegations

1. Each Head of Union Delegation shall be responsible for locally implementing and managing all measures relating to the protection of EEAS security interests within the Union Delegation's premises and competence.

In consultation with the competent authorities of the Host State when necessary, he will take all reasonably practicable measures to ensure that appropriate physical and organisational measures are in place to achieve this aim.

The Head of Delegation shall draw up security procedures for the protection of the dependants as defined in Article 2(c), when appropriate, taking into account any administrative arrangement, as referred to in Article 3(3). The Head of Delegation shall report annually on all security related issues within his remit to the Head of the EEAS Security Directorate.

He shall be assisted, in these tasks, by the EEAS Security Directorate, by EEAS staff in the Delegation exercising dedicated security tasks and functions, and by dedicated security staff posted where necessary.

2. In addition, the Head of Delegation will:

— establish detailed Delegation security and contingency plans, on the basis of generic standard operating procedures;

— operate an effective 24/7 system for managing security incidents and emergencies within the Delegation scope of operation;

— ensure that all staff deployed in the Delegation are covered by insurance as required by the conditions in the area;

— ensure that security is part of the Union Delegation induction training to be given to all staff deployed in the Delegation before or upon arriving in the Delegation; and

— ensure that any recommendations made following security assessments are implemented, and provide written reports at regular intervals on their implementation and on other security issues to the EEAS Security Authority.

3. Whilst remaining both responsible and accountable for safeguarding the security management as well as for ensuring corporate resilience, the Head of Delegation may delegate the execution of his or her security tasks to the Delegation Security Coordinator ("DSC"), being the Deputy Head of Delegation or, where none is appointed, an appropriate alternative.

In particular, the following responsibilities could be entrusted to the DSC:

— to liaise on security issues with competent authorities of the host nation and the appropriate counterparts in the Member States' embassies and diplomatic missions.

— to implement appropriate security management procedures related to the EEAS Security interests, including the protection of EUCI;

— to brief staff about the security rules that are applicable to them, and on the particular risks in the host country;

— to submit requests to the EEAS Security Directorate regarding those positions which require a Personnel Security Clearance (PSC), and

— to keep the Head of Delegation, the Regional Security Officer (RSO) and the EEAS Security Directorate continuously informed with regard to incidents or developments in the area which have a bearing on the protection of EEAS security interests,.

4. The Head of Delegation can delegate security tasks of an administrative or technical character to the Head of Administration and other members of the Delegation staff.

5. The Union Delegation shall be assisted by a Regional Security Officer (RSO). The RSOs shall undertake the roles defined below in the Delegations within each of their respective geographical areas of responsibility.

In certain circumstances, where the prevailing security situation dictates, a dedicated RSO may be assigned to a specific delegation as full time resident.

An RSO may be required to relocate to an area outside his present area of responsibility, including the Headquarters in Brussels, or even take up a residential post according to the relevant security situation in any country, and as required by the EEAS Security Directorate.

6. The RSOs shall be under the direct hierarchical control of the EEAS Security Directorate, but under the direct functional and administrative control of the relevant Head of Delegation. They shall assist the Head of Delegation and the Delegation staff in arranging and implementing all physical, organisational and procedural measures related to the security of all Delegation staff regardless of their administrative origin

7. RSOs provide the Head of Delegation and Delegation staff with advice and support. Where appropriate, in particular where a dedicated RSO is a full time resident, he or she can assist a Union Delegation in security management and implementation, including the preparation of security contracts, the management of accreditations and clearances.

Article 13

CSDP Operations and EU Special Representatives

The EEAS Security Directorate assists and advises the Director of the Crisis Management and Planning Directorate (CMPD), the Director General of the EU Military Staff (EUMS), the Civilian Operations Commander heading the Civilian Planning and Conduct Capacity (CPCC), and the EU Military Operations Commanders on security aspects of CSDP operations, and the EU Special Representatives on security aspects of their mandate, complementary to the specific provisions existing in this regard in the relevant policies adopted by the Council.

Article 14

The EEAS Security Committee

1. A EEAS Security Committee is hereby established.

It shall be chaired by the COO or a designated delegate, and shall meet as instructed by the Chair or at the request of any of its members. The EEAS Security Directorate shall support the Chair in this function and provide administrative assistance, as necessary, to the Committee proceedings.

2. The EEAS Security Committee shall be composed of representatives of:

— each Member State;

— the Security Office of the General Secretariat of the Council;

— the Security Directorate of the Directorate General for Human Resources and Security of the Commission.

A Member State delegation to the EEAS Security Committee may consist of members of:

— the National Security Authority and/or the Designated Security Authority,

— the departments in charge of security in the Ministries of Foreign Affairs.

3. The Committee's representatives may be accompanied and advised by experts as they deem necessary. Representatives of other EU Institutions, agencies or bodies may be invited to attend when issues relevant to their security are discussed.

4. Without prejudice to paragraph 5 below, the EEAS Security Committee shall assist the EEAS, by means of consultation, on all security issues relevant to EEAS activities, to Headquarters and Union Delegations.

In particular, without prejudice to paragraph 5 below, the EEAS Security Committee:

(a) shall be consulted on:

— security policies, guidelines, concepts or other methodology documents related to security, in particular as regards the protection of classified information and the measures to be taken in the event of a failure by EEAS staff to comply with the security rules;

— technical security aspects which may influence the HR decision to submit a recommendation to the Council for the opening of negotiations for security of information agreements referred to in Article 10,1(a) of Annex A;

— any amendments to this decision.

(b) may be consulted or informed, as appropriate, on issues relating to the security of staff and assets within EEAS Headquarters and Union Delegations, without prejudice to Article 3(3);

(c) shall be informed of any compromises or losses of EUCI occurred within the EEAS.

5. Any change to the rules relating to the protection of EUCI contained in this decision and its Annex A shall require the unanimous favourable opinion of the Member States as represented in the EEAS Security Committee. Such unanimous favourable opinion shall also be required before:

— entering into negotiations of administrative arrangements as referred to in Article 10(1)(b) of Annex A;

— releasing classified information in the exceptional circumstances referred to in Paragraphs 9, 11 and 12 of Annex A VI

— assuming the information originator's responsibility in the circumstances referred to in Article 10(4), last sentence, of Annex A.

When a unanimous favourable opinion is requested, this condition will be met when no objections are expressed by Member States Delegations during the Committee proceedings.

6. The EEAS Security Committee shall take full account of security policies and guidelines in force in the Council and the Commission.

7. The EEAS Security Committee receives the list of annual EEAS inspections, and the inspection reports, once finalised.

8. Organisation of the meetings:

— The EEAS Security Committee shall meet at least twice a year. Additional meetings, either in its fully fledged configuration or in NSA/DSA or in MFA security format, can be arranged by the Chair or requested by the members of the Committee.

— The EEAS Security Committee shall organise its activities in such a way that it can make recommendations on specific areas of security. It may establish other expert sub-areas as necessary. It shall draw up terms of reference for such expert sub-areas and receive reports from them on their activities.

— The EEAS Security Directorate shall be responsible for preparing items for discussion. The Chair shall draw up the provisional agenda for each meeting. The members of the Committee may propose additional items for discussion.

Article 15

Security inspections

1. The EEAS security authority shall ensure that security inspections are undertaken, on a regular basis, within the EEAS Headquarters and within Union Delegations in order to assess the adequacy of security measures and to verify their compliance with this Decision. The EEAS Security Directorate may, where appropriate, designate contributing experts to participate in security inspections to EU agencies and bodies established under title V, Chapter 2 of the TEU.

2. EEAS Security Inspections are conducted under the authority of the EEAS Security Directorate and, when appropriate, with the support of security experts representing other EU Institutions or Member States., in particular in the context of the arrangements referred to in Article 3(3).

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

Where necessary, relevant security experts based in Member State Missions in the third States and/or representatives of the diplomatic security departments of the Member States may be invited to participate in the security inspection of the Union Delegation.

4. Provisions for implementing this Article as regards the protection of EUCI are set out in Annex A III.

Article 16

Assessment visits

Assessment visits shall be arranged to ascertain the effectiveness of the security measures in place in a third State or international organisation for protecting EUCI exchanged under an administrative arrangement as referred to in Article 10(1)(b) of Annex A.

The EEAS Security Directorate may designate contributing experts to participate in assessment visits to third States or international organisations with which the EU has concluded a security of information Agreement as referred to in Article 10(1)(a) of Annex A,

Article 17

Business continuity planning

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

Article 18

Travel advice for missions outside the EU

The EEAS Security Directorate shall ensure the availability of travel advice regarding missions of Staff placed under the responsibility of the EEAS outside the EU, drawing upon the resources of all relevant services of the EEAS - in particular the SITROOM, the INTCEN, the geographical departments and the Union Delegations.

The EEAS Security Directorate provides, on request, and drawing upon aforementioned resources, specific travel advice regarding missions by Staff placed under the responsibility of the EEAS to third States presenting a high risk or an increased risk level.

Article 19

Health and Safety

The EEAS security rules complement the EEAS rules for the protection of health and safety, as adopted by the High Representative.

Article 20

Implementation and review

1. The EEAS security authority shall, after consultation with the EEAS Security Committee as appropriate, approve security policies or guidelines setting out any measures necessary to implement these rules in the EEAS, and shall build up the necessary capacity covering all aspects of security, in close cooperation with the Member States' competent security authorities and with the support of the relevant services of the EU Institutions.

2. In accordance with article 4(5) of Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the European External Action Service, transitional arrangements may be used, as necessary, through service-level agreements with the relevant services of the General Secretariat of the Council and of the Commission.

3. The HR shall ensure overall consistency in the application of this Decision, and shall keep these security rules under review.

4. The EEAS security rules are to be implemented in close cooperation with the Member States' competent security authorities, with the Security Office of the General Secretariat of the Council and with the Security Directorate of the Directorate General for Human Resources and Security of the Commission

5. EEAS shall ensure that all aspects of the security process are taken into account within the EEAS crisis response system.

6. The COO, as Security Authority, and the head of the EEAS Security Directorate shall ensure the implementation of this decision.

Article 21

Replacement of previous decisions

1. This decision shall repeal and replace the 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 [1].

2. This decision shall repeal the Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 23 February 2011 on the Designation and tasks of the Delegated Security Authority of the European External Action Service.

Article 22

Final provisions

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

It shall be published in the *Official Journal of the European Union*.

The competent authorities in the EEAS shall duly and timely inform all staff falling within the scope of this decision and its annexes, on the content, entry into force and any subsequent modifications thereof.

Done at Brussels, 19 April 2013.

The High Representative

C. ASHTON

[1] OJ C 304, 15.10.2011, p. 5

ANNEX A

PRINCIPLES AND STANDARDS FOR PROTECTING EUCI

Article 1

Purpose, scope and definitions

1. This Annex sets out the basic principles and minimum standards of security for protecting EUCI.

2. These basic principles and minimum standards shall apply to the EEAS and to Staff placed under the responsibility of the EEAS as referred to and defined respectively in Articles 1 and 2 of this Decision.

Article 2

Definition of EUCI, security classifications and markings

1. "EU classified information" (EUCI) means any information or material the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States, designated by an EU security classification.

2. EUCI shall be classified at one of the following levels:

(a) TRES SECRET UE/EU TOP SECRET: information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States.

(b) SECRET UE/EU SECRET: information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States.

(c) CONFIDENTIEL UE/EU CONFIDENTIAL: information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States.

(d) RESTREINT UE/EU RESTRICTED: information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

3. EUCI shall bear a security classification marking in accordance with paragraph 2. It may bear additional markings to designate the field of activity to which it relates, identify the originator, limit distribution, restrict use or indicate releasability.

Article 3

Classification management

1. The EEAS shall ensure that EUCI is appropriately classified, clearly identified as classified information and retains its classification level for only as long as necessary.

2. EUCI shall not be downgraded or declassified nor shall any of the markings referred to in Article 2(3) be modified or removed without the prior written consent of the originator.

3. The EEAS security authority shall approve, after consulting the EEAS Security Committee pursuant to article 14(5) of this Decision, a security policy on creating EUCI which shall include a practical classification guide.

Article 4

Protection of classified information

1. EUCI shall be protected in accordance with this Decision.

2. The holder of any item of EUCI shall be responsible for protecting it in accordance with this Decision.

3. 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 table of equivalence of security classifications contained in Appendix B to Council Decision 2011/292/EU of 31 March 2011 on the security rules for protecting EU classified information.

The EEAS shall establish appropriate procedures to maintain accurate records as to the originator of the

— classified information EEAS receives; and

— source material included in classified information originated by the EEAS.

The EEAS Security Committee shall be informed of these procedures.

4. Large quantities or a compilation of EUCI may warrant a level of protection corresponding to a higher classification than that of its components.

Article 5

Personnel security for handling EU classified information

1. Personnel security is the application of measures to ensure that access to EUCI is granted only to individuals who have:

— a need-to-know;

— for access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, been security cleared to the relevant level, or are otherwise duly authorised by virtue of their functions in accordance with national laws and regulations; and

— been briefed on their responsibilities.

2. Personnel Security Clearance (PSC) procedures shall determine whether an individual, taking into account his loyalty, trustworthiness and reliability, may be authorised to access EUCI.

3. All individuals shall be briefed on and acknowledge in writing their responsibilities to protect EUCI in accordance with this Decision before being granted access to EUCI, and at regular intervals thereafter.

4. Provisions for implementing this Article are set out in Annex A I.

Article 6

Physical security of EU classified information

1. Physical security is the application of physical and technical protective measures to deter unauthorised access to EUCI.

2. Physical security measures shall be designed to deny surreptitious or forced entry by an intruder, to deter, impede and detect unauthorised actions and to allow for differentiation in personnel in their access to EUCI on a need-to-know basis. Such measures shall be determined based on a risk management process.

3. Physical security measures shall be put in place for all premises, buildings, offices, rooms and other areas in which EUCI is handled or stored, including areas housing communication and information systems as defined in Article 8(2).

4. Areas in which EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is stored shall be established as Secured Areas in accordance with Annex A II and approved by the EEAS security authority.

5. Only approved equipment or devices shall be used for protecting EUCI at the level CONFIDENTIEL UE/EU CONFIDENTIAL or above.

6. Provisions for implementing this Article are set out in Annex A II.

Article 7

Management of classified information

1. The management of classified information is the application of administrative measures for controlling EUCI throughout its life-cycle to supplement the measures provided for in Articles 5, 6 and 8 and thereby help deter, detect and recover from deliberate or accidental compromise or loss of such information. Such measures relate in particular to the creation, registration, copying, translation, carriage, handling, storage and destruction of EUCI.

2. Information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be registered for security purposes prior to distribution and on receipt. The competent authorities in the EEAS shall establish a registry system for this purpose. Information classified TRES SECRET UE/EU TOP SECRET shall be registered in designated registries.

3. Services and premises where EUCI is handled or stored shall be subject to regular inspection by the EEAS security authority.

4. EUCI shall be conveyed between services and premises outside physically protected areas as follows:

(a) as a general rule, EUCI shall be transmitted by electronic means protected by cryptographic products approved in accordance with Article 7(5) of this Decision and according to clearly defined Security Operational Procedures (SecOPs);

(b) when the means referred to in point (a) are not used, EUCI shall be carried either:

(i) on electronic media (e.g. USB sticks, CDs, hard drives) protected by cryptographic products approved in accordance with Article 7(5) of this Decision; or

(ii) in all other cases, as prescribed by the EEAS security authority in accordance with the relevant protective measures laid down in Annex A III, Section V.

5. Provisions for implementing this Article are set out in Annex A III.

Article 8

Protection of EUCI handled in communication and information systems

1. Information Assurance (IA) in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Effective IA shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. IA shall be based on a risk management process.

2. "Communication and Information System" (CIS) means any system enabling the handling of information in electronic form. A communication and information system shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources. This Annex shall apply to any EEAS CIS handling EUCI.

3. CIS shall handle EUCI in accordance with the concept of IA.

4. All CIS handling EUCI shall undergo an accreditation process. Accreditation shall aim at obtaining assurance that all appropriate security measures have been implemented and that a sufficient level of protection of the EUCI and of the CIS has been achieved in accordance with this Decision. The accreditation statement shall determine the maximum classification level of the information that may be handled in a CIS as well as the corresponding terms and conditions.

5. CIS handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be protected in such a way that the information cannot be compromised by unintentional electromagnetic emanations ("TEMPEST security measures").

6. Where the protection of EUCI is provided by cryptographic products, such products shall be approved in accordance with Article 7(5) of this Decision.

7. During transmission of EUCI by electronic means, approved cryptographic products shall be used. Notwithstanding this requirement, specific procedures may be applied under emergency circumstances or specific technical configurations as specified in Annex A IV.

8. Pursuant to Article 7(6) of this Decision, the following IA functions will be established to the extent necessary:

(a) an IA Authority (IAA);

(b) a TEMPEST Authority (TA);

(c) a Crypto Approval Authority (CAA);

(d) a Crypto Distribution Authority (CDA).

9. Pursuant to Article 7(7) of this Decision, for each system shall be established:

(a) a Security Accreditation Authority (SAA);

(b) an IA Operational Authority.

10. Provisions for implementing this Article are set out in Annex A IV.

Article 9

Industrial security

1. Industrial security is the application of measures to ensure the protection of EUCI by contractors or subcontractors in pre-contract negotiations and throughout the life-cycle of classified contracts. As a general rule, such contracts shall not involve access to information classified TRES SECRET UE/EU TOP SECRET.

2. The EEAS may entrust by contract tasks involving or entailing access to or the handling or storage of EUCI by industrial or other entities registered in a Member State, or in a third State with which a security of information agreement or an administrative arrangement referred to in Article 10(1) of Annex A has been concluded.

3. The EEAS, as contracting authority, shall ensure that the minimum standards on industrial security set out in this Decision, and referred to in the contract, are complied with when awarding classified contracts to industrial or other entities. It shall ensure compliance with such minimum standards through the relevant NSA/DSA.

4. Contractors or subcontractors registered in a Member State and participating in classified contracts or sub-contracts which require to handle and store information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within their facilities, either in the performance of such contracts or during the pre-contractual stage, shall hold a Facility Security Clearance (FSC) at the relevant classification level, granted by the NSA, DSA or any other competent security authority of the said Member State.

5. Contractor or subcontractor personnel who, for the performance of a classified contract, require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall hold a PSC granted by the respective National Security Authority (NSA), Designated Security Authority (DSA) or any other competent security authority in accordance with national laws and regulations and the minimum standards laid down in Annex A I.

6. Provisions for implementing this Article are set out in Annex A V.

Article 10

Exchange of classified information with third States and International Organisations

1. The EEAS can only exchange EUCI with a third State or international organisation where:

(a) a security of information agreement between the EU and that third State or international organisation, concluded in accordance with Article 37 TEU and Article 218 TFEU, is in force; or

(b) an administrative arrangement between the HR and the competent security authorities of that third State or international organisation, for the exchange of information classified, in principle, no higher than RESTREINT UE/EU RESTRICTED, concluded in accordance with the procedure set out in Article 14(5) of this Decision, has taken effect; or

(c) a framework or ad-hoc participation agreement between the EU and that third State in the context of a CSDP crisis management operation, concluded in accordance with Article 37 TEU and Article 218 TFEU, is applicable,

and the conditions set out in that instrument have been met.

Exceptions to the general rule above are set out in Annex A VI, Section V.

2. Administrative arrangements referred to in paragraph 1(b) shall contain provisions to ensure that when third States or international organisations receive EUCI, such information is given protection appropriate to its classification level and according to minimum standards which are no less stringent than those laid down in this Decision.

Information exchanged on the basis of agreements referred to in paragraph 1(c) shall be limited to information concerning CSDP operations in which the third state in question participates on the basis of these agreements and in accordance with their provisions.

3. Assessment visits to third States or international organisations, as referred to in Article 16 of this Decision shall be arranged to ascertain the effectiveness of the security measures in for protecting any EUCI exchanged.

4. The decision to release EUCI held by the EEAS to a third State or international organisation shall be taken on a case-by-case basis, according to the nature and content of such information, the recipient's need-to-know and the measure of advantage to the EU.

The EEAS shall seek the written consent of any entity which has provided classified information as source material for EUCI which the EEAS has originated, to establish that there are no objections to release.

If the originator of the classified information for which release is desired is not the EEAS, the EEAS shall first seek the originator's written consent to release.

If, however, the EEAS cannot establish the originator, the EEAS security authority shall assume the originator's responsibility after having obtained the unanimous favourable opinion of the Member States as represented in the EEAS Security Committee.

5. Provisions for implementing this Article are set out in Annex A VI.

Article 11

Breaches of security and compromise of classified information

1. Any breach or suspected breach of security, and any compromise or suspected compromise of classified information shall be reported immediately to the EEAS Security Directorate, which shall inform, as appropriate, the Security Directorate of the Directorate General for Human Resources and Security of the Commission, and the Security Office of the General Secretariat of the Council, the Member State(s) concerned, or other entity concerned.

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 Commission, the Security Office of the General Secretariat of the Council or the NSA of the Member State(s) concerned, or other entity concerned, as appropriate, and shall take all appropriate measures in accordance with the relevant laws and regulations to:

(a) assess the potential damage caused to the interests of the EU or of the Member States;

(b) take appropriate measures to prevent a recurrence;

(c) safeguard evidence;

(d) ensure that the case is investigated by personnel not immediately concerned with the breach in order to establish the facts;

(e) notify the appropriate authorities of the effects of the event and of the action taken; and

(f) inform the originator.

3. Any member of staff under the responsibility of the EEAS 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 the compromise or loss of classified information shall be liable to disciplinary and/or legal action in accordance with the applicable laws, rules and regulations.

The Security Directorate of the Directorate General for Human Resources and Security of the Commission, the Security Office of the General Secretariat of the Council or the NSA of the Member State(s) concerned, or other entity concerned shall be immediately informed, as appropriate.

4. Whilst an investigation into the breach and/or compromise is ongoing, the Head of the EEAS Security Directorate may suspend the individual's access to EUCI and to EEAS premises. The Security Directorate of the Directorate General for Human Resources and Security of the Commission, the Security Office of the General Secretariat of the Council or the NSA of the Member State(s) or other entity concerned shall be immediately informed of this decision.

ANNEX A I

PERSONNEL SECURITY

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 5 of Annex A. It lays down in particular the criteria that the EEAS shall apply for determining whether an individual, taking into account his loyalty, trustworthiness and reliability, may be authorised to have access to EUCI, and the investigative and administrative procedures to be followed to that effect.

2. The "Personnel Security Clearance" (PSC) for access to EUCI is a statement by a competent authority of a Member State which is made following completion of a security investigation conducted by the competent authorities of a Member State and which certifies that an individual may, provided his "need-to-know" has been determined, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date; the individual thus described is said to be "security cleared".

3. The "Personnel Security Clearance Certificate" (PSCC) is a certificate issued by the EEAS Security authority establishing that an individual is security cleared, and which shows the level of EUCI to which that individual may be granted access, the date of validity of the relevant PSC and the date of the expiry of the certificate itself.

4. The "Authorisation to access EUCI" is an authorisation by the EEAS Security Authority which is taken in accordance with this Decision after a PSC has been issued by the competent authorities of a Member State, and which certifies that an individual may, provided his "need-to-know" has been determined, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date; the individual thus described is said to be "security cleared".

II. AUTHORISING ACCESS TO EUCI

5. Access to information classified RESTREINT UE/EU RESTRICTED does not require a security clearance and is granted after:

   (a) the individual's statutory or contractual link to the EEAS has been established,

   (b) the individual's need-to-know has been determined,

   (c) he has been briefed on the security rules and procedures for protecting EUCI and has acknowledged in writing his responsibilities to protect EUCI in accordance with this Decision.

6. An individual shall only be authorised to access information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above after:

   (a) his need-to-know has been determined;

   (b) he has been granted a PSC to the relevant level or is otherwise duly authorised by virtue of his functions in accordance with national laws and regulations; and

   (c) he has been briefed on the security rules and procedures for protecting EUCI and has acknowledged in writing his responsibilities with regard to protecting such information.

7. EEAS shall identify the positions in its structures which require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above and therefore require a PSC to the relevant level, as referred to in Article 4 above.

8. EEAS Staff shall declare whether they hold the citizenship of more than one country.

PSC request procedures in the EEAS

9. For EEAS Staff, the appointing EEAS Authority shall forward the completed personnel security questionnaire to the NSA of the Member State of which the individual is a national requesting that a security investigation be undertaken for the level of EUCI to which the individual will require access.

10. Where an individual holds citizenship of more than one country, the vetting request will be addressed to the NSA of the country under whose nationality the person has been recruited.

11. Where information relevant for a security investigation becomes known to the EEAS concerning an individual who has applied for a PSC, the EEAS, acting in accordance with the relevant rules and regulations, shall notify the relevant NSA thereof.

12. Following completion of the security investigation, the relevant NSA shall notify the EEAS Security Directorate of the outcome of such an investigation.

(a) Where the security investigation results in an assurance that nothing adverse is known which would call into question the loyalty, trustworthiness and reliability of the individual, the EEAS Security Authority may grant the individual concerned an Authorisation to access EUCI up to the relevant level until a specified date;

(b) EEAS shall take all appropriate measures to ensure that conditions or restrictions imposed by the NSA are duly implemented. The NSA will be informed about the outcome.

(c) Where the security investigation does not result in such an assurance, the EEAS Security Authority shall notify the individual concerned, who may ask to be heard by the EEAS Security Authority. The EEAS Security Authority may ask the competent NSA for any further clarification it can provide according to its national laws and regulations. If the outcome is confirmed, an Authorisation to access EUCI shall not be granted. In that case EEAS shall take all appropriate measure to ensure that the applicant will be denied any access to EUCI.

13. The security investigation together with the results obtained, on which the EEAS bases its decision on whether or not to grant an authorisation to access EUCI, shall be subject to the relevant laws and regulations in force in the Member State concerned, including those concerning appeals. Decisions by the EEAS Security Authority shall be subject to appeals in accordance with the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the European Union, laid down in Regulation (EEC, Euratom, ECSC) No 259/68 [1] (hereinafter referred to as "the Staff Regulations").

14. The assurance on which a PSC is based, provided it remains valid, shall cover any assignment by the individual concerned within the EEAS, the General Secretariat of the Council or the Commission.

15. If an individual's period of service does not commence within 12 months of the notification of the outcome of the security investigation to the EEAS Security Authority, or if there is a break of 12 months or more in an individual's service, during which time he has not been employed in the EEAS, in other EU Institutions, agencies or bodies, or in a position with a national administration of a Member State, which requires access to classified information, this outcome shall be referred to the relevant NSA for confirmation that it remains valid and appropriate.

16. Where information becomes known to the EEAS concerning a security risk posed by an individual who holds a valid PSC, the EEAS, acting in accordance with the relevant rules and regulations, shall notify the relevant NSA thereof. Where an NSA notifies the EEAS of withdrawal of an assurance given in accordance with paragraph 12(a) for an individual who holds a valid Authorisation to access EUCI, the EEAS Security Authority may ask for any clarification the NSA can provide according to its national laws and regulations. If the adverse information is confirmed, the aforementioned Authorisation shall be withdrawn and the individual shall be excluded from access to EUCI and from positions where such access is possible or where he might endanger security.

17. Any decision to withdraw an Authorisation to access EUCI from an EEAS staff member and, where appropriate, the reasons for doing so shall be notified to the individual concerned, who may ask to be heard by the EEAS Security Authority. Information provided by an NSA shall be subject to the relevant laws and regulations in force in the Member State concerned, including those concerning appeals. Decisions by the EEAS Security Authority shall be subject to appeals in accordance with the Staff Regulations.

18. National experts seconded to the EEAS for a position requiring access to classified information CONFIDENTIEL UE/EU CONFIDENTIAL or above shall present a valid PSC for access to EUCI to the relevant level to the EEAS Security Authority prior to taking up their assignment. The above process shall be managed by the sending Member State.

Records of PSCs

19. A database on the security clearance status of all staff placed under the responsibility of the EEAS and of EEAS contractors' personnel shall be maintained by the EEAS. These records shall include the level of EUCI to which the individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date the PSC was granted and its period of validity.

20. Appropriate coordination procedures shall be put in place with Member States and other EU Institutions, agencies and bodies to ensure that the EEAS holds an accurate and comprehensive record of security clearance status of all Staff placed under the responsibility of the EEAS and of EEAS contractors' personnel.

[1] OJ L 56, 4.3.1968, p. 1.

21. The EEAS Security Authority may issue a Personnel Security Clearance Certificate (PSCC) showing the level of EUCI to which the individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date of validity of the relevant PSC and the date of expiry of the certificate itself.

Exemptions from the PSC requirement

22. Individuals duly authorised to access EUCI by virtue of their functions in accordance with national laws and regulations shall be briefed, as appropriate, by the EEAS Security Directorate on their security obligations in respect of protecting EUCI.

III. SECURITY EDUCATION AND AWARENESS

23. Prior to being authorised to access EUCI, all individuals shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the EEAS.

24. All individuals who are authorised to have access to, or required to handle EUCI, shall initially be made aware of, and periodically briefed on the threats to security and must report immediately to the appropriate security authorities any approach or activity that they consider suspicious or unusual.

25. All individuals granted access to EUCI must be subject to ongoing personnel security measures (i.e. aftercare) for the duration that they handle EUCI. Ongoing personnel security is the responsibility of:

a) Individuals granted access to EUCI: Individuals are personally responsible for their own security conduct and must report immediately to the appropriate security authorities any approach or activity that they consider suspicious or unusual, and any changes in their personal circumstances that may have an impact on their PSC or Authorization to access EUCI.

b) Line managers: They are responsible for ensuring that their staff are aware of the security measures and responsibilities to protect EUCI, for monitoring the security conduct of their staff and for either addressing any security matters of concern themselves, or reporting to the appropriate security authorities any adverse information that may have an impact on their staff's PSC or Authorization to access EUCI.

c) Security actors of the EEAS security organisation as referred to in Article 12 of this decision: They are responsible for providing security awareness briefings to ensure staff in their area are periodically briefed, for fostering a strong security culture in their area of responsibility, for putting in place measures to monitor the security conduct of staff, and for reporting to the appropriate security authorities any adverse information that may have an impact on any individual's PSC.

d) EEAS and Member States: shall put in place the necessary channels to communicate information that may have an impact on any individual's PSC or Authorization to access EUCI.

26. All individuals who cease to be employed on duties requiring access to EUCI shall be made aware of, and where appropriate acknowledge in writing, their obligations in respect of the continued protection of EUCI.

IV. EXCEPTIONAL CIRCUMSTANCES

27. For reasons of urgency, where duly justified in the interests of the EEAS and pending completion of a full security investigation, the EEAS Security Authority may, after consulting the NSA of the Member State of which the individual is a national and subject to the outcome of preliminary checks to verify that no adverse information is known, grant a temporary authorisation for EEAS officials and other servants to access EUCI for a specific function. A full security investigation should be completed as soon as possible. Such temporary authorisations shall be valid for a period not exceeding six months and shall not permit access to information classified TRES SECRET UE/EU TOP SECRET. All individuals who have been granted a temporary authorisation shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the EEAS.

28. When an individual is to be assigned to a position that requires a PSC at one level higher than that currently possessed by the individual, the assignment may be made on a provisional basis, provided that:

(a) the compelling need for access to EUCI at a higher level shall be justified, in writing, by the individual's superior;

(b) access shall be limited to specific items of EUCI in support of the assignment;

(c) the individual holds a valid PSC;

(d) action has been initiated to obtain authorisation for the level of access required for the position;

(e) satisfactory checks have been made by the competent authority that the individual has not seriously or repeatedly infringed security regulations;

(f) the assignment of the individual is approved by the competent EEAS authority; and

(g) the relevant NSA/DSA which issued the individual's PSC has been consulted and no objection has been received;

(h) a record of the exception, including a description of the information to which access was approved, is kept by the registry or subordinate registry responsible

29. The above procedure shall be used for one-time access to EUCI at one level higher than that to which the individual has been security cleared. Recourse to this procedure shall not be made on a recurring basis.

30. In very exceptional circumstances, such as missions in hostile environments or during periods of mounting international tension when emergency measures require it, in particular for the purposes of saving lives, HR, Executive Secretary General or Chief Operating Officer may grant, where possible in writing, access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET to individuals who do not possess the requisite PSC, provided that such permission is absolutely necessary and there are no reasonable doubts as to the loyalty, trustworthiness and reliability of the individual concerned. A record shall be kept of this permission describing the information to which access was approved.

31. In the case of information classified TRES SECRET UE/EU TOP SECRET, this emergency access shall be confined to EU nationals who have been authorised access to either the national equivalent of TRES SECRET UE/EU TOP SECRET or information classified SECRET UE/EU SECRET.

32. The EEAS Security Committee shall be informed of cases when recourse is made to the procedure set out in paragraphs 29 and 30.

33. The EEAS Security Committee shall receive an annual report on recourse to the procedures set out in this section.

V. ATTENDANCE AT MEETINGS IN THE EEAS HEADQUARTERS AND UNION DELEGATIONS.

34. Individuals assigned to participate in meetings in the EEAS Headquarters and Union Delegations at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed may only do so upon confirmation of the individual's PSC status. For Member States' representatives, officials from the GSC and Commission, a PSCC or other proof of PSC shall be forwarded by the appropriate authorities to the EEAS Security Directorate, the Union Delegation Security Coordinator, or exceptionally be presented by the person concerned. Where applicable, a consolidated list of names may be used, giving the relevant proof of PSC.

35. Where a PSC for access to EUCI is withdrawn from an individual whose duties require attendance at meetings in the EEAS Headquarters or Union Delegation at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed, the EEAS shall be informed by the competent authority thereof.

VI. POTENTIAL ACCESS TO EUCI

36. When individuals are to be employed in circumstances in which they may potentially have access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, they shall be appropriately security cleared or escorted at all times.

37. Couriers, guards and escorts shall be security cleared to the relevant level or otherwise appropriately investigated in accordance with national laws and regulations, be briefed at regular intervals on security procedures for protecting EUCI and on their duties for protecting such information entrusted to them or to which they may inadvertently have access.

ANNEX A II

PHYSICAL SECURITY OF EU CLASSIFIED INFORMATION

I. **INTRODUCTION**

1. This Annex sets out provisions for implementing Article 6 of Annex A. It lays down minimum requirements for the physical protection of premises, buildings, offices, rooms and other areas where EUCI is handled and stored, including areas housing CIS.

2. Physical security measures shall be designed to prevent unauthorised access to EUCI by:

(a) ensuring that EUCI is handled and stored in an appropriate manner;

(b) allowing for segregation of personnel in terms of access to EUCI on the basis of their need-to-know and, where appropriate, their security clearance;

(c) deterring, impeding and detecting unauthorised actions; and

(d) denying or delaying surreptitious or forced entry by intruders.

II. **PHYSICAL SECURITY REQUIREMENTS AND MEASURES**

3. The EEAS shall apply a risk management process for protecting EUCI on their premises to ensure that a commensurate level of physical protection is afforded against the assessed risk. The risk management process shall take account of all relevant factors, in particular:

(a) the classification level of EUCI;

(b) the form and volume of EUCI, bearing in mind that large quantities or a compilation of EUCI may require more stringent protective measures to be applied;

(c) the surrounding environment and structure of the buildings or areas housing EUCI;

(d) the third country threat assessment as developed by INTCEN on the basis in particular of Union Delegation reports, and

(e) the assessed threat from intelligence services which target the EU or Member States and from sabotage, terrorist, subversive or other criminal activities.

4. The EEAS security authority, applying the concept of defence in depth, shall determine the appropriate combination of physical security measures to be implemented. These can include one or more of the following:

(a) a perimeter barrier: a physical barrier which defends the boundary of an area requiring protection;

(b) intrusion detection systems (IDS): an IDS may be used to enhance the level of security offered by a perimeter barrier, or in rooms and buildings in place of, or to assist, security staff;

(c) access control: access control may be exercised over a site, a building or buildings on a site or to areas or rooms within a building. Control may be exercised by electronic or electro-mechanical means, by security personnel and/or a receptionist, or by any other physical means;

(d) security personnel: trained, supervised and, where necessary, appropriately security cleared security personnel may be employed, *inter alia*, in order to deter individuals planning covert intrusion;

(e) closed circuit television (CCTV): CCTV may be used by security personnel in order to verify incidents and IDS alarms on large sites or at perimeters;

(f) security lighting: security lighting may be used to deter a potential intruder, as well as to provide the illumination necessary for effective surveillance directly by security personnel or indirectly through a CCTV system; and

(g) any other appropriate physical measures designed to deter or detect unauthorised access or prevent loss of or damage to EUCI.

5. The EEAS Security Directorate may conduct entry and exit searches to act as a deterrent to the unauthorised introduction of material or the unauthorised removal of EUCI from premises or buildings.

6. When EUCI is at risk from overlooking, even accidentally, appropriate measures shall be taken to counter this risk.

7. For new facilities, physical security requirements and their functional specifications shall be defined as part of the planning and design of the facilities. For existing facilities, physical security requirements shall be implemented to the maximum extent possible.

III. **EQUIPMENT FOR THE PHYSICAL PROTECTION OF EUCI**

8. When acquiring equipment (such as security containers, shredding machines, door locks, electronic access control systems, IDS, alarm systems) for the physical protection of EUCI, the EEAS security authority shall ensure that the equipment meets approved technical standards and minimum requirements.

9. The technical specifications of equipment to be used for the physical protection of EUCI shall be set out in security guidelines to be approved by the EEAS Security Committee.

10. Security systems shall be inspected at regular intervals and equipment shall be maintained regularly. Maintenance work shall take account of the outcome of inspections to ensure that equipment continues to operate at optimum performance.

11. The effectiveness of individual security measures and of the overall security system shall be re-evaluated during each inspection.

IV. **PHYSICALLY PROTECTED AREAS**

12. Two types of physically protected areas, or the national equivalents thereof, shall be established for the physical protection of EUCI:

(a) Administrative Areas and

(b) Secured Areas (including technically Secured Areas).

13. The EEAS security authority shall establish that an area meets the requirements to be designated as an Administrative Area, a Secured Area or a technically Secured Area.

14. For Administrative Areas:

(a) a visibly defined perimeter shall be established which allows individuals and, where possible, vehicles to be checked;

(b) unescorted access shall be granted only to individuals who are duly authorised by the EEAS Security Directorate; and

(c) all other individuals shall be escorted at all times or be subject to equivalent controls.

15. For Secured Areas:

(a) a visibly defined and protected perimeter shall be established through which all entry and exit are controlled by means of a pass or personal recognition system;

(b) unescorted access shall be granted only to individuals who are security-cleared to the appropriate level and specifically authorised to enter the area on the basis of their need-to-know;

(c) all other individuals shall be escorted at all times or be subject to equivalent controls.

16. Where entry into a Secured Area constitutes, for all practical purposes, direct access to the classified information contained in it, the following additional requirements shall apply:

(a) the level of highest security classification of the information normally held in the area shall be clearly indicated;

(b) all visitors shall require specific authorisation to enter the area, shall be escorted at all times and shall be appropriately security cleared unless steps are taken to ensure that no access to EUCI is possible;

(c) electronic devices shall be left outside the area.

17. Secured Areas protected against eavesdropping shall be designated technically Secured Areas. The following additional requirements shall apply:

(a) such areas shall be IDS equipped, be locked when not occupied and be guarded when occupied. Any keys shall be controlled in accordance with Section VI of this Annex;

(b) all persons and material entering such areas shall be controlled;

(c) such areas shall be regularly physically and/or technically inspected as required by the EEAS security authority. Such inspections shall also be conducted following any unauthorised entry or suspicion of such an entry; and

(d) such areas shall be free of unauthorised communication lines, unauthorised telephones or other unauthorised communication devices and electrical or electronic equipment;

18. Notwithstanding point (d) of paragraph 17, before being used in areas where meetings are held or work is being performed involving information classified SECRET UE/EU SECRET and above, and where the threat to EUCI is assessed as high, any communications devices and electrical or electronic equipment shall first be examined by the EEAS security authority to ensure that no intelligible information can be inadvertently or illicitly transmitted by such equipment beyond the perimeter of the Secured Area.

19. Secured Areas which are not occupied by duty personnel on a 24-hour basis shall, where appropriate, be inspected at the end of normal working hours and at random intervals outside normal working hours, unless an IDS is in place.

20. Secured Areas and technically Secured Areas may be set up temporarily within an Administrative Area for a classified meeting or any other similar purpose.

21. Security operating procedures shall be drawn up for each Secured Area stipulating:

(a) the level of EUCI which may be handled and stored in the area;

(b) the surveillance and protective measures to be maintained;

(c) the individuals authorised to have unescorted access to the area by virtue of their need-to-know and security clearance;

(d) where appropriate, the procedures for escorts or for protecting EUCI when authorising any other individuals to access the area;

(e) any other relevant measures and procedures.

22. Strong rooms shall be constructed within Secured Areas. The walls, floors, ceilings, windows and lockable doors shall be approved by the EEAS security authority and afford protection equivalent to a security container approved for the storage of EUCI of the same classification level.

V. PHYSICAL PROTECTIVE MEASURES FOR HANDLING AND STORING EUCI

23. EUCI which is classified RESTREINT UE/EU RESTRICTED may be handled:

(a) in a Secured Area,

(b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals, or

(c) outside a Secured Area or an Administrative Area provided the holder carries the EUCI in accordance with paragraphs 30 to 42 of Annex A III and has undertaken to comply with compensatory measures laid down in security instructions issued by the EEAS security authority to ensure that EUCI is protected from access by unauthorised persons.

24. EUCI which is classified RESTREINT UE/EU RESTRICTED shall be stored in suitable locked office furniture in an Administrative Area or a Secured Area. It may temporarily be stored outside a Secured Area or an Administrative Area provided the holder has undertaken to comply with compensatory measures laid down in security instructions issued by the EEAS security authority.

25. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET may be handled:

(a) in a Secured Area;

(b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals; or

(c) outside a Secured Area or an Administrative Area provided the holder:

(i) carries the EUCI in accordance with paragraphs 30 to 42 of Annex A III;

(ii) has undertaken to comply with compensatory measures laid down in security instructions issued by the EEAS security authority to ensure that EUCI is protected from access by unauthorised persons;

(iii) keeps the EUCI at all times under his personal control; and

(iv) in the case of documents in paper form, has notified the relevant registry of the fact.

26. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET shall be stored within a Secured Area, in a security container or strong room.

27. EUCI which is classified TRES SECRET UE/EU TOP SECRET shall be handled in a Secured Area.

28. EUCI which is classified TRES SECRET UE/EU TOP SECRET shall be stored in a Secured Area at the Headquarters under one of the following conditions:

(a) in a security container that is in accordance with paragraph 8 with one or more of the following supplementary controls:

(i) continuous protection or verification by cleared security staff or duty personnel;

(ii) an approved IDS in combination with security response personnel;

or

(b) in an IDS-equipped strong room in combination with security response personnel.

29. Rules governing the carriage of EUCI outside physically protected areas are set out in Annex A III.

VI. **CONTROL OF KEYS AND COMBINATIONS USED FOR PROTECTING EUCI**

30. The EEAS security authority shall define procedures for managing keys and combination settings for offices, rooms, strong rooms and security containers. Such procedures shall protect against unauthorised access.

31. Combination settings shall be committed to memory by the smallest possible number of individuals needing to know them. Combination settings for security containers and strong rooms storing EUCI shall be changed:

(a) on receipt of a new container;

(b) whenever there is a change in personnel knowing the combination;

(c) whenever a compromise has occurred or is suspected;

(d) when a lock has undergone maintenance or repair; and

(e) at least every 12 months.

ANNEX A III

MANAGEMENT OF CLASSIFIED INFORMATION

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 7 of Annex A. It lays down the administrative measures for controlling EUCI throughout its life-cycle in order to help deter, detect and recover from deliberate or accidental compromise or loss of such information.

II. CLASSIFICATION MANAGEMENT

Classifications and markings

2. Information shall be classified where it requires protection with regard to its confidentiality.

3. The originator of EUCI shall be responsible for determining the security classification level, in accordance with the relevant classification guidelines, and for the dissemination of the information.

4. The classification level of EUCI shall be determined in accordance with Article 2(2) of Annex A and by reference to the security policy to be approved in accordance with Article 3(3) of Annex A.

5. Classified information of the Member States exchanged with the EEAS shall be awarded the same level of protection as EUCI bearing the equivalent classification. A table of equivalence can be found in Appendix B to Council Decision 2011/292/EU of 31 March 2011 on the security rules for protecting EU classified information.

6. The security classification and, where applicable, the date or specific event after which it may be downgraded or declassified, shall be clearly and correctly indicated, regardless of whether the EUCI is in paper, oral, electronic or any other form.

7. Individual parts of a given document (i.e. pages, paragraphs, sections, annexes, appendices, attachments and enclosures) may require different classifications and shall be marked accordingly, including when stored in electronic form.

8. To the extent possible, documents containing parts with different classification levels shall be structured so that parts with a different classification level may be easily identified and detached if necessary.

9. The overall classification level of a document or file shall be at least as high as that of its most highly classified component. When information from various sources is collated, the final product shall be reviewed to determine its overall security classification level, since it may warrant a higher classification than its component parts.

10. The classification of a letter or note covering enclosures shall be as high as the highest classification of its enclosures. The originator shall indicate clearly at which level it is classified when detached from its enclosures by means of an appropriate marking, e.g.:

CONFIDENTIEL UE/EU CONFIDENTIAL

Without attachment(s) RESTREINT UE/EU RESTRICTED

Markings

11. In addition to one of the security classification markings set out in Article 2(2) of Annex A, EUCI may bear additional markings, such as:

(a) an identifier to designate the originator;

(b) any caveats, code words or acronyms specifying the field of activity to which the document relates, a particular distribution on a need-to-know basis or restrictions on use;

(c) releasability markings.

12. Following a decision to release EUCI to a third State of International Organization, the EEAS Security Directorate shall forward the classified information concerned, which shall bear a releasability marking indicating the third State or international organisation to which it is to be released.

13. A list of authorised markings will be adopted by the EEAS Security Authority.

Abbreviated classification markings

14. Standardised abbreviated classification markings may be used to indicate the classification level of individual paragraphs of a text. Abbreviations shall not replace the full classification markings.

15. The following standard abbreviations may be used within EU classified documents to indicate the classification level of sections or blocks of text of less than a single page:

TRES SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Creation of EUCI

16. When creating an EU classified document:

(a) each page shall be marked clearly with the classification level;

(b) each page shall be numbered;

(c) the document shall bear a reference number and a subject, which is not itself classified information, unless it is marked as such;

(d) the document shall be dated;

(e) documents classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall bear a copy number on every page, if they are to be distributed in several copies.

17. Where it is not possible to apply paragraph 15 to EUCI, other appropriate measures shall be taken in accordance with security guidelines to be established pursuant to this Decision.

Downgrading and declassification of EUCI

18. At the time of its creation, the originator shall indicate, where possible, and in particular for information classified RESTREINT UE/EU RESTRICTED, whether EUCI can be downgraded or declassified on a given date or following a specific event.

19. The EEAS shall regularly review EUCI held by it to ascertain whether the classification level still applies. The EEAS shall establish a system to review the classification level of registered EUCI that it has originated no less frequently than every five years. Such a review shall not be necessary where the originator has indicated from the outset a specific time when the information will automatically be downgraded or declassified and the information has been marked accordingly.

III. REGISTRATION OF EUCI FOR SECURITY PURPOSES

20. A central registry shall be established in Headquarters. For every organisational entity within the EEAS in which EUCI is handled, a responsible registry shall be established, subordinated to the central registry, to ensure that EUCI is handled in accordance with this Decision. Registries shall be established as Secured Areas as defined in Annex A.

Each Union Delegation establishes its own EUCI registry.

The EEAS security authority shall designate a Chief Registry Officer for these registries.

21. For the purposes of this Decision, registration for security purposes (hereinafter referred to as "registration") means the application of procedures that record the life-cycle of information, including its dissemination and destruction. In the case of a CIS, registration procedures may be performed by processes within the CIS itself.

22. All material classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be registered when it arrives at or leaves an organisational entity including Union Delegations. Information classified TRES SECRET UE/EU TOP SECRET shall be registered in designated registries.

23. The Central Registry shall be, in EEAS Headquarters, the main point of entry and exit for classified information exchanges with third States and international organisations. It shall keep a record of all these exchanges.

24. The HR shall approve a security policy on the registration of EUCI for security purposes, in accordance with article 14 of this Decision.

Tres secret UE/EU top secret registries

25. The Central Registry shall be designated in the EEAS Headquarters to act as the central receiving and dispatching authority for information classified TRES SECRET UE/EU TOP SECRET. Where necessary, subordinate registries may be designated to handle such information for registration purposes.

26. Such subordinate registries may not transmit TRES SECRET UE/EU TOP SECRET documents directly to other subordinate registries of the same central TRES SECRET UE/EU TOP SECRET registry or externally without the express written approval of the latter.

IV. COPYING AND TRANSLATING EU CLASSIFIED DOCUMENTS

27. TRES SECRET UE/EU TOP SECRET documents shall not be copied or translated without the prior written consent of the originator.

28. Where the originator of documents classified SECRET UE/EU SECRET and below has not imposed caveats on their copying or translation, such documents may be copied or translated on instruction from the holder.

29. The security measures applicable to the original document shall apply to copies and translations thereof. The copies of CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be created only by a relevant (sub) registry with a secured copy-machine. The copies must be registered.

V. CARRIAGE OF EUCI

30. Carriage of EUCI shall be subject to the protective measures set out in paragraphs 31 to 41. When EUCI is carried on electronic media, and notwithstanding Article 7(4) of Annex A, the protective measures set out below may be supplemented by appropriate technical countermeasures prescribed by the EEAS security authority so as to minimise the risk of loss or compromise.

31. The EEAS security authority shall issue instructions on the carriage of EUCI in accordance with this Decision.

Within a building or self-contained group of buildings

32. EUCI carried within a building or self-contained group of buildings shall be covered in order to prevent observation of its contents.

33. Within a building or self-contained group of buildings, information classified TRES SECRET UE/EU TOP SECRET shall be carried by appropriately security cleared individuals, in a secured envelope bearing only the addressee's name.

Within the EU

34. EUCI carried between buildings or premises within the EU shall be packaged so that it is protected from unauthorised disclosure.

35. The carriage of information classified up to SECRET UE/EU SECRET within the EU shall be by one of the following means:

(a) military, government or diplomatic courier, as appropriate;

(b) hand carriage, provided that:

(i) EUCI does not leave the possession of the bearer, unless it is stored in accordance with the requirements set out in Annex A II;

(ii) EUCI is not opened *en route* or read in public places;

(iii) individuals are security cleared to the appropriate level and briefed on their security responsibilities;

(iv) individuals are provided with a courier certificate where necessary;

(c) postal services or commercial courier services, provided that:

(i) they are approved by the relevant NSA in accordance with national laws and regulations;

(ii) they apply appropriate protective measures in accordance with minimum requirements to be laid down in security guidelines pursuant to Article 20(1) of this Decision.

In the case of carriage from one Member State to another, the provisions of point (c) shall be limited to information classified up to CONFIDENTIEL UE/EU CONFIDENTIAL.

36. Material classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET (e.g. equipment or machinery) which cannot be carried by the means referred to in paragraph 34 shall be transported as freight by commercial carrier companies in accordance with Annex A V.

37. The carriage of information classified TRES SECRET UE/EU TOP SECRET between buildings or premises within the EU shall be by military, government or diplomatic courier, as appropriate.

From within the EU to the territory of a third State, or between EU entities in third States

38. EUCI carried from within the EU to the territory of a third State, or between EU entities in third States, shall be packaged in such a way that it is protected from unauthorised disclosure.

39. The carriage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET from within the EU to the territory of a third State, and the carriage of any EUCI classified up to SECRET UE/EU SECRET between EU entities in third States, shall be by one of the following means:

(a) military or diplomatic courier;

(b) hand carriage, provided that:

(i) the package bears an official seal, or is packaged so as to indicate that it is an official consignment and should not undergo customs or security scrutiny;

(ii) individuals carry a courier certificate identifying the package and authorising them to carry the package;

(iii) EUCI does not leave the possession of the bearer, unless it is stored in accordance with the requirements set out in Annex A II;

(iv) EUCI is not opened *en route* or read in public places; and

(v) individuals are security cleared to the appropriate level and briefed on their security responsibilities.

40. The carriage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET released by the EU to a third State or international organisation shall comply with the relevant provisions under a security of information Agreement or an administrative arrangement in accordance with Article 10(2) of Annex A.

41. Information classified RESTREINT UE/EU RESTRICTED may also be carried from within the EU to the territory of a third State by postal services or commercial courier services.

42. The carriage of information classified TRES SECRET UE/EU TOP SECRET from within the EU to the territory of a third State, or between EU entities in third States, shall be by military or diplomatic courier.

VI. **DESTRUCTION OF EUCI**

43. EU classified documents that are no longer required may be destroyed, without prejudice to the relevant rules and regulations on archiving.

44. Documents subject to registration in accordance with Article 7(2) of Annex A shall be destroyed by the responsible registry on instruction from the holder or from a competent authority. The logbooks and other registration information shall be updated accordingly.

45. For documents classified SECRET UE/EU SECRET or TRES SECRET UE/EU TOP SECRET, destruction shall be performed in the presence of a witness who shall be cleared to at least the classification level of the document being destroyed.

46. The registrar and the witness, where the presence of the latter is required shall sign a destruction certificate, which shall be filed in the registry. The registry shall keep destruction certificates of TRES SECRET UE/EU TOP SECRET documents for a period of at least ten years and of documents CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET for a period of at least five years.

47. Classified documents, including those classified RESTREINT UE/EU RESTRICTED, shall be destroyed by methods which meet relevant EU or equivalent standards or which have been approved by Member States in accordance with national technical standards so as to prevent reconstruction in whole or in part.

48. The destruction of computer storage media used for EUCI shall be in accordance with paragraph 36 of Annex A IV.

VII. SECURITY INSPECTIONS

EEAS security inspections

49. In accordance with Article 15 of this Decision, the EEAS security inspections encompass:

(a) general security inspections, whose aim shall be to assess the general security level of the EEAS Headquarters, Union Delegations and all dependent or related premises, especially in order to evaluate effectiveness of security measures implemented for protecting the EEAS security interests;

(b) EUCI security inspections, whose aim shall be to evaluate, generally in view of an accreditation, the effectiveness of measures implemented for protecting EUCI in EEAS Headquarters and Union Delegations.

In particular, such inspections shall be carried out, inter alia to:

(i) ensure that the required minimum standards for protecting EUCI laid down in this Decision are respected;

(ii) emphasise the importance of security and effective risk management within the entities inspected;

(iii) recommend countermeasures to mitigate the specific impact of loss of confidentiality, integrity or availability of classified information; and

(iv) reinforce security authorities' ongoing security education and awareness programmes.

Conduct of and reporting on EEAS security inspections

50. EEAS Security inspections shall be conducted by an inspection team of the EEAS Security Directorate and, when necessary, with the support of security experts of other EU Institutions or Member States.

The inspection team shall have access to any location where EUCI is handled, in particular registries and CIS points of presence.

51. EEAS Security inspections in Union Delegations can be conducted, whenever necessary, with the support of the Security Officers of the Member States' embassies located in the third countries.

52. Before the end of each calendar year, the EEAS security authority shall adopt a security inspection programme for EEAS for the following year.

53. Whenever necessary, security inspections that are not foreseen in the programme above can be arranged by the EEAS Security Authority.

54. At the end of the security inspection, the main conclusions and recommendations shall be presented to the inspected entity. Thereafter, a report on the inspection shall be drawn up by the inspection team. Where corrective actions and recommendations have been proposed, sufficient details shall be included in the report to support the conclusions reached. The report shall be forwarded to the EEAS security authority and to the head of the inspected entity.

A regular report shall be prepared under the responsibility of the EEAS Security Directorate to highlight the lessons learned from the inspections conducted over a specified period and examined by the EEAS Security Committee.

Conduct of and reporting on security inspections in EU agencies and bodies established under Title V, Chapter 2 of the TEU

55. The EEAS Security Directorate may, where appropriate, designate contributing experts to participate in joint EU inspection teams carrying out inspections in EU agencies and bodies established under Title V, Chapter 2 of the TEU.

EEAS security inspections checklist

56. The EEAS Security Directorate shall draw up and update a security inspection checklist of items to be verified in the course of a EEAS security inspection. This checklist shall be forwarded to the EEAS Security Committee.

57. The information to complete the checklist shall be obtained in particular during the inspection from the security management of the entity being inspected. Once completed with the detailed responses, the checklist shall be classified by agreement with the inspected entity. It shall not form part of the inspection report.

ANNEX A IV

PROTECTION OF EUCI HANDLED IN CIS

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 8 of Annex A.

2. The following Information Assurance (IA) properties and concepts are essential for the security and correct functioning of operations on Communication and Information Systems (CIS):

Authenticity: the guarantee that information is genuine and from *bona fide* sources;

Availability: the property of being accessible and usable upon request by an authorised entity;

Confidentiality: the property that information is not disclosed to unauthorised individuals, entities or processes;

Integrity: the property of safeguarding the accuracy and completeness of information and assets;

Non-repudiation: the ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied.

II. INFORMATION ASSURANCE PRINCIPLES

3. The provisions set out below shall form the baseline for the security of any CIS handling EUCI. Detailed requirements for implementing these provisions shall be defined in IA security policies and security guidelines.

Security risk management

4. Security risk management shall be an integral part of defining, developing, operating and maintaining CIS. Risk management (assessment, treatment, acceptance and communication) shall be conducted as an iterative process jointly by representatives of the system owners, project authorities, operating authorities and security approval authorities, using a proven, transparent and fully understandable risk assessment process. The scope of the CIS and its assets shall be clearly defined at the outset of the risk management process.

5. The EEAS competent authorities shall review the potential threats to CIS and shall maintain up-to-date and accurate threat assessments which reflect the current operational environment. They shall constantly update their knowledge of vulnerability issues and periodically review the vulnerability assessment to keep up with the changing information technology (IT) environment.

6. The aim of security risk management shall be to apply a set of security measures which results in a satisfactory balance between user requirements and residual security risk.

7. The specific requirements, scale and the degree of detail determined by the relevant Security Accreditation Authority (SAA) for accrediting a CIS shall be commensurate with the assessed risk, taking account of all relevant factors, including the classification level of the EUCI handled in the CIS. Accreditation shall include a formal residual risk statement and acceptance of the residual risk by a responsible authority.

Security throughout the CIS-life cycle

8. Ensuring security shall be a requirement throughout the entire CIS life-cycle from initiation to withdrawal from service.

9. The role and interaction of each actor involved in a CIS with regard to its security shall be identified for each phase of the life-cycle.

10. Any CIS, including its technical and non-technical security measures, shall be subject to security testing during the accreditation process to ensure that the appropriate level of assurance of the implemented security measures is obtained and to verify that they are correctly implemented, integrated and configured.

11. Security assessments, inspections and reviews shall be performed periodically during the operation and maintenance of a CIS and when exceptional circumstances arise.

12. Security documentation for a CIS shall evolve over its life-cycle as an integral part of the process of change and configuration management.

Best practice

13. The EEAS shall cooperate with GSC, Commission and Member States to develop best practice for protecting EUCI handled on CIS. Best practice guidelines shall set out technical, physical, organisational and procedural security measures for CIS with proven effectiveness in countering given threats and vulnerabilities.

14. The protection of EUCI handled on CIS shall draw on lessons learned by entities involved in IA within and outside the EU.

15. The dissemination and subsequent implementation of best practice shall help achieve an equivalent level of assurance for the various CIS operated by the EEAS which handle EUCI.

Defence in depth

16. To mitigate risk to CIS, a range of technical and non-technical security measures, organised as multiple layers of defence, shall be implemented. These layers shall include:

(a) *Deterrence:* security measures aimed at dissuading any adversary planning to attack the CIS;

(b) *Prevention:* security measures aimed at impeding or blocking an attack on the CIS;

(c) *Detection:* security measures aimed at discovering the occurrence of an attack on the CIS;

(d) *Resilience:* security measures aimed at limiting impact of an attack to a minimum set of information or CIS assets and preventing further damage; and

(e) *Recovery:* security measures aimed at regaining a secure situation for the CIS.

The degree of stringency and applicability of such security measures shall be determined following a risk assessment.

17. The EEAS competent authorities shall ensure that they can respond to incidents which may transcend organisational and national boundaries to coordinate responses and share information about these incidents and the related risk (computer emergency response capabilities).

Principle of minimality and least privilege

18. Only the functionalities, devices and services to meet operational requirements shall be implemented in order to avoid unnecessary risk.

19. CIS users and automated processes shall be given only the access, privileges or authorisations they require to perform their tasks in order to limit any damage resulting from accidents, errors, or unauthorised use of CIS resources.

20. Registration procedures performed by a CIS, where required, shall be verified as part of the accreditation process.

Information Assurance awareness

21. Awareness of the risks and available security measures is the first line of defence for the security of CIS. In particular all personnel involved in the life-cycle of CIS, including users, shall understand:

(a) that security failures may significantly harm the CIS and the whole organisation;

(b) the potential harm to others which may arise from interconnectivity and interdependency; and

(c) their individual responsibility and accountability for the security of CIS according to their roles within the systems and processes.

22. To ensure that security responsibilities are understood, IA education and awareness training shall be mandatory for all personnel involved, including senior management and CIS users.

Evaluation and approval of IT-security products

23. The required degree of confidence in the security measures, defined as a level of assurance, shall be determined following the outcome of the risk management process and in line with the relevant security policies and security guidelines.

24. The level of assurance shall be verified by using internationally recognised or nationally approved processes and methodologies. This includes primarily evaluation, controls and auditing.

25. Cryptographic products for protecting EUCI shall be evaluated and approved by a national Crypto Approval Authority (CAA) of a Member State.

26. Prior to being recommended for approval by the EEAS CAA in accordance with Article 7(5) of this Decision, such cryptographic products shall have undergone a successful second party evaluation by an Appropriately Qualified Authority (AQUA) of a Member State not involved in the design or manufacture of the equipment. The degree of detail required in a second party evaluation shall depend on the envisaged maximum classification level of EUCI to be protected by these products.

27. Where warranted on specific operational grounds, the EEAS CAA may, upon recommendation by the Council Security Committee, waive the requirements under paragraphs 25 or 26 and grant an interim approval for a specific period in accordance with Article 7(5) of this Decision.

28. An AQUA shall be a CAA of a Member State that has been accredited on the basis of criteria laid down by the Council to undertake the second evaluation of cryptographic products for protecting EUCI.

29. The High Representative shall approve a security policy on the qualifications and approval of non-cryptographic IT security products.

Transmission within Secured Areas

30. Notwithstanding the provisions of this Decision, when transmission of EUCI is confined within Secured Areas, unencrypted distribution or encryption at a lower level may be used based on the outcome of a risk management process and subject to the approval of the SAA.

Secure interconnection of CIS

31. For the purposes of this Decision, an interconnection shall mean the direct connection of two or more IT systems for the purpose of sharing data and other information resources (e.g. communication) in a unidirectional or multidirectional way.

32. A CIS shall treat any interconnected IT system as untrusted and shall implement protective measures to control the exchange of classified information.

33. For all interconnections of CIS with another IT system the following basic requirements shall be met:

(a) business or operational requirements for such interconnections shall be stated and approved by the competent authorities;

(b) the interconnection shall undergo a risk management and accreditation process and shall require the approval of the competent SAAs; and

(c) Boundary Protection Services (BPS) shall be implemented at the perimeter of all CIS.

34. There shall be no interconnection between an accredited CIS and an unprotected or public network, except where the CIS has approved BPS installed for such a purpose between the CIS and the unprotected or public network. The security measures for such interconnections shall be reviewed by the competent Information Assurance Authority (IAA) and approved by the competent SAA.

When the unprotected or public network is used solely as a carrier and the data is encrypted by a cryptographic product approved in accordance with Article 7(5) of this Decision, such a connection shall not be deemed to be an interconnection.

35. The direct or cascaded interconnection of a CIS accredited to handle TRES SECRET UE/EU TOP SECRET to an unprotected or public network shall be prohibited.

Computer storage media

36. Computer storage media shall be destroyed in accordance with procedures approved by the EEAS security authority.

37. Computer storage media shall be reused, downgraded or declassified in accordance with a security policy to be established pursuant to Article 7(2) of this Decision.

Emergency circumstances

38. Notwithstanding the provisions of this Decision, the specific procedures described below may be applied for a limited period of time in an emergency, such as during impending or actual crisis, conflict, war situations or in exceptional operational circumstances.

39. EUCI may be transmitted using cryptographic products which have been approved for a lower classification level or without encryption with the consent of the competent authority if any delay would cause harm clearly outweighing the harm entailed by any disclosure of the classified material and if:

(a) the sender and recipient do not have the required encryption facility or have no encryption facility; and

(b) the classified material cannot be conveyed in time by other means.

40. Classified information transmitted under the circumstances set out in paragraph 39 shall not bear any markings or indications distinguishing it from information which is unclassified or which can be protected by an available cryptographic product. Recipients shall be notified of the classification level, without delay, by other means.

41. Should recourse be made to paragraph 39, a subsequent report shall be made to the EEAS Security Directorate and, by it, to the EEAS Security Committee. This report will at least state the sender, the recipient and the originator of each piece of EUCI.

III. **INFORMATION ASSURANCE FUNCTIONS AND AUTHORITIES**

42. The following IA functions shall be established in the EEAS. These functions do not require single organisational entities. They shall have separate mandates. However, these functions, and their accompanying responsibilities, may be combined or integrated in the same organisational entity or split into different organisational entities, provided that internal conflicts of interests or tasks are avoided.

Information Assurance Authority (IAA)

43. The IAA shall be responsible for:

(a) developing IA security policies and security guidelines and monitoring their effectiveness and relevance;

(b) safeguarding and administering technical information related to cryptographic products;

(c) ensuring that IA measures selected for protecting EUCI comply with the relevant policies governing their eligibility and selection;

(d) ensuring that cryptographic products are selected in compliance with policies governing their eligibility and selection;

(e) coordinating training and awareness on IA;

(f) consulting with the system provider, the security actors and representatives of users in respect of IA security policies and security guidelines; and

(g) ensuring appropriate expertise is available in the expert sub-area of the EEAS Security Committee for IA issues.

TEMPEST Authority

44. The TEMPEST Authority (TA) shall be responsible for ensuring compliance of CIS with TEMPEST policies and guidelines. It shall approve TEMPEST countermeasures for installations and products to protect EUCI to a defined level of classification in its operational environment.

Crypto Approval Authority (CAA)

45. The CAA shall be responsible for ensuring that cryptographic products comply with respective cryptographic policy. It shall approve a cryptographic product to protect EUCI to a defined level of classification in its operational environment.

Crypto Distribution Authority (CDA)

46. The CDA shall be responsible for:

(a) managing and accounting for EU crypto material;

(b) ensuring that appropriate procedures are enforced and channels established for accounting, secure handling, storage and distribution of all EU crypto material; and

(c) ensuring the transfer of EU crypto material to or from individuals or services using it.

Security Accreditation Authority (SAA)

47. The SAA for each system shall be responsible for:

(a) ensuring that CIS comply with the relevant security policies and security guidelines, providing a statement of approval for CIS to handle EUCI to a defined level of classification in its operational environment, stating the terms and conditions of the accreditation, and criteria under which re-approval is required;

(b) establishing a security accreditation process, in accordance with the relevant policies, clearly stating the approval conditions for CIS under its authority;

(c) defining a security accreditation strategy setting out the degree of detail for the accreditation process commensurate with the required level of assurance;

(d) examining and approving security-related documentation, including risk management and residual risk statements, System-specific Security Requirement Statements (hereinafter referred to as "SSRSs"), security implementation verification documentation and Security Operating Procedures (hereinafter referred to as "SecOPs"), and ensuring that it complies with the EEAS's security rules and policies;

(e) checking implementation of security measures in relation to the CIS by undertaking or sponsoring security assessments, inspections or reviews;

(f) defining security requirements (e.g. personnel security clearance levels) for sensitive positions in relation to the CIS;

(g) endorsing the selection of approved cryptographic and TEMPEST products used to provide security for a CIS;

(h) approving, or where relevant, participating in the joint approval of the interconnection of a CIS to other CIS; and

(i) consulting the system provider, the security actors and representatives of the users with respect to security risk management, in particular the residual risk, and the terms and conditions of the approval statement.

48. The EEAS SAA shall be responsible for accrediting all CIS operating within the remit of the EEAS.

Security Accreditation Board (SAB)

49. A joint SAB shall be responsible for accrediting CIS within the remit of both the EEAS SAA and Member States' SAAs. It shall be composed of an SAA representative from each Member State and be attended by an SAA representative of the GSC and Commission. Other entities with nodes on a CIS shall be invited to attend when that system is under discussion.

The SAB shall be chaired by a representative of the EEAS SAA. It shall act by consensus of SAA representatives of institutions, Member States and other entities with nodes on the CIS. It shall make periodic reports on its activities to the EEAS Security Committee and shall notify it of all accreditation statements.

Information Assurance Operational Authority

50. The IA Operational Authority for each system shall be responsible for:

(a) developing security documentation in line with security policies and security guidelines, in particular the System-specific Security Requirement Statement (SSRS) including the residual risk statement, the Security Operating Procedures (SecOPs) and the crypto plan within the CIS accreditation process;

(b) participating in selecting and testing the system-specific technical security measures, devices and software, to supervise their implementation and to ensure that they are securely installed, configured and maintained in accordance with the relevant security documentation;

(c) participating in selecting TEMPEST security measures and devices if required in the SSRS and ensuring that they are securely installed and maintained in cooperation with the TA;

(d) monitoring implementation and application of the SecOPs and, where appropriate, delegating operational security responsibilities to the system owner;

(e) managing and handling cryptographic products, ensuring the custody of crypto and controlled items and, if so required, ensuring the generation of cryptographic variables;

(f) conducting security analysis reviews and tests, in particular to produce the relevant risk reports, as required by the SAA;

(g) providing CIS-specific IA training;

(h) implementing and operating CIS-specific security measures.

ANNEX A V

INDUSTRIAL SECURITY

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 9 of Annex A. It lays down general security provisions applicable to industrial or other entities in pre-contract negotiations and throughout the life-cycle of classified contracts let by the EEAS.

2. The High Representative shall approve a policy on industrial security outlining in particular detailed requirements regarding Facility Security Clearances (FSCs), Security Aspects Letters (SALs), visits, transmission and carriage of EUCI.

II. SECURITY ELEMENTS IN A CLASSIFIED CONTRACT

Security classification guide (SCG)

3. Prior to launching an invitation to tender or letting a classified contract, the EEAS, as the contracting authority, shall determine the security classification of any information to be provided to bidders and contractors, as well as the security classification of any information to be created by the contractor. For that purpose, the EEAS shall prepare a SCG to be used for the performance of the contract.

4. In order to determine the security classification of the various elements of a classified contract, the following principles shall apply:

   (a) in preparing an SCG, the EEAS shall take into account all relevant security aspects, including the security classification assigned to information provided and approved to be used for the contract by the originator of the information;

   (b) the overall level of classification of the contract may not be lower than the highest classification of any of its elements; and

   (c) where relevant, the EEAS shall liaise with the Member States' NSAs/DSAs or any other competent security authority concerned in the event of any changes regarding the classification of information created by or provided to contractors in the performance of a contract and when making any subsequent changes to the SCG.

Security aspects letter (SAL)

5. The contract-specific security requirements shall be described in an SAL. The SAL shall, where appropriate, contain the SCG and shall be an integral part of a classified contract or sub-contract.

6. The SAL shall contain provisions requiring the contractor and/or subcontractor to comply with the minimum standards laid down in this Decision. Non-compliance with these minimum standards may constitute sufficient grounds for the contract to be terminated.

Programme/project security instructions (PSI)

7. Depending on the scope of programmes or projects involving access to or handling or storage of EUCI, specific Programme/Project Security Instructions (PSI) may be prepared by the contracting authority designated to manage the programme or project. The PSI shall require the approval of the Member States' NSAs/DSAs or any other competent security authority participating in the programme/project and may contain additional security requirements.

III. FACILITY SECURITY CLEARANCE (FSC)

8. The EEAS Security Directorate shall request the NSA or DSA or other competent security authority of the Member State concerned to grant an FSC to indicate, in accordance with national laws and regulations, that an industrial or other entity can protect EUCI at the appropriate classification level (CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET) within its facilities. A contractor, subcontractor, or potential contractor or subcontractor shall not be provided with or granted access to EUCI, until proof of FSC has been transmitted to the EEAS.

9. Where relevant, the EEAS, as the contracting authority, shall notify the appropriate NSA/DSA or any other competent security authority that an FSC is required in the pre-contractual stage or for performing the contract. An FSC or PSC shall be required in the pre-contractual stage where EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has to be provided in the course of the bidding process.

10. The EEAS as contracting authority shall not award a classified contract with a preferred bidder before having received confirmation from the NSA/DSA or any other competent security authority of the Member State in which the contractor or subcontractor concerned is registered that, where required, an appropriate FSC has been issued.

11. The EEAS as contracting authority shall request the NSA/DSA or any other competent security authority which has issued an FSC to notify it of any adverse information affecting the FSC. In the case of a sub-contract, the NSA/DSA or any other competent security authority shall be informed accordingly.

12. Withdrawal of an FSC by the relevant NSA/DSA or any other competent security authority shall constitute sufficient grounds for the EEAS, as the contracting authority, to terminate a classified contract or exclude a bidder from the competition.

IV. PERSONNEL SECURITY CLEARANCES (PSCs) FOR CONTRACTORS' PERSONNEL

13. All personnel working for contractors requiring access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall have been appropriately security cleared and have a need-to-know to access the information. Although a PSC is not required for access to EUCI at the level of RESTREINT UE/EU RESTRICTED, the need-to-know for such access shall exist.

14. Applications for the PSCs for contractor personnel shall be made to the NSA/DSA responsible for the entity.

15. The EEAS shall point out to contractors wishing to employ a national of a third State in a position that requires access to EUCI, that it is the responsibility of the NSA/DSA of the Member State in which the hiring entity is located and incorporated to determine whether the individual can be granted access to such information, in accordance with this Decision, and to confirm that the originator's consent must have been provided before such access is given.

V. CLASSIFIED CONTRACTS AND SUB-CONTRACTS

16. Where EUCI is provided to a bidder at the pre-contractual stage, the invitation to tender shall contain a provision obliging a bidder which fails to submit a bid or which is not selected to return all classified documents within a specified period of time.

17. Once a classified contract or sub-contract has been awarded, the EEAS, as the contracting authority, shall notify the contractor's or subcontractor's NSA/DSA or any other competent security authority about the security provisions of the classified contract.

18. When such contracts are terminated or they end, the EEAS, as the contracting authority (and/or the NSA/DSA or any other competent security authority, as appropriate, in the case of a sub-contract) shall promptly notify the NSA/DSA or any other competent security authority of the Member State in which the contractor or subcontractor is registered.

19. As a general rule, the contractor or subcontractor shall be required to return to the contracting authority, upon termination or ending of the classified contract or sub-contract, any EUCI held by it.

20. Specific provisions for the disposal of EUCI during the performance of the contract or upon its termination or ending shall be laid down in the SAL.

21. Where the contractor or subcontractor is authorised to retain EUCI after termination or ending of a contract, the minimum standards contained in this Decision shall continue to be complied with and the confidentiality of EUCI shall be protected by the contractor or subcontractor.

22. The conditions under which the contractor may subcontract shall be defined in the invitation to tender and in the contract.

23. A contractor shall obtain permission from the EEAS, as the contracting authority, before sub-contracting any parts of a classified contract. No subcontract may be awarded to industrial or other entities registered in a non-EU Member State which has not concluded a security of information Agreement with the EU.

24. The contractor shall be responsible for ensuring that all sub-contracting activities are undertaken in accordance with the minimum standards laid down in this Decision and shall not provide EUCI to a subcontractor without the prior written consent of the contracting authority.

25. With regard to EUCI created or handled by the contractor or subcontractor, the rights incumbent on the originator shall be exercised by the contracting authority.

VI. VISITS IN CONNECTION WITH CLASSIFIED CONTRACTS

26. Where the EEAS, contractors or subcontractors require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in each other's premises for the performance of a classified contract, visits shall be arranged by liaison with the NSAs/DSAs or any other competent security authority concerned. This is without prejudice to the prerogative of the NSAs/DSAs, in the context of specific projects, to agree on a procedure whereby such visits can be arranged directly.

27. All visitors shall hold an appropriate PSC and have a "need-to-know" for access to the EUCI related to the EEAS contract.

28. Visitors shall be given access only to EUCI related to the purpose of the visit.

VII. TRANSMISSION AND CARRIAGE OF EUCI

29. With regard to the transmission of EUCI by electronic means, the relevant provisions of Article 8 of Annex A, and of Annex A IV shall apply.

30. With regard to the carriage of EUCI, the relevant provisions of Annex A III shall apply, in accordance with national laws and regulations.

31. For the transport of classified material as freight, the following principles shall be applied when determining security arrangements:

(a) security shall be assured at all stages during transportation from the point of origin to the final destination;

(b) the degree of protection afforded to a consignment shall be determined by the highest classification level of material contained within it;

(c) an FSC at the appropriate level shall be obtained for companies providing transportation, if it also implies that classified information is stored in contractors' facilities. In any case, personnel handling the consignment shall be appropriately security cleared in accordance with Annex A I;

(d) prior to any cross-border movement of material classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, a transportation plan shall be drawn up by the consignor and approved by the EEAS when appropriate in liaison with the NSA/DSAs of both the consignor and the consignee or any other competent security authority concerned;

(e) journeys shall be point to point to the extent possible, and shall be completed as quickly as circumstances permit;

(f) whenever possible, routes should be only through Member States. Routes through States other than Member States should only be undertaken when authorised by the EEAS or any other competent security authority of the States of both the consignor and the consignee.

VIII. TRANSFER OF EUCI TO CONTRACTORS LOCATED IN THIRD STATES

32. EUCI shall be transferred to contractors and subcontractors located in third States that have a valid security agreement with the EU in accordance with security measures agreed between the EEAS, as the contracting authority, and the NSA/DSA of the third State concerned where the contractor is registered.

IX. HANDLING AND STORAGE OF INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED

33. In liaison, as appropriate, with the NSA/DSA of the Member State the EEAS, as the contracting authority, shall be entitled to conduct visits to contractors'/subcontractors' facilities on the basis of contractual provisions in order to verify that the relevant security measures for the protection of EUCI at the level RESTREINT UE/EU RESTRICTED as required under the contract have been put in place.

34. To the extent necessary under national laws and regulations, NSAs/DSAs or any other competent security authority shall be notified by the EEAS as the contracting authority of contracts or sub-contracts containing information classified RESTREINT UE/EU RESTRICTED.

35. An FSC or a PSC for contractors or subcontractors and their personnel shall not be required for contracts let by the EEAS containing information classified RESTREINT UE/EU RESTRICTED.

36. The EEAS, as the contracting authority, shall examine the responses to invitations to tender for contracts which require access to information classified RESTREINT UE/EU RESTRICTED, notwithstanding any requirement relating to FSC or PSC which may exist under national laws and regulations.

37. The conditions under which the contractor may subcontract shall be in accordance with paragraphs 22-24.

38. Where a contract involves handling information classified RESTREINT UE/EU RESTRICTED in a CIS operated by a contractor, the EEAS as contracting authority shall ensure that the contract or any sub-contract specifies the necessary technical and administrative requirements regarding accreditation of the CIS commensurate with the assessed risk, taking account of all relevant factors. The scope of accreditation of such CIS shall be agreed between the contracting authority and the relevant NSA/DSA.

ANNEX A VI

EXCHANGE OF CLASSIFIED INFORMATION WITH THIRD STATES AND INTERNATIONAL ORGANISATIONS

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 10 of Annex A.

II. FRAMEWORKS GOVERNING THE EXCHANGE OF CLASSIFIED INFORMATION

2. The EEAS may exchange EUCI with third States or international organisations in accordance with Article 10(1) of Annex A.

To support the HR in performing the responsibilities set out in Article 218 TFEU:

(a) the relevant EEAS geographical or thematic department, in consultation with the EEAS Security Directorate, shall, when appropriate, identify the need for a long term exchange of EUCI with the third State or international organisation concerned;

(b) the EEAS Security Directorate, in consultation with the relevant EEAS geographical department, shall, where appropriate, submit to the HR the draft texts to be proposed to the Council by virtue of Article 218(3),(5), and (6) of TFEU;

(c) the EEAS Security Directorate shall support the HR in conducting negotiations, in coordination with the relevant services of the Commission and of the General Secretariat of the Council;

(d) in relation to agreements or arrangements with third States for their participation in CSDP crisis management operations as referred to in Article 10(1)(c) of Annex A, the EEAS Crisis Management and Planning Directorate, in consultation with the relevant EEAS services, shall, where appropriate, submit to the HR the draft texts to be proposed to the Council by virtue of Article 218(3),(5), and (6) of TFEU, and shall support the HR in conducting negotiations in coordination with the relevant services of the EEAS and of the General Secretariat of the Council.

3. Where security of information agreements provide for technical implementing arrangements to be agreed between the EEAS Security Directorate - in coordination with the Security Directorate of the Directorate General for Human Resources and Security of the Commission and the Security Office of the General Secretariat of the Council - and the competent security authority of the third State or international organisation in question, such arrangements shall take account of the level of protection provided by the security regulations, structures and procedures in place in the third State or international organisation concerned.

4. Where a long-term need exists for the EEAS to exchange information classified no higher than RESTREINT UE/EU RESTRICTED with a third State or international organisation, and where it has been established that the party in question does not have a sufficiently developed security system for it to be possible to enter into a security of information agreement, the HR may, after having obtained the unanimous favourable opinion of the EEAS Security Committee in accordance with Article 14(5) of this Decision, enter into an administrative arrangement with the competent security authorities of the third State or international organisation in question.

5. No EUCI shall be exchanged by electronic means with a third State or international organisation unless explicitly provided for in the security of information agreement or administrative arrangement.

6. Under an administrative arrangement on the exchange of classified information, the EEAS and the third State or international organisation shall each designate a registry as the main point of entry and exit for classified information exchanged. For the EEAS, this will be the EEAS central registry.

7. Administrative arrangements shall as a general rule take the form of an exchange of letters.

III. ASSESSMENT VISITS

8. Assessment visits referred to in Article 16 of this Decision shall be conducted by mutual agreement with the third State or international organisation concerned, and shall evaluate:

(a) the regulatory framework applicable for protecting classified information;

(b) any specific features of the third State or international organisation's security laws, regulations, policies or procedures which may have an impact on the maximum level of classified information that may be exchanged;

(c) the security measures and procedures currently in place for the protection of classified information; and

(d) security clearance procedures for the level of EUCI to be released.

9. No EUCI shall be exchanged before an assessment visit has been conducted and the level at which classified information may be exchanged between the parties has been determined, based on the equivalency of the level of protection that will be afforded to it.

If, pending such assessment visit, the HR is made aware of any exceptional or urgent reasons for exchanging classified information, the EEAS shall:

(a) first seek the originator's written consent to establish that there are no objections to release.

(b) refer to the EEAS security authority, who may decide to release, provided that the unanimous favourable opinion of the Member States as represented in the EEAS Security Committee has been obtained.

If the EEAS cannot establish the originator, the EEAS security authority shall assume the originator's responsibility after having obtained the unanimous favourable opinion of the EEAS Security Committee.

IV. AUTHORITY TO RELEASE EUCI TO THIRD STATES OR INTERNATIONAL ORGANISATIONS

10. Where a framework exists in accordance with Article 10(1) of Annex A for exchanging classified information with a third State or international organisation, the decision to release EUCI by the EEAS to a third State or international organisation shall be taken by the EEAS security authority, which may delegate such authorisation to senior EEAS officials or other persons under its authority.

11. If the originator of the classified information to be released, including the originators of source material it may contain, is not the EEAS, the EEAS shall first seek the originator's written consent to establish that there are no objections to release. If the EEAS cannot establish the originator, the EEAS security authority shall assume the originator's responsibility after having obtained the unanimous favourable opinion of the Member States as represented in the EEAS Security Committee.

V. EXCEPTIONAL AD HOC RELEASE OF EUCI

12. In the absence of one of the frameworks referred to in Article 10(1) of Annex A, and when the interests of the EU or of one or more of its Member States require the release of EUCI for political, operational or urgent reasons, EUCI may exceptionally be released to a third State or international organisation once the following actions have been taken.

The EEAS Security Directorate shall, after ensuring that conditions referred to in Paragraph 11 above are met:

(a) to the extent possible, verify with the security authorities of the third State or international organisation concerned that its security regulations, structures and procedures are such that EUCI released to it will be protected in accordance with standards no less stringent than those laid down in this Decision;

(b) invite the EEAS Security Committee to formulate an opinion, on the basis of the available information, regarding the confidence that can be placed on the security regulations, structures and procedures in the third State or international organisation to which the EUCI is to be released;

(c) refer to the EEAS security authority, who may decide to release, provided that the unanimous favourable opinion of the Member States as represented in the EEAS Security Committee has been obtained.

13. In the absence of one of the frameworks referred to in Article 10(1) of Annex A, the third party in question shall undertake in writing to protect the EUCI appropriately.

APPENDIX A

DEFINITIONS

For the purposes of this Decision, the following definitions shall apply:

"Accreditation" means the process leading to a formal statement by the Security Accreditation Authority (SAA) that a system is approved to operate with a defined level of classification, in a particular security mode in its operational environment and at an acceptable level of risk, based on the premise that an approved set of technical, physical, organisational and procedural security measures has been implemented;

"Asset" means anything that is of value to an organisation, its business operations and their continuity, including information resources that support the organisation's mission;

"Authorization to access EUCI" means an authorisation by the EEAS Security Authority, which is taken in accordance with this Decision after a PSC has been issued by the competent authorities of a Member State, and which certifies that an individual may, provided his "need-to-know" has been determined, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date — see Article 2 of Annex A I;

"Breach" is an act or omission by an individual which is contrary to the security rules laid down in this Decision and/or to the security policies or guidelines setting out any measures necessary for its implementation;

"CIS life-cycle" means the entire duration of existence of a CIS, which includes initiation, conception, planning, requirements analysis, design, development, testing, implementation, operation, maintenance and decommissioning;

"Classified contract" means a contract entered into by the EEAS with a contractor for the supply of goods, execution of works or provision of services, the performance of which requires or involves access to or the creation of EUCI;

"Classified subcontract" means a contract entered into by a contractor of the EEAS with another contractor (i.e. the subcontractor) for the supply of goods, execution of works or provision of services, the performance of which requires or involves access to or the creation of EUCI;

"Communication and information system" (CIS) means any system enabling the handling of information in electronic form. A communication and information system shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources; — see Article 8 (2) of Annex A;

"Compromise of EUCI" means the total or partial disclosure of EUCI to unauthorised persons or entities — see Article 8(2);

"Contractor" means an individual or legal entity possessing the legal capacity to undertake contracts;

"Cryptographic (Crypto) products" are cryptographic algorithms, cryptographic hardware and software modules, and products including implementation details and associated documentation and keying material;

"CSDP operation" means a military or civilian crisis management operation under Title V, Chapter 2, of the TEU;

"Declassification" means the removal of any security classification;

"Defence in depth" means the application of a range of security measures organised as multiple layers of defence;

"Designated Security Authority" (DSA) means an authority responsible to the National Security Authority (NSA) of a Member State which is responsible for communicating to industrial or other entities national policy on all matters of industrial security and for providing direction and assistance in its implementation. The function of DSA may be carried out by the NSA or by any other competent authority;

"Document" means any recorded information regardless of its physical form or characteristics;

"Downgrading" means a reduction in the level of security classification;

"EU classified information" (EUCI) means any information or material the unauthorized disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States, designated by an EU security classification — see Article 2 (f);

"Facility Security Clearance" (FSC) means an administrative determination by an NSA or DSA that, from the security viewpoint, a facility can afford an adequate level of protection to EUCI of a specified security classification level and its personnel who require access to EUCI have been appropriately security cleared and briefed on the relevant security requirements necessary to access and protect EUCI;

"Handling" of EUCI means all possible actions to which EUCI may be subject throughout its life-cycle. It comprises its creation, processing, carriage, downgrading, declassification and destruction. In relation to CIS it also comprises its collection, display, transmission and storage;

"Holder" means a duly authorised individual with an established need-to-know who is in possession of an item of EUCI and is accordingly responsible for protecting it;

"Industrial or other entity" means an entity involved in supplying goods, executing works or providing services; this may be an industrial, commercial, service, scientific, research, educational or development entity or a self-employed individual;

"Industrial security" is the application of measures to ensure the protection of EUCI by contractors or subcontractors in pre-contract negotiations and throughout the life-cycle of classified contracts. — see Article 9 (1) of Annex A;

"Information Assurance" in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Effective IA shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. IA shall be based on a risk management process — see Article 8(1) of Annex A;

"Interconnection" means, for the purposes of this Decision, the direct connection of two or more IT systems for the purpose of sharing data and other information resources (e.g. communication) in a unidirectional or multidirectional way — see Annex A IV, paragraph 31;

"Management of classified information" is the application of administrative measures for controlling EUCI throughout its life-cycle to supplement the measures provided for in Articles 5, 6 and 8 and thereby help deter, detect and recover from deliberate or accidental compromise or loss of such information. Such measures relate in particular to the creation, registration, copying, translation, carriage, handling, storage and destruction of EUCI — see Article 7(1) of Annex A;

"Material" means any document or item of machinery or equipment, either manufactured or in the process of manufacture;

"Originator" means the EU institution, agency or body, Member State, third state or international organisation under whose authority classified information has been created and/or introduced into the EU's structures;

"Personnel security" is the application of measures to ensure that access to EUCI is granted only to individuals who have:

— a need-to-know;

— for access to CONFIDENTIEL UE/EU CONFIDENTIAL information or above, been security cleared to the relevant level, or are otherwise duly authorised by virtue of their functions in accordance with national laws and regulations; and

— been briefed on their responsibilities,

see Article 5 (1) of Annex A;

"Personnel Security Clearance" (PSC) for access to EUCI means a statement by a competent authority of a Member State which is made following completion of a security investigation conducted by the competent authorities of a Member State and which certifies that an individual may, provided his "need-to-know" has been determined, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date; the individual thus described is said to be "security cleared";

"Personnel Security Clearance Certificate" (PSCC) means a certificate issued by a competent authority establishing that an individual is security cleared and holds a valid PSC, and which shows the level of EUCI to which that individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date of validity of the relevant PSC and the date of expiry of the certificate itself;

"Physical security" is the application of physical and technical protective measures to deter unauthorised access to EUCI — see Article 6 of Annex A;

"Programme/Project Security Instruction" (PSI) means a list of security procedures which are applied to a specific programme/project in order to standardise security procedures. It may be revised throughout the programme/project;

"Registration" means the application of procedures that record the life-cycle of information, including its dissemination and destruction. see Annex A III, paragraph 21;

"Residual risk" means the risk which remains after security measures have been implemented, given that not all threats are countered and not all vulnerabilities can be eliminated;

"Risk" means the potential that a given threat will exploit internal and external vulnerabilities of an organisation or of any of the systems it uses and thereby cause harm to the organisation and to its tangible or intangible assets. It is measured as a combination of the likelihood of threats occurring and their impact;

"Risk acceptance" is the decision to agree to the further existence of a residual risk after risk treatment.

"Risk assessment" consists of identifying threats and vulnerabilities and conducting the related risk analysis, i.e. the analysis of probability and impact.

"Risk communication" consists of developing awareness of risks among CIS user communities, informing approval authorities such risks and reporting them to operating authorities.

"Risk management process" means the entire process of identifying, controlling and minimising uncertain events that may affect the security of an organisation or of any of the systems it uses. It covers the entirety of risk-related activities, including assessment, treatment, acceptance and communication;

"Risk treatment" consists of mitigating, removing, reducing (through an appropriate combination of technical, physical, organisational or procedural measures), transferring or monitoring the risk.

"Security Aspects Letter" (SAL) means a set of special contractual conditions issued by the contracting authority which forms an integral part of any classified contract involving access to or the creation of EUCI, that identifies the security requirements or those elements of the contract requiring security protection — see Annex A V, Section II;

"Security Classification Guide" (SCG) means a document which describes the elements of a programme or contract which are classified, specifying the applicable security classification levels. The SCG may be expanded throughout the life of the programme or contract and the elements of information may be re-classified or downgraded; where an SCG exists it shall be part of the SAL — see Annex A V, Section II;

"Security investigation" means the investigative procedures conducted by the competent authority of a Member State in accordance with its national laws and regulations in order to obtain an assurance that nothing adverse is known which would prevent an individual from being granted a national or EU PSC for access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above);

"Security Operating Procedures" (SecOPs) means a description of the security policy implementation to be adopted, of the operating procedures to be followed and of the personnel responsibilities;

"Specific Security Requirement Statement" (SSRS) means a binding set of security principles to be observed and of detailed security requirements to be implemented, underlying the process of certification and accreditation of CIS;

"TEMPEST" means the investigation, study and control of compromising electromagnetic emanations and the measures to suppress them;

"Threat" means a potential cause of an unwanted incident which may result in harm to an organisation or any of the systems it uses; such threats may be accidental or deliberate (malicious) and are characterised by threatening elements, potential targets and attack methods;

"Vulnerability" means a weakness of any nature that can be exploited by one or more threats. Vulnerability may be an omission or it may relate to a weakness in controls in terms of their strength, completeness or consistency and may be of a technical, procedural, physical, organisational or operational nature.