DECISION AB n° 13/2015

OF THE ADMINISTRATIVE BOARD
OF THE AGENCY FOR THE COOPERATION OF ENERGY REGULATORS

of 17 September 2015

establishing security measures and procedures in the form of a Security Policy and an operational Security Manual

THE ADMINISTRATIVE BOARD OF THE AGENCY FOR THE COOPERATION OF ENERGY REGULATORS,

HAVING REGARD to Regulation (EC) No 713/2009 of the European Parliament and of the Council of 13 July 2009 establishing an Agency for the Cooperation of Energy Regulators[1] and, in particular, Articles 1(1) and 13(4) thereof,

WHEREAS:

(1) It is appropriate to establish operational procedures and measures to ensure that all activities which require handling EU classified information (EUCI) are covered by a comprehensive security system for protecting classified information.

(2) In accordance with national laws and regulations and to the extent required for the functioning of the Agency, the Member States should respect this Decision when their competent authorities, personnel or contractors handle EUCI, in order that each may be assured that an equivalent level of protection is afforded to EUCI.

(3) The Agency should determine the appropriate framework for sharing EUCI held by the Agency with other Union institutions, bodies, offices or agencies, as appropriate, in accordance with this Decision and inter-institutional arrangements in force.

(4) EU Special Representatives and the members of their teams should apply the security rules adopted by the Agency for protecting EUCI where so provided in the relevant Agency act.

(5) In order to ensure the application of the security rules for protecting EUCI in a timely manner this Decision should enter into force on the date of its publication,

(6) It is necessary for the Agency to establish an operational structure for crisis management in the form of procedures, alert states and measures to be used under all foreseeable security conditions. Having appropriate and proportionate security measures in place will ensure that the Agency staff and its premises are adequately equipped to respond to the relevant risk level.

[1] OJ L211, 14.8.2009, p.1

(7) It is necessary to implement these principles through a security policy of the Agency and an operational security manual,

HAS ADOPTED THIS DECISION:

Article 1

The Security Policy and the Operational Security Manual, as annexed to this Decision as per Annex A and Annex B, are hereby adopted.

Article 2

The Director of the Agency is delegated to adopt decisions and administrative notices to implement or make non-essential amendments to the Security Policy and the operational Security Manual.

The Director of the Agency may delegate the tasks mentioned in the first paragraph of this Article to the Agency's Security Officer by a separate delegation decision, in full compliance with the internal rules of procedure.

Article 3

This Decision shall enter into force on the date of its signature. The Decision shall be communicated to the staff, brought to the attention of the Staff Committee and published on the intranet of the Agency.

Done at Ljubljana on 17 September 2015.

For the Administrative Board:

SIGNED

Razvan Eugen Nicolescu
Chairman of the Administrative Board

ACER
Agency for the Cooperation of Energy Regulators

ANNEX A

SECURITY POLICY

OF THE AGENCY FOR THE COOPERATION OF ENERGY REGULATORS

Article 1

Purpose, scope and definitions

1. This Decision lays down the basic principles and minimum standards of security for protecting EU Classified Information (EUCI).
2. These basic principles and minimum standards shall apply to the Agency and be respected by the counterparties belonging to Member States which may engage in exchange or use of information owned by or in the custody of the Agency in accordance with their respective national laws and regulations, in order that each may be assured that an equivalent level of protection is afforded to EUCI.
3. For the purposes of this Decision, the definitions set out in Appendix A of Annex A shall apply.

Article 2

Definition of EUCI, security classifications and markings

1. EUCI means any information or material designated by a 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.
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 competent authorities 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 Agency shall approve 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 Union, the Agency 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.
4. An aggregate of EUCI may warrant a level of protection corresponding to a higher classification than that of its individual components.

Article 5

Security risk management

1. Risk to EUCI shall be managed as a process. This process shall be aimed at determining known security risks, defining security measures to reduce such risks to an acceptable level in accordance with the basic principles and minimum standards set out in this Decision and at applying those measures in line with the concept of defence in depth as defined in Appendix A of Annex A. The effectiveness of such measures shall be continuously evaluated.
2. Security measures for protecting EUCI throughout its life-cycle shall be commensurate in particular with its security classification, the form and the volume of the information or material, the location and construction of facilities housing EUCI and the locally assessed threat of malicious and/or criminal activities, including espionage, sabotage and terrorism.
3. Contingency plans shall take account of the need to protect EUCI during emergency situations in order to prevent unauthorised access, disclosure or loss of integrity or availability.

4. Preventive and recovery measures to minimise the impact of major failures or incidents on the handling and storage of EUCI shall be included in business continuity plans.

Article 6

Implementation of this Decision

1. Where necessary, the Director, on recommendation by the Security Committee, shall approve security policies setting out measures for implementing this Decision.
2. The Agency Security Committee may agree at its level security guidelines to supplement or support this Decision and any security policies approved by the Director.

Article 7

Personnel security

1. Personnel security is the application of measures to ensure that access to EUCI is granted only to individuals who have:
   a) a need-to-know,
   b) been security cleared to the relevant level, where appropriate, and
   c) been briefed on their responsibilities.
2. Personnel security clearance procedures shall be designed to determine whether an individual, taking into account his loyalty, trustworthiness and reliability, may be authorised to access EUCI.
3. All staff members in the Agency whose duties require them to have access to or handle EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be security cleared to the relevant level before being granted access to such EUCI. Such individuals must be authorised by the ASA to access EUCI up to a specified level and up to a specified date.
4. Personnel of counterparties belonging to a Member States referred to in Article 15(3) whose duties may require access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be security cleared to the relevant level or otherwise duly authorised by virtue of their functions, in accordance with national laws and regulations, before being granted access to such EUCI.
5. Before being granted access to EUCI and at regular intervals thereafter, all individuals shall be briefed on and acknowledge their responsibilities to protect EUCI in accordance with this Decision.
6. Provisions for implementing this Article are set out in Annex I.

Article 8

Physical security

1. Physical security is the application of physical and technical protective measures to prevent 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 segregation of 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 10(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 II and approved by the competent 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 II.

Article 9

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 7, 8 and 10 and thereby help deter and detect deliberate or accidental compromise or loss of such information. Such measures relate in particular to the creation, registration, transmission, copying, translation, downgrading, declassification, carriage 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 Director and the counterparties in the Member States 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 European Commission Directorate General Human Resources and Security – Security Directorate or by the Agency Security Office.

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 10(6);

(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 10(6); or

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

5. Provisions for implementing this Article are set out in Annexes III and IV.

Article 10

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 CIS shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources. This Decision shall apply to CIS handling EUCI.

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

4. All CIS 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. Security measures shall be implemented to protect CIS handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL and above against compromise of such information through unintentional electromagnetic emanations ('TEMPEST security

measures'). Such security measures shall be commensurate with the risk of exploitation and the level of classification of the information.

6. Where the protection of EUCI is provided by cryptographic products, such products shall be approved as follows:

   (a) the confidentiality of information classified SECRET UE/EU SECRET and above shall be protected by cryptographic products approved by the Director as Crypto Approval Authority (CAA), upon recommendation by the Agency Security Committee;

   (b) the confidentiality of information classified CONFIDENTIEL UE/EU CONFIDENTIAL or RESTREINT UE/EU RESTRICTED shall be protected by cryptographic products approved by the Director as CAA, upon recommendation by the Agency Security Committee.

   Notwithstanding point (b), within Member States' national systems, the confidentiality of EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or RESTREINT UE/EU RESTRICTED may be protected by cryptographic products approved by a Member State's CAA.

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 IV.

8. The Director and the competent authorities of the Member States respectively shall establish or identify the following IA functions:

   (a) an IA Authority (IAA);

   (b) a TEMPEST Authority (TA);

   (c) a Crypto Approval Authority (CAA);

   (d) a Crypto Distribution Authority (CDA).

9. For each system, the competent authorities of the Agency and of the Member States respectively shall establish:

   (a) a Security Accreditation Authority (SAA);

(b) an IA Operational Authority.

10. Provisions for implementing this Article will be defined following the conclusion of agreements with supervisory authorities, international organisations and the administrations of third countries.

Article 11

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. Such contracts shall not involve access to information classified TRES SECRET UE/EU TOP SECRET.

2. The Agency may entrust 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 which has concluded an agreement or an administrative arrangement in accordance with point (a) or (b) of Article 13(2).

3. The Agency, 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.

4. The National Security Authority (NSA), the Designated Security Authority (DSA) or any other counterparties of each Member State shall ensure, to the extent possible under national laws and regulations, that contractors and subcontractors registered in their territory take all appropriate measures to protect EUCI in pre-contract negotiations and when performing a classified contract.

5. The NSA, DSA or any other competent security authority of each Member State shall ensure, in accordance with national laws and regulations, that contractors or subcontractors registered in the respective Member State participating in classified contracts or sub-contracts which require access to 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, hold a Facility Security Clearance (FSC) at the relevant classification level.

6. 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 be granted a Personnel Security Clearance (PSC) by the respective NSA, DSA or any other competent security authority in accordance with national laws and regulations and the minimum standards laid down in Annex I.

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

Article 12

Sharing EUCI

1. The Agency shall determine the conditions under which it may share EUCI held by it with other Union institutions, bodies, offices or agencies or counterparties belonging to Member States. An appropriate framework may be put in place to that effect, including by entering into interinstitutional agreements or other arrangements where necessary for that purpose.

2. Any such framework shall ensure that EUCI is given protection appropriate to its classification level and according to basic principles and minimum standards which shall be equivalent to those laid down in this Decision.

Article 13

Exchange of classified information with supervisory authorities, international organisations and the administrations of third countries

1. Where the Agency determines that there is a need to exchange EUCI with supervisory authorities, international organisations and the administrations of third countries, an appropriate framework shall be put in place to that effect.

2. In order to establish such a framework and define reciprocal rules on the protection of classified information exchanged:

   (a) the Union shall conclude agreements with supervisory authorities, international organisations and the administrations of third countries on security procedures for exchanging and protecting classified information (‘security of information agreements’); or

   (b) the Director may enter into administrative arrangements where the classification level of EUCI to be released is as a general rule no higher than RESTREINT UE/EU RESTRICTED.

3. Security of information agreements or administrative arrangements referred to in paragraph 2 shall contain provisions to ensure that when supervisory authorities, international organisations and the administrations of third countries 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.

4. The decision to release EUCI originating in the Agency to supervisory authorities, international organisations and the administrations of third countries shall be taken by the Director 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 Union. If the originator of the classified information for which release is desired is not the Agency, the Agency shall first seek the originator's written consent to release. If the originator cannot be established, the Agency shall assume the former's responsibility.

5. Assessment visits shall be arranged to ascertain the effectiveness of the security measures in place in the supervisory authorities, international organisations and the administrations of third countries for protecting EUCI provided or exchanged.

Article 14

Breaches of security and compromise of EUCI

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.

2. Compromise of EUCI occurs when, as a result of a breach of security, it has wholly or in part been disclosed to unauthorised persons.

3. Any breach or suspected breach of security shall be reported immediately to the Security Officer.

4. Where it is known or where there are reasonable grounds to assume that EUCI has been compromised or lost, the NSA or other competent authority shall take all appropriate measures in accordance with the relevant laws and regulations to:

   (a) inform the originator;

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

(c) assess the potential damage caused to the interests of the Union or of the Member States;

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

(e) notify the appropriate authorities of the action taken.

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

Article 15

Responsibility for implementation

1. The Agency shall take all necessary measures to ensure overall consistency in the application of this Decision.

2. The Agency shall take all necessary measures to ensure that, when handling or storing EUCI or any other classified information, this Decision is applied in premises used by the Agency, by Agency officials and other servants, by personnel seconded to the Agency and by Agency contractors.

3. Member States shall take all appropriate measures, in accordance with their respective national laws and regulations, to ensure that when EUCI is handled or stored, this Decision is respected by:

(a) personnel of Member States' National Regulatory Authorities, and national delegates attending meetings of the Agency or of its preparatory bodies, or participating in other Agency activities;

(b) other personnel in Member States' national administrations, including personnel seconded to those administrations, whether they serve on the territory of the Member States or abroad;

(c) other persons in the Member States duly authorised by virtue of their functions to have access to EUCI; and

(d) Member States' contractors, whether on the territory of the Member States or abroad.

Article 16

The organisation of security in the Agency

1. As part of its role in ensuring overall consistency in the application of this Decision, the Agency shall approve:

   (a) agreements referred to in Article 13(2)(a);

   (b) decisions authorising or consenting to the release of EUCI originating in or held by the Agency to supervisory authorities, international organisations and the administrations of third countries, in accordance with the principle of originator consent;

   (c) an annual assessment visit programme recommended by the Agency Security Committee for visits to assess Member States' and their counterparties services and premises, entities which apply this Decision or the principles thereof, and for assessment visits to supervisory authorities, international organisations and the administrations of third countries in order to ascertain the effectiveness of measures implemented for protecting EUCI; and

   (d) security policies as foreseen in Article 6(1).

2. The Director shall be the Agency Security Authority ("ASA"). In that capacity, the ASA shall:

   (a) implement the Agency's security policy and keep it under review;

   (b) coordinate with Member States' NSAs on all security matters relating to the protection of classified information relevant for the Agency's activities;

   (c) grant Agency staff members officials, other servants and seconded national experts authorisation for access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above in accordance with Article 7(3);

   (d) as appropriate, order investigations into any actual or suspected compromise or loss of classified information held by or originating in the Agency and request the relevant security authorities to assist in such investigations;

   (e) undertake periodic inspections of the security arrangements for protecting classified information on Agency premises;

(f) ensure that security measures are coordinated as necessary with the competent authorities and counterparties of the Member States which are responsible for protecting classified information and, as appropriate, supervisory authorities, international organisations and the administrations of third countries, including on the nature of threats to the security of EUCI and the means of protection against them; and

(g) enter into the administrative arrangements referred to in Article 13(2)(b).

The Security Officer of the Agency shall assist the ASA in the performance of the responsibilities entailed by the function of the ASA.

Should also ensure that their national competent authorities provide information to the Agency, on the nature of threats to the security of EUCI and the means of protection against them.

Article 17

Agency Security Committee

1. An Agency Security Committee is hereby established. It shall examine and assess any security matter within the scope of this Decision and make recommendations to the ASA and/or the Administrative Board as appropriate.

2. The Agency Security Committee shall be composed by the ASA, the IT Officer, the Security Officer and the Heads of Departments of the Agency. It shall be chaired by the Director or by his designated delegate. It shall meet as instructed by the ASA, or at the request of the ASA.

3. The Agency Security Committee shall organise its activities in such a way that it can make recommendations on specific areas of security. Where appropriate, it may consult the Agency's DPO. The Agency Security Committee shall establish an expert sub-area for IA issues and 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 including, as appropriate, any recommendations for the Agency.

ANNEXES

ANNEX I

Personnel Security

ANNEX II

Physical Security

ANNEX III

Management of classified information

ANNEX IV

Protection of EUCI handled in CIS

ANNEX V

Industrial security

ACER
Agency for the Cooperation of Energy Regulators

ANNEX I

PERSONNEL SECURITY

I. INTRODUCTION

1. This Annex sets out the provisions for implementing Article 7 of Annex A. It lays down criteria 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.

II. GRANTING ACCESS TO EUCI

2. An individual shall only be granted access to classified information after:

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

   (b) he has been briefed on the security rules and procedures for protecting EUCI and has acknowledged his responsibilities with regard to protecting such information; and

   (c) in the case of information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above:

   — 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, or

   — in the case of Agency officials, other servants or seconded national experts, he has been given authorisation for access to EUCI by the ASA in accordance with paragraphs 16 to 25 of Annex I up to a specified level and up to a specified date.

3. The Agency shall identify the positions in their structures which require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above and therefore require security clearance to the relevant level.

III. PERSONNEL SECURITY CLEARANCE REQUIREMENTS

4. After having received a duly authorised request, NSAs or other competent national authorities shall be responsible for ensuring that security investigations are carried out on their nationals who require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above. Standards of investigation shall be in accordance with national laws and regulations with a view to issuing a PSC or providing an assurance for the individual to be granted authorisation for access to EUCI, as appropriate.

5. Should the individual concerned reside in the territory of another Member State or of a third State, the competent national authorities shall seek assistance from the competent authority of the State of residence in accordance with national laws and regulations. Member States shall assist one another in carrying out security investigations in accordance with national laws and regulations.

6. Where permissible under national laws and regulations, NSAs or other competent national

authorities may conduct investigations on non-nationals who require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above. Standards of investigation shall be in accordance with national laws and regulations.

Security investigation criteria

7. The loyalty, trustworthiness and reliability of an individual for the purposes of being security cleared for access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be determined by means of a security investigation. The competent national authority shall make an overall assessment based on the findings of such a security investigation. The principal criteria used for that purpose include, to the extent possible under national laws and regulations, an examination of whether the individual:

(a) has committed or attempted to commit, conspired with or aided and abetted another to commit any act of espionage, terrorism, sabotage, treason or sedition;

(b) is, or has been, an associate of spies, terrorists, saboteurs, or of individuals reasonably suspected of being such or an associate of representatives of organisations or foreign states, including foreign intelligence services, which may threaten the security of the Union and/or Member States unless these associations were authorised in the course of official duty;

(c) is, or has been, a member of any organisation which by violent, subversive or other unlawful means seeks, inter alia, to overthrow the government of a Member State, to change the constitutional order of a Member State or to change the form or the policies of its government;

(d) is, or has been, a supporter of any organisation described in point (c), or who is, or who has been closely associated with members of such organisations;

(e) has deliberately withheld, misrepresented or falsified information of significance, particularly of a security nature, or has deliberately lied in completing a personnel security questionnaire or during the course of a security interview;

(f) has been convicted of a criminal offence or offences;

(g) has a history of alcohol dependence, use of illegal drugs and/or misuse of legal drugs;

(h) is or has been involved in conduct which may give rise to the risk of vulnerability to blackmail or pressure;

(i) by act or through speech, has demonstrated dishonesty, disloyalty, unreliability or untrustworthiness;

(j) has seriously or repeatedly infringed security regulations; or has attempted, or succeeded in, unauthorised activity in respect of communication and information systems; and

(k) may be liable to pressure or conflict of interests (e.g. through holding one or more non-EU nationalities or through relatives or close associates who could be vulnerable to foreign intelligence services, terrorist groups or other subversive organisations, or individuals whose aims may threaten the security interests of the Union and/or Member States).

8. Where appropriate and in accordance with national laws and regulations, an individual's financial and medical background may also be considered relevant during the security

investigation.

9. Where appropriate and in accordance with national laws and regulations, a spouse's, cohabitant's or close family member's conduct and circumstances may also be considered relevant during the security investigation.

Investigative requirements for access to EUCI

Initial granting of a security clearance

10. The initial security clearance for access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET shall be based on a security investigation covering at least the last 5 years, or from age 18 to the present, whichever is the shorter, which shall include the following:

    (a) the completion of a national personnel security questionnaire for the level of EUCI to which the individual may require access; once completed, this questionnaire shall be forwarded to the competent security authority;

    (b) identity check/citizenship/nationality status — the individual's date and place of birth shall be verified and his identity checked. Citizenship status and/or nationality, past and present, of the individual shall be established; this shall include an assessment of any vulnerability to pressure from foreign sources, for example, due to former residence or past associations; and

    (c) national and local records check — a check shall be made of national security and central criminal records, where the latter exist, and/or other comparable governmental and police records. The records of law enforcement agencies with legal jurisdiction where the individual has resided or been employed shall be checked.

11. The initial security clearance for access to information classified TRES SECRET UE/EU TOP SECRET shall be based on a security investigation covering at least the last 10 years, or from age 18 to the present, whichever is the shorter. If interviews are conducted as stated in point (e), investigations shall cover at least the last 7 years, or from age 18 to the present, whichever is the shorter. In addition to the criteria indicated in paragraph 7 above, the following elements shall be investigated, to the extent possible under national laws and regulations, before granting a TRES SECRET UE/EU TOP SECRET PSC; they may also be investigated before granting a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET PSC, where required by national laws and regulations:

    (a) financial status — information shall be sought on the individual's finances in order to assess any vulnerability to foreign or domestic pressure due to serious financial difficulties, or to discover any unexplained affluence;

    (b) education — information shall be sought to verify the individual's educational background at schools, universities and other education establishments attended since his 18th birthday, or during a period judged appropriate by the investigating authority;

    (c) employment — information covering present and former employment shall be sought, reference being made to sources such as employment records, performance or efficiency reports and to employers or supervisors;

    (d) military service — where applicable, the service of the individual in the armed forces

and type of discharge shall be verified; and

(e) interviews — where provided for and admissible under national law, an interview or interviews shall be conducted with the individual. Interviews shall also be conducted with other individuals who are in a position to give an unbiased assessment of the individual's background, activities, loyalty, trustworthiness and reliability. When it is national practice to ask the subject of the investigation for referrals, referees shall be interviewed unless there are good reasons for not doing so.

12. Where necessary and in accordance with national laws and regulations, additional investigations may be conducted to develop all relevant information available on an individual and to substantiate or disprove adverse information.

Renewal of a security clearance

13. After the initial granting of a security clearance and provided that the individual has had uninterrupted service with a national administration or the Agency and has a continuing need for access to EUCI, the security clearance shall be reviewed for renewal at intervals not exceeding 5 years for a TRES SECRET UE/EU TOP SECRET clearance and 10 years for SECRET UE/EU SECRET and CONFIDENTIEL UE/EU CONFIDENTIAL clearances, with effect from the date of notification of the outcome of the last security investigation on which they were based. All security investigations for renewing a security clearance shall cover the period since the previous such investigation.

14. For renewing security clearances, the elements outlined in paragraphs 10 and 11 shall be investigated.

15. Requests for renewal shall be made in a timely manner taking account of the time required for security investigations. Nevertheless, where the relevant NSA or other competent national authority has received the relevant request for renewal and the corresponding personnel security questionnaire before a security clearance expires, and the necessary security investigation has not been completed, the competent national authority may, where admissible under national laws and regulations, extend the validity of the existing security clearance for a period of up to 12 months. If, at the end of this 12-month period, the security investigation has still not been completed, the individual shall be assigned to duties which do not require a security clearance.

Authorisation procedures in the Agency

16. For officials and other servants in the Agency, the ASA 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.

17. Where information relevant for a security investigation becomes known to the Agency concerning an individual who has applied for a security clearance for access to EUCI, the Agency, acting in accordance with the relevant rules and regulations, shall notify the relevant NSA thereof.

18. Following completion of the security investigation, the relevant NSA shall notify the ASA of the outcome of such an investigation, using the standard format for the correspondence prescribed by the Agency Security Committee.

(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 ASA may grant the individual concerned authorisation for access to EUCI up to the relevant level until a specified date.

(b) Where the security investigation does not result in such an assurance, the Agency ASA shall notify the individual concerned, who may ask to be heard by the ASA. The ASA may ask the competent NSA for any further clarification it can provide according to its national laws and regulations. If the outcome is confirmed, authorisation shall not be granted for access to EUCI.

19. The security investigation together with the results obtained shall be subject to the relevant laws and regulations in force in the Member State concerned, including those concerning appeals. Decisions by the Appointing Authority, in the capacity of ASA, 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 Council Regulation (EEC, Euratom, ECSC) No 259/68[2] ('the Staff Regulations and Conditions of Employment').

20. National experts seconded to the Agency for a position requiring access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall present a valid Personnel Security Clearance Certificate (PSCC) for access to EUCI to the ASA prior to taking up their assignment, on the basis of which the ASA shall issue an authorisation for access to EUCI.

21. The Agency will accept the authorisation for access to EUCI granted by any other Union institution, body or agency, provided it remains valid. Authorisation will cover any assignment by the individual concerned within the Agency. The Union institution, body or agency in which the individual is taking up employment will notify the relevant NSA of the change of employer.

22. 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 ASA, or if there is a break of 12 months in an individual's service, during which time he has not been employed in the Agency or in a position with a national administration of a Member State, this outcome shall be referred to the relevant NSA for confirmation that it remains valid and appropriate.

23. Where information becomes known to the Agency concerning a security risk posed by an individual who has authorisation for access to EUCI, the Agency, acting in accordance with the relevant rules and regulations, shall notify the relevant NSA thereof and may suspend access to EUCI or withdraw authorisation for access to EUCI.

24. Where an NSA notifies the Agency of withdrawal of an assurance given in accordance with paragraph 18(a) for an individual who has authorisation for access to EUCI, the ASA may ask for any clarification the NSA can provide according to its national laws and regulations. If the adverse information is confirmed, 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.

[2] Council Regulation (EEC, Euratom, ECSC) No 259/68 of 29 February 1968 laying down the Staff Regulations and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1.).

25. Any decision to withdraw or suspend an authorisation from an Agency official or other servant for access to EUCI and, where appropriate, the reasons for doing so shall be notified to the individual concerned, who may ask to be heard by the Appointing Authority, in the capacity of ASA. 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 Appointing Authority shall be subject to appeals in accordance with the Staff Regulations and Conditions of Employment.

Records of security clearances and authorisations

26. Records of PSCs and authorisations granted for access to information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be maintained respectively by each Member State and by the Agency. These records shall contain as a minimum the level of EUCI to which the individual may be granted access, the date the security clearance was granted and its period of validity.

27. The competent security authority may issue a 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 for access to EUCI or authorisation for access to EUCI and the date of expiry of the certificate itself.

Exemptions from the PSC requirement

28. Access to EUCI by individuals in Member States duly authorised by virtue of their functions shall be determined in accordance with national laws and regulations; such individuals shall be briefed on their security obligations in respect of protecting EUCI.

IV. SECURITY EDUCATION AND AWARENESS

29. All individuals who have been granted a security clearance 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 Member State and by the Agency, as appropriate.

30. All individuals who are authorised to have access to, or required to handle EUCI, shall initially be made aware, 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.

31. All individuals who cease to be employed in 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.

V. EXCEPTIONAL CIRCUMSTANCES

32. Where permissible under national laws and regulations, security clearance granted by a competent national authority of a Member State for access to national classified information may, for a temporary period pending the granting of a PSC for access to EUCI, allow access by national officials to EUCI up to the equivalent level specified in the table of equivalence in Appendix B of Annex A where such temporary access is required

in the interests of the Union. NSAs shall inform the Agency Security Committee where national laws and regulations do not permit such temporary access to EUCI.

33. For reasons of urgency, where duly justified in the interests of the service and pending completion of a full security investigation, the ASA may, after consulting the NSA of the Member State of whom 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 Agency officials and other servants to access EUCI for a specific function. Such temporary authorisations shall be valid for a period not exceeding 6 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 Agency.

34. When an individual is to be assigned to a position that requires a security clearance 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 or authorisation for access to EUCI;

(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 authority; and

(g) a record of the exception, including a description of the information to which access was approved, shall be kept by the registry or subordinate registry responsible.

35. 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.

36. Where national laws and regulations of a Member State stipulate more stringent rules with respect to temporary authorisations, provisional assignments, one-time access or emergency access by individuals to classified information, the procedures foreseen in this Section shall be implemented only within any limitations set forth in the relevant national laws and regulations.

37. The Agency Security Committee shall receive an annual report on recourse to the procedures set out in this Section.

VI. ATTENDANCE AT MEETINGS IN THE AGENCY

41. Subject to paragraph 28, individuals assigned to participate in meetings of the Agency (including Boards, Working Groups or other structures or substructures) at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed

may only do so upon confirmation of the individual's security clearance status. For delegates, a PSCC or other proof of security clearance shall be forwarded by the appropriate authorities to the Agency Security Office, or exceptionally be presented by the delegate concerned. Where applicable, a consolidated list of names may be used, giving the relevant proof of security clearance.

42. Where a PSC for access to EUCI is withdrawn for security reasons from an individual whose duties require attendance at meetings of the Agency (including Boards, Working Groups or other structures or substructures), the competent authority shall inform the Agency thereof.

VII. POTENTIAL ACCESS TO EUCI

43. 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 on security procedures for protecting EUCI and be instructed on their duties for protecting such information entrusted to them.

ACER
Agency for the Cooperation of Energy Regulators

ANNEX II

PHYSICAL SECURITY

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 8 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. Physical security measures shall be selected on the basis of a threat assessment made by the competent authorities. The Agency and Member States shall each 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; and

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

4. The Agency and/or the competent security authority of the hosting Member State, 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 NSA of the Hosting Member State can be authorised to 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 Agency and/or the competent 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 Agency 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).

In this Decision, all references to Administrative Areas and Secured Areas, including technically Secured Areas, shall be understood as also referring to the national equivalents thereof.

13. The ASA 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 ASA; 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 and specifically authorised to enter the area on the basis of their need-to-know; and

(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.

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;

(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 competent security authority. Such inspections shall also be conducted following any unauthorised entry or suspicion of such 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 competent 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; and

(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 competent 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 28 to 41 of Annex III and has undertaken to comply with compensatory measures laid down in security instructions issued by the competent 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 competent 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 28 to 41 of Annex III;

(ii) has undertaken to comply with compensatory measures laid down in security

instructions issued by the competent 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 in a Secured Area either in a security container or in a 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 under one of the following conditions:

(a) in a security container in line with paragraph 8 with at least one of the following supplementary controls:

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

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

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

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

VI. CONTROL OF KEYS AND COMBINATIONS USED FOR PROTECTING EUCI

30. The ASA 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 III

MANAGEMENT OF CLASSIFIED INFORMATION

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 9 of Annex A. It lays down the administrative measures for controlling EUCI throughout its life-cycle in order to help deter and detect 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 initial 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. The security classification shall be clearly and correctly indicated, regardless of whether the EUCI is on paper, oral, electronic or in any other form.
6. 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.
7. 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.
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 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

10. 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; or

(d) where applicable, the date or specific event after which it may be downgraded or declassified.

Abbreviated classification markings

11. 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.

12. 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

13. 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; and

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

14. Where it is not possible to apply paragraph 13 to EUCI, other appropriate measures shall be taken in accordance with security guidelines to be established pursuant to Article 6(2).

Downgrading and declassification of EUCI

15. 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.

16. The Agency shall regularly review EUCI held by it to ascertain whether the classification level still applies. The Agency shall establish a system to review the classification level of EUCI which 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 that the information will automatically be downgraded or declassified and the information has been marked accordingly.

III. REGISTRATION OF EUCI FOR SECURITY PURPOSES

17. For every Department within the Agency and Member States' national administrations in which EUCI is handled, a responsible registry shall be identified to ensure that EUCI is handled in accordance with this Decision. Registries shall be established as Secured Areas as defined in Annex II.

18. For the purposes of this Decision, registration for security purposes ('registration') means the application of procedures which record the life-cycle of material, including its dissemination and destruction.

19. All material classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be registered in designated registries when it arrives at or leaves an organisational entity.

20. The Central Registry of Classified Documents within the Agency shall keep a record of all classified information released by the Council and the Agency to third States and international organisations, and of all classified information received from third States or international organisations.

21. In the case of a CIS, registration procedures may be performed by processes within the CIS itself.

22. The Agency shall approve a security policy on the registration of EUCI for security purposes.

TRES SECRET UE/EU TOP SECRET REGISTRIES

23. A dedicated registry in the counterparties belonging to the Member States and in the Agency shall 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.

24. 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

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

26. 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.

27. The security measures applicable to the original document shall apply to copies and translations thereof.

V. CARRIAGE OF EUCI

28. Carriage of EUCI shall be subject to the protective measures set out in paragraphs 30 to 41. When EUCI is carried on electronic media, and notwithstanding Article 9(4), the protective measures set out below may be supplemented by appropriate technical countermeasures prescribed by the competent security authority so as to minimise the risk of loss or compromise.

29. The ASA and the competent security authorities in the Member States shall issue instructions on the carriage of EUCI in accordance with this Decision.

Within a building or self-contained group of buildings

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

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

Within the Union

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

33. The carriage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within the Union 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 II;

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

(iii) individuals are briefed on their security responsibilities; and

(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; and

(ii) they apply appropriate protective measures in accordance with minimum requirements to be laid down in security guidelines pursuant to Article 6(2).

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.

34. Information classified RESTREINT UE/EU RESTRICTED may also be carried by postal services or commercial courier services. A courier certificate is not required for the carriage of such information.

35. 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 33 shall be transported as freight by commercial carrier companies in accordance with Annex V.

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

From within the Union to the territory of a third State

37. EUCI carried from within the Union to the territory of a third State shall be packaged in such a way that it is protected from unauthorised disclosure.

38. The carriage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET from within the Union to the territory of a third State 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 II;

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

(v) individuals are briefed on their security responsibilities.

39. The carriage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET released by the Union 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 13(2)(a) or (b).

40. Information classified RESTREINT UE/EU RESTRICTED may also be carried by postal services or commercial courier services.

41. The carriage of information classified TRES SECRET UE/EU TOP SECRET from within the Union to the territory of a third State shall be by military or diplomatic courier.

VI. DESTRUCTION OF EUCI

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

43. Documents subject to registration in accordance with Article 9(2) 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.

44. For documents classified SECRET UE/EU SECRET or TRÈS 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.

45. 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 10 years and of documents CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET for a period of at least five years.

46. Classified documents, including those classified RESTREINT UE/EU RESTRICTED, shall be destroyed by methods which meet relevant Union 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.

47. The destruction of computer storage media used for EUCI shall be in accordance with paragraph 37 of Annex IV.

48. In the event of an emergency, if there is an imminent risk of unauthorised disclosure EUCI shall be destroyed by the holder in such a way that it cannot be reconstructed in whole or in part. The originator and originating registry shall be informed of the emergency destruction of registered EUCI.

ANNEX IV

PROTECTION OF EUCI HANDLED IN CIS

I. INTRODUCTION

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

2. The following IA properties and concepts are essential for the security and correct functioning of operations on 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 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 treatment shall be to apply a set of security measures which results in a satisfactory balance between user requirements, cost and residual security risk.

7. The specific requirements, scale and the degree of detail determined by the relevant 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 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 Agency and the Member States shall cooperate 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 Union.

15. The dissemination and subsequent implementation of best practice shall help achieve an equivalent level of assurance for the various CIS operated by the Agency and by Member States 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 of such security measures shall be determined following a risk

assessment.

17. The NSA or other competent authority shall ensure that:

(a) cyber defence capabilities are implemented to respond to threats which may transcend organisational and national boundaries; and

(b) responses are coordinated and information about these threats, incidents and the related risk is shared (computer emergency response capabilities).

Principle of minimality and least privilege

18. Only the essential 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;

(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 CAA of a Member State.

26. Prior to being recommended for approval by the ASA in accordance with Article 10(6) of Annex A, 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. The Agency shall approve a security policy on the evaluation and approval of cryptographic products.

27. Where warranted on specific operational grounds, the ASA as appropriate may, upon recommendation by the Agency Security Committee, waive the requirements under paragraphs 25 or 26 of this Annex and grant an interim approval for a specific period in accordance with the procedure laid down in Article 10(6) of Annex A.

28. The Agency, acting upon recommendation by the Agency Security Committee, may accept the evaluation, selection and approval process of cryptographic products of a third State or international organisation and accordingly deem such cryptographic products approved for protecting EUCI released to that third state or international organisation.

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

30. The Agency shall approve a security policy on the qualification and approval of non-cryptographic IT security products.

Transmission within Secured and Administrative Areas

31. Notwithstanding the provisions of this Decision, when transmission of EUCI is confined within Secured Areas or Administrative Areas, unencrypted transmission 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

32. 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.

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

34. 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.

35. 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 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 10, such a connection shall not be deemed to be an interconnection.

36. 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

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

38. Computer storage media shall be reused, downgraded or declassified in accordance with security guidelines to be established pursuant to Article 6(2) of Annex A.

Emergency circumstances

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

40. 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.

41. 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.

42. Should recourse be made to paragraph 39 of this Annex a subsequent report shall be made to the competent authority and to the Agency Security Committee.

III. INFORMATION ASSURANCE FUNCTIONS AND AUTHORITIES

43. The following IA functions shall be established in the Member States and the Agency. 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

44. The IAA shall be responsible for:

(a) developing IA security policies and security guidelines and monitoring their

effectiveness and pertinence;

(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 to IA security policies and security guidelines; and

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

TEMPEST Authority

45. 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

46. The Crypto Approval Authority (CAA) shall be responsible for ensuring that cryptographic products comply with national cryptographic policy or the Agency's cryptographic policy. It shall grant the approval of a cryptographic product to protect EUCI to a defined level of classification in its operational environment. As regards the Member States, the CAA shall in addition be responsible for evaluating cryptographic products.

Crypto Distribution Authority

47. The Crypto Distribution Authority (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

48. 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 ('SSRSs'), security implementation verification documentation and security operating procedures ('SecOPs'), and ensuring that it complies with the Agency'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 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.

49. The Agency SAA shall be responsible for accrediting all CIS operating within the remit of the Agency.

50. The relevant SAA of a Member State shall be responsible for accrediting CIS and components thereof operating within the remit of a Member State.

51. A joint Security Accreditation Board (SAB) shall be responsible for accrediting CIS within the remit of both the Agency 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 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 Agency 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 Agency Security Committee and shall notify all accreditation statements to it.

Information Assurance Operational Authority

52. 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 SSRS including the residual risk statement, the 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; and

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

ANNEX V

INDUSTRIAL SECURITY

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 11 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 Agency.

2. The Agency shall approve guidelines on industrial security outlining in particular detailed requirements regarding 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 a call for tender or letting a classified contract, the Agency, 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 Agency shall prepare an 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 Agency 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 Agency 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 a 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 the 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 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 PSI and may contain additional security requirements.

III. FACILITY SECURITY CLEARANCE (FSC)

8. An FSC shall be granted by the NSA or DSA or any other competent security authority of a Member State 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. It shall be presented to the Agency, as the contracting authority, before a contractor or subcontractor or potential contractor or subcontractor may be provided with or granted access to EUCI.

9. When issuing an FSC, the relevant NSA or DSA shall, as a minimum:

(a) evaluate the integrity of the industrial or other entity;

(b) evaluate ownership, control, or the potential for undue influence that may be considered a security risk;

(c) verify that the industrial or any other entity has established a security system at the facility which covers all appropriate security measures necessary for the protection of information or material classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in accordance with the requirements laid down in this Decision;

(d) verify that the personnel security status of management, owners and employees who are required to have access to information classified CONFIDENTIEL UE/EU

CONFIDENTIAL or SECRET UE/EU SECRET has been established in accordance with the requirements laid down in this Decision; and

(e) verify that the industrial or any other entity has appointed a Facility Security Officer who is responsible to its management for enforcing the security obligations within such an entity.

10. Where relevant, the Agency, 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.

11. The 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.

12. The NSA/DSA or any other competent security authority which has issued an FSC shall notify the Agency as contracting authority about changes affecting the FSC. In the case of a sub-contract, the NSA/DSA or any other competent security authority shall be informed accordingly.

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

IV. CLASSIFIED CONTRACTS AND SUB-CONTRACTS

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

15. Once a classified contract or sub-contract has been awarded, the Agency, 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.

16. When such contracts are terminated, the Agency, 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.

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

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

19. Where the contractor or subcontractor is authorised to retain EUCI after termination 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.

20. The conditions under which the contractor may subcontract shall be defined in the call for

tender and in the contract.

21. A contractor shall obtain permission from the Agency, 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 Union.

22. 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.

23. 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.

V. VISITS IN CONNECTION WITH CLASSIFIED CONTRACTS

24. Where the Agency, contractors' or subcontractors' personnel 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 in liaison with the NSAs/DSAs or any other competent security authority concerned. However, in the context of specific projects, the NSAs/DSAs may also agree on a procedure whereby such visits can be arranged directly.

25. All visitors shall hold an appropriate PSC and have a 'need-to-know' for access to the EUCI related to the Agency contract.

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

VI. TRANSMISSION AND CARRIAGE OF EUCI

27. With regard to the transmission of EUCI by electronic means, the relevant provisions of Article 10 of Annex A and Annex IV shall apply.

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

29. 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. In such cases, personnel handling the consignment shall be security cleared in accordance with Annex 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 NSA/DSAs 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; and

(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 NSA/DSA or any other competent security authority of the States of both the consignor and the consignee.

VII. TRANSFER OF EUCI TO CONTRACTORS LOCATED IN THIRD STATES

30. EUCI shall be transferred to contractors and subcontractors located in third States in accordance with security measures agreed between the Agency, as the contracting authority, and the NSA/DSA of the concerned third State where the contractor is registered.

VIII INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED

31. In liaison, as appropriate, with the NSA/DSA of the Member State, the Agency, as the contracting authority, shall be entitled to conduct inspections of 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.

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

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

34. The Agency, 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.

35. The conditions under which the contractor may subcontract shall be in accordance with paragraph 21 of this Annex.

36. Where a contract involves handling information classified RESTREINT UE/EU RESTRICTED in a CIS operated by a contractor, the Agency as contracting authority shall ensure that the contract or any subcontract 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.

Appendices

Appendix A

Definitions

Appendix B

Equivalence of security classifications

Appendix C

List of national security authorities (NSAs)

Appendix D

List of abbreviations

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;

'Authorisation for access to EUCI' means a decision by the ASA taken on the basis of an assurance given by a competent authority of a Member State that a Agency official, other servant or seconded national expert may, provided his 'need-to-know' has been determined and he has been appropriately briefed on his responsibilities, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date;

'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 Agency 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 Agency 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) — see Article 10(2);

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

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

‘Cryptographic product’ means a product whose primary and main functionality is the provision of security services (confidentiality, integrity, availability, authenticity, non-repudiation) through one or more cryptographic mechanisms;

‘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) — see Article 2(1) of Annex A;

‘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;

‘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’ — see Article 11(1) of Annex A;

‘Information Assurance’ — see Article 10(1) of Annex A;

‘Interconnection’ — see Annex IV, paragraph 32;

‘Management of classified information’ — see Article 9(1) of Annex A;

‘Material’ means any document, data carrier or item of machinery or equipment, either manufactured or in the process of manufacture;

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

‘Personnel security’ — see Article 7(1) of Annex A;

‘Personnel Security Clearance’ (PSC) 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 be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date;

‘Personnel Security Clearance Certificate’ (PSCC) means a certificate issued by a competent authority establishing that an individual is security cleared and holds a valid security clearance certificate or authorisation from the ASA for access to EUCI, 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’ — see Article 8(1) 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’ — see Annex III, paragraph 18;

‘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 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;

‘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;

‘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 PSC or an authorisation for access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above);

‘Security mode of operation’ means the definition of the conditions under which a CIS operates based on the classification of information handled and the clearance levels, formal access approvals, and need-to-know of its users. Four modes of operation exist for handling or transmitting classified information: dedicated mode, system-high mode, compartmented mode and multilevel mode:

—‘Dedicated mode’ means a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, and with a common need-to-know for all of the information handled within the CIS,

—‘System-high mode’ means a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, but not all individuals with access to the CIS have a common need-to-know for the information handled within the CIS; approval to access information may be granted by an individual,

—‘Compartmented mode’ means a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, but not all individuals with access to the CIS have a formal authorisation to access all of the information handled within the CIS; formal authorisation implies a formal central management of access control as distinct from an individual’s discretion to grant access,

—‘Multilevel mode’ means a mode of operation in which not all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, and not all individuals with access to the CIS have a common need-to-know for the information handled within the CIS;

‘Security 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;

‘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. A 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.

Appendix B

EQUIVALENCE OF SECURITY CLASSIFICATIONS

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOM	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgium	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	nota ([1]) below
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Czech Republic	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Denmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germany	Streng geheim	Geheim	VS ([2])— Vertraulich	VS — Nur für den Dienstgebrauch
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ireland	Top Secret	Secret	Confidential	Restricted
Greece	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spain	Secreto	Reservado	Confidencial	Difusión Limitada LIMITADA

France	Très Secret Défense	Secret Défense	Confidentiel Défense	nota (3) below
Croatia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Latvia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lithuania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hungary	'Szigorúan titkos!'	'Titkos!'	'Bizalmas!'	'Korlátozott terjesztésű!'
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Netherlands	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Poland	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Romania	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenia	Strogo tajno	Tajno	Zaupno	Interno
Slovakia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Sweden (5)	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
United Kingdom	UK TOP SECRET	UK SECRET	No equivalent(6)	UK OFFICIAL — SENSITIVE

(1) Diffusion Restreinte/Beperkte Verspreiding is not a security classification in Belgium. Belgium handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

(2) Germany: VS = Verschlusssache.

(3) France does not use the classification 'RESTREINT' in its national system. France handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

(4) Sweden: the security classification markings in the top row are used by the defence authorities and the markings in the bottom row by other authorities.

(5)The UK handles and protects EUCI marked CONFIDENTIEL UE/EU CONFIDENTIAL in accordance with the protective security requirements for UK SECRET.

Appendix C

LIST OF NATIONAL SECURITY AUTHORITIES (NSAs)

BELGIUM Autorité nationale de Sécurité SPF Affaires étrangères, Commerce extérieur et Coopération au Développement 15, rue des Petits Carmes 1000 Bruxelles Tel. Secretariat: +32 25014542 Fax +32 25014596 E-mail: nvo-ans@diplobel.fed.be	**ESTONIA** National Security Authority Department Estonian Ministry of Defence Sakala 1 15094 Tallinn Tel. +372 717 0019, +372 7170117 Fax +372 7170213 E-mail: nsa@mod.gov.ee
BULGARIA State Commission on Information Security 90 Cherkovna Str. 1505 Sofia Tel. +359 29333600 Fax +359 29873750 E-mail: dksi@government.bg Website: www.dksi.bg	**IRELAND** National Security Authority Department of Foreign Affairs 76 - 78 Harcourt Street Dublin 2 Tel. +353 14780822 Fax +353 14082959
CZECH REPUBLIC Národní bezpečnostní úřad (National Security Authority) Na Popelce 2/16 150 06 Praha 56 Tel. +420 257283335 Fax +420 257283110 E-mail: czech.nsa@nbu.cz Website: www.nbu.cz	**GREECE** Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ) Διεύθυνση Ασφαλείας και Αντιπληροφοριών ΣΤΓ 1020 -Χολαργός (Αθήνα) Ελλάδα Τηλ.: +30 2106572045 (ώρες γραφείου) +30 2106572009 (ώρες γραφείου) Φαξ: +30 2106536279 +30 2106577612 Hellenic National Defence General Staff (HNDGS)

	Counter Intelligence and Security Directorate (NSA) 227-231 HOLARGOS STG 1020 ATHENS Tel. +30 2106572045 +30 2106572009 Fax +30 2106536279 +30 2106577612
DENMARK Politiets Efterretningstjeneste (Danish Security Intelligence Service) Klausdalsbrovej 1 2860 Søborg Tel. +45 33148888 Fax +45 33430190 Forsvarets Efterretningstjeneste (Danish Defence Intelligence Service) Kastellet 30 2100 Copenhagen Ø Tel. +45 33325566 Fax +45 33931320	**SPAIN** Autoridad Nacional de Seguridad Oficina Nacional de Seguridad Avenida Padre Huidobro s/n 28023 Madrid Tel. +34 913725000 Fax +34 913725808 E-mail: nsa-sp@areatec.com
GERMANY Bundesministerium des Innern Referat ÖS III 3 Alt-Moabit 101 D D-11014 Berlin Tel. +49 30186810 Fax +49 30186811441 E-mail: oesIII3@bmi.bund.de	**FRANCE** Secrétariat général de la défense et de la sécurité nationale Sous-direction Protection du secret (SGDSN/PSD) 51 Boulevard de la Tour-Maubourg 75700 Paris 07 SP Tel. +33 171758177 Fax +33 171758200
CROATIA Office of the National Security Council Croatian NSA Jurjevska 34 10000 Zagreb Croatia Tel. +385 14681222 Fax +385 14686049 www.uvns.hr	**LUXEMBOURG** Autorité nationale de Sécurité Boîte postale 2379 1023 Luxembourg Tel. +352 24782210 central +352 24782253 direct Fax +352 24782243
ITALY Presidenza del Consiglio dei Ministri D.I.S. - U.C.Se Via di Santa Susanna, 15 00187 Roma Tel. +39 0661174266 Fax +39 064885273	**HUNGARY** Nemzeti Biztonsági Felügyelet (National Security Authority of Hungary) H-1024 Budapest, Szilágyi Erzsébet fasor 11/B Tel. +36 (1) 7952303 Fax +36 (1) 7950344

	Postal address: H-1357 Budapest, PO Box 2 E-mail: nbf@nbf.hu Website: www.nbf.hu
CYPRUS ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ Εθνική Αρχή Ασφάλειας (ΕΑΑ) Υπουργείο Άμυνας Λεωφόρος Εμμανουήλ Ροΐδη 4 1432 Λευκωσία, Κύπρος Τηλέφωνα: +357 22807569, +357 22807643, +357 22807764 Τηλεομοιότυπο: +357 22302351 Ministry of Defence Minister's Military Staff National Security Authority (NSA) 4 Emanuel Roidi street 1432 Nicosia Tel. +357 22807569, +357 22807643, +357 22807764 Fax +357 22302351 E-mail: cynsa@mod.gov.cy	**MALTA** Ministry for Home Affairs and National Security P.O. Box 146 MT-Valletta Tel. +356 21249844 Fax +356 25695321
LATVIA National Security Authority Constitution Protection Bureau of the Republic of Latvia P.O.Box 286 LV-1001 Riga Tel. +371 67025418 Fax +371 67025454 E-mail: ndi@sab.gov.lv	**NETHERLANDS** Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Postbus 20010 2500 EA Den Haag Tel. +31 703204400 Fax +31 703200733 Ministerie van Defensie Beveiligingsautoriteit Postbus 20701 2500 ES Den Haag Tel. +31 703187060 Fax +31 703187522
LITHUANIA Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija (The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority) Gedimino 40/1 LT-01110 Vilnius Tel. +370 706 66701, +370 706 66702	**AUSTRIA** Informationssicherheitskommission Bundeskanzleramt Ballhausplatz 2 1014 Wien Tel. +43 1531152594 Fax +43 1531152615 E-mail: ISK@bka.gv.at

Fax +370 706 66700 E-mail: nsa@vsd.lt	
POLAND Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency) 2A Rakowiecka St. 00-993 Warszawa Tel. +48 225857360 Fax +48 225858509 E-mail: nsa@abw.gov.pl Website: www.abw.gov.pl	**SLOVAKIA** Národný bezpečnostný úrad (National Security Authority) Budatínska 30 P.O. Box 16 850 07 Bratislava Tel. +421 268692314 Fax +421 263824005 Website: www.nbusr.sk
PORTUGAL Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 1300-342 Lisboa Tel. +351 213031710 Fax +351 213031711	**FINLAND** National Security Authority Ministry for Foreign Affairs P.O. Box 453 FI-00023 Government Tel. +358 16055890 Fax +358 916055140 E-mail: NSA@formin.fi
ROMANIA Oficiul Registrului Național al Informațiilor Secrete de Stat (Romanian NSA – ORNISS National Registry Office for Classified Information) Strada Mureș nr. 4 012275 Bucharest Tel. +40 212245830 Fax +40 212240714 E-mail: nsa.romania@nsa.ro Website: www.orniss.ro	**SWEDEN** Utrikesdepartementet (Ministry for Foreign Affairs) UD-RS S 10339 Stockholm Tel. +46 84051000 Fax +46 87231176 E-mail: ud-nsa@foreign.ministry.se
SLOVENIA Urad Vlade RS za varovanje tajnih podatkov Gregorčičeva 27 1000 Ljubljana Tel. +386 14781390 Fax +386 14781399 E-mail: gp.uvtp@gov.si	**UNITED KINGDOM** UK National Security Authority Room 335, 3rd Floor 70 Whitehall London SW1A 2AS Tel. 1: +44 2072765645 Tel. 2: +44 2072765497 Fax +44 2072765651 E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk

Appendix D

LIST OF ABBREVIATIONS

Acronym	Meaning
AQUA	Appropriately Qualified Authority
BPS	Boundary Protection Services
CAA	Crypto Approval Authority
CCTV	Closed Circuit Television
CDA	Crypto Distribution Authority
CFSP	Common Foreign and Security Policy
CIS	Communication and Information Systems handling EUCI
Coreper	Committee of Permanent Representatives
CSDP	Common Security and Defence Policy
DSA	Designated Security Authority
ECSD	European Commission Security Directorate
EUCI	EU Classified Information
EUSR	EU Special Representative
FSC	Facility Security Clearance
GSC	General Secretariat of the Council
IA	Information Assurance
IAA	Information Assurance Authority
IDS	Intrusion Detection System
IT	Information Technology
NSA	National Security Authority
PSC	Personnel Security Clearance
PSCC	Personnel Security Clearance Certificate
PSI	Programme/Project Security Instructions
SAA	Security Accreditation Authority
SAB	Security Accreditation Board
SAL	Security Aspects Letter
SecOPs	Security Operating Procedures
SCG	Security Classification Guide
SSRS	System-Specific Security Requirement Statement

TA	TEMPEST Authority

ANNEX B

SECURITY MANUAL

OF THE AGENCY FOR THE COOPERATION OF ENERGY REGULATORS

4 AWARENESS:

The goal of this manual is to prevent safety and security incidents through awareness and education of Agency staff.

We kindly ask you to read this guide carefully, it might help make your actions in case of an incident predictable to others and better understand the actions of your colleagues.

2 SECURITY CLAUSE:

Agency staff shall treat the information hereafter as internal Agency information. Communication of any this information to third persons to whom this information was not addressed is considered as possible harmful to the interests of the European Institutions.

Agency staff shall inform the Director or the Security Officer (SO) immediately if she/he suspects any disclosure of the information he received in the context any involved project.

3 ART. 17 Staff Regulations:

1. An official shall refrain from any unauthorised disclosure of information received in the line of duty, unless that information has already been made public or is accessible to the public.

2. An official shall continue to be bound by this obligation after leaving the service.

1 INTELLIGENCE SECURITY ADVICE:

In case you are having strong indications or just even a slightly sense that you are or were in contact with a third party acting against the interest of the Agency inform your SO immediately. It does not matter how long this contact was ongoing.

You are **never too late** to inform your SO. Never put yourself or any of your colleagues in danger. Do not abruptly break the contact; wait for further instructions.

ACER
Agency for the Cooperation of Energy Regulators

INDEX

Contents

FOREWORD

This manual describes the safety and security guidelines for the Agency for the Cooperation of Energy Regulators (also addressed as “the Agency”) and any external branch office in a general way. This manual is alike for the entire Agency but holds in certain chapter's specific information related to the local situation, limitations and possibilities, as well as the electronic and physical security measures related to specific ACER departments and not common to all the others. The guidelines hereafter describe the security and safety situation starting with a normal day-to-day situation.

These guidelines are to help to create a working environment as comfortable and secure as possible. For these guidelines to be effective, you must understand a number of concepts about the relationship between the physical design of buildings and event occurrences.

Security and safety situations can differ. They depend on short or longer term events or incidents, environmental or metrological changes, mankind generate threats (demonstrations, attacks) and local political or social circumstances. The assessments of these threats to the Agency result in a risk evaluation that might engender changes in the alert state and have an influence on the normal working and living conditions in the Agency.

The safety and security policy is part of the management of the Agency and is based on legality, transparency, accountability, subsidiarity and proportionality.

> **Legality** indicates the need to stay strictly within the legal framework in executing security functions and the need to conform to the legal requirements. The provisions in the Staff Regulations fully apply, notably its Article 17 on the obligation of staff to exercise discretion with regard to Agency information and its Title VI on disciplinary measures. Finally it means that breaches of security within the responsibility of the Agency have to be dealt with in a manner consistent with Agency policy on disciplinary actions and with its policy on cooperation with Member States in the area of criminal justice.
> **Transparency** indicates the need for clarity regarding all security rules and provisions, for balance between the different services and the different domains (physical security versus information protection etc.) and the need for a consistent and structured security awareness policy. It also defines a need for clear written guidelines for implementing security measures.
> **Accountability** means that responsibilities in the domain of security will be clearly defined. Moreover it indicates the need to test regularly whether these responsibilities have been correctly executed.
> **Subsidiarity and proportionality** mean that security shall be organised on the lowest possible level. It also indicates that security activities shall be limited to only those elements that really need it. And finally it means that security measures shall be proportional to the interests to be protected and to

the actual or potential threat to these interests, allowing for a defence which causes the least possible disruption.

Reference documents

- By analogy Euratom Regulation Number 3 of 31 July 1958
- By analogy Commission Decision of 16 August 2006 C(2006) 3602 (security of information systems)
- By analogy Commission Decision C(94)2129 of 8 September 1994 (Responsibilities of the security office)
- Regulation (EC) No 1049/2001 (public access to documents)
- Regulation (EC) No 45/2001 (regulation on the protection of personal data)
- By analogy Commission Decision C(2006) 1623 establishing a harmonised policy for health and safety at work for all commission staff
- By analogy Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission and Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information
- By analogy Council Decision of 31 March 2011 on the security rules for protecting EU classified information (2011/292/EU)

Alert states

An alert state is a set of security measures intended to provide a specific level of protection to the staff, information, buildings and other assets from any threat and to ensure its operational capacity. These security measures are implemented and discontinued in a general or selective manner, as the threat level increases or decreases.
The Agency applicable alert state is decided by mean of Director's Decision, after consulting the Security Officer and the Local Police Authorities and/or based on their risk assessment.

There are four levels of alert:

WHITE

This is the standard state which holds the basic security and safety measures. See the Chapter 10 for detailed information about this state in the Agency (Standard Procedures).

YELLOW

With the exception of staff responsible for safety and security matters, who will be coordinating appropriate security measures with the host nation authorities, police and emergency services, your professional activities may continue «as usual». Nevertheless we ask for your patience and understanding when you are confronted with any extra measures when accessing the Agency premises, due to additional, more stringent, security checks, including:

- Reinforcement of guards where necessary and ensuring that buildings' security services are sufficiently resourced
- Limiting, where appropriate, the number of access points to building reception areas and/or garages
- Denying access to visitors' vehicles
- Reinforcing access controls: checking valid Agency access passes individually; extra checking of delivery of goods; conducting checks of vehicles and hand luggage of any person and increasing checks on incoming external mail.
- Certain activities might move to alternative times or places.

ORANGE

To better ensure your safety, "business as usual" will be severely curtailed:

- Non-essential activities which may place staff at risk will be postponed or moved to alternative places
- Access to Agency premises will be limited to staff and denied to all visitors
- Opening hours of premises will be restricted and garages closed except to service cars.
- A risk assessment may lead to the evacuation of the building when considered vulnerable.

RED

Depending on the nature and severity of the threat, staff will be given instructions on the actions expected of them and how critical activities are to be maintained whilst respecting the following safety precautions:

- Non-essential activities which may place staff at risk are cancelled
- Risk assessment and safety precautions may prohibit staff from congregating together in large groups
- Access to the Agency premises will be denied to all visitors and deliveries by external contractors will be prohibited
- Garages closed to all cars
- Staff may be evacuated from the premises and buildings considered to be under threat may be temporarily closed.

Sometimes staff might feel these measures as disrupting their day-to-day work live. Nevertheless the intentions of these guidelines are to preventively ensure the safety and security of you and your colleagues working conditions. We ask for your

comprehension when you are confronted with a situation that might not seem directly in line with your understanding of the situation. At the same time we are open to all constructive suggestions to help improve this guide and the work and living conditions in your place of work.

GENERAL INFORMATION YOU SHOULD KNOW

1.1 The Agency

- The Agency official address is:

  Agency for the Cooperation of Energy Regulators
  Reception desk - Floor 12
  Trg republike, 3
  1000 – Ljubljana
  Slovenia

- The Agency general phone number is:

+386 (0) 8 205 34 00

1.2 The Telephone

- The Agency telephone switchboard is manned from **08:30** hours to **17:30** hours on workings days:
- The switchboard is operated by Agency staff.
- **Outside these hours the switchboard is unattended.**

You can still receive incoming phone calls outside office hours, on your direct line.

1.3 Opening hours:

- The guard service is present in the Agency 24 hours 7 days a week
- The **guards open the gates at 7.00**
- The **guards close the gates at 24.00**
- **Guards are always available to open the gate outside opening hours, an intercom is placed on the Agency entrance gate, as an alternative a mobile phone number is located on the same position when the guards are performing routine checks around the Agency premises.**

Closing hours and days:

- The Agency closure dates are published on the Intranet and/or on the Agency Web Site (http://www.acer.europa.eu).. In principle, it is also closed on Saturdays and Sundays, except in exceptional cases.

CONTACT FOR HELP

1.1 During working hours

During working hours you contact your SO (or his/her deputy) or Head of Administration for any Security and safety matter.

1.2 Outside working hours

You shall in case of a security or safety incident outside office hours directly contact the SO (number is published on intranet). In case you directly contact the police or fire brigade if such is needed, do not forget to contact also the SO and the guard at the building entrance in order to enable the correct procedures.

If you call for help report clearly:

- WHO you are;
- WHERE you are (country, city, address, house number, building name, floor).
- WHERE the incident is taking place country, city, address, house number, building name, floor – in case you are not on site anymore.
- WHAT is happening
- Why you call: WHAT help you require
- WHEN you discovered the incident
- HOW many people are involved
- HOW you can be contacted
- SO WHAT do you want to say more…….anything else to report

CONTACTS

1.1 Emergency Meeting Point

Šubičeva ulica in the garden next to the Slovenian Parliament entrance (clearly marked with this sign)

List of staff with First Aid Training

Mr. Christophe CESSON, Mr. Christophe GENCE-CREUX, Mrs. Pia-Johanna Fallstrom-Mujkic, Mrs. Lea SLOKAR, Mrs. Saša BORKO, Mr. Thomas QUERRIOUX, Mr. Sofronis Papageorgiou, Mr. Uros GABRIJEL and Mr. Ernst TREMMEL, Mrs.Pia-Johanna FALLSTROM-MUJKIĆ, Mr. Savvas SAVVIDES, Mr. Stefano BRACCO, Mr. Sebastian SZOTOWSKI, Mrs. Saša BORKO GRGIČ, Ms. Mateja VAVTAR

List of evacuation guides

- Ground floor: please, refer to the guard desk
- First floor: Mr. Uros GABRIJEL and Mr. Ernst TREMMEL
- Second floor: Mrs.Pia-Johanna FALLSTROM-MUJKIĆ, Mr. Savvas SAVVIDES, Mr. Stefano BRACCO.
- Sixth Floor: please refer to Mr. Stefano Bracco
- Tenth Floor: Mr. Sebastian SZOTOWSKI
- 12th Floor: Mrs. Saša BORKO GRGIČ, Ms. Mateja VAVTAR
- 14th Floor: please refer to Mr. Stefano Bracco

Guard Company

The guard company's name is: **Sintal koncern**
The guard company dispatch centre: +386 1 513 01 00
The guard company emergency number: +386 1 513 01 00
The guard company administration phone number: +386 1 513 01 00

Getting external assistance

The police

The police emergency phone number is: **113**
The phone number of the local police station is: +386 01 475 06 00
The local police station is located: Trdinova ulica 10, 1000 Ljubljana
The name of our neighbourhood police man is:
He can be reached:

The fire department

The fire department emergency number is: **112**
The nearest fire department is situated: **Gasilska brigada Ljubljana**
Vojkova cesta 19
1000 Ljubljana

Medical

The medical emergency number is: **112**
The nearest local hospital is: **University Medical Centre Ljubljana**
The address is: **Zaloška 14, Ljubljana, Slovenija**
The phone number is: **+386(1) 522 84 08 and +386(1) 522 84 09**

The nearest local doctor is: **BARSOS-MC** phone: **+386 1 242 0700**

The nearest local pharmacy: **Lekarna Barsos-H** phone: **+386 1 242 87 40**

Internal Agency Organisation

Your SO:

- The Security Officer in the Agency is: **Stefano BRACCO – Tel. 405 or +386 030 291861**
- Please refer to the Agency Intranet web-pages for more information.

Your LSA (Local System Administrator)

- The Local Systems Administrator is:
- The LSA home base is in:
- The LSA phone contact address is:

SAFETY and SECURITY SETUP

1.1 Training

Whenever possible the personnel will be given the opportunity to train themselves to obtain the necessary skills, attend first-aid courses and firefighting training either on their own initiative or by organising them in-house.

New personnel will receive these instructions and instructions on:

- the use of exits and emergency exits
- location and use of fire extinguishers
- location and use of first-aid kits
- how to act in case the building needs to be evacuated

1.2 Relation BCP and Safety and Security

Both the Business Continuity Plans and Security and Safety need planning and analysing.

Safety and security will influence your daily work; it should protect you and create a fine work environment. When the stress on the work environment increases; the security alert states might be increased. At a certain point or because of a sudden event the line of acceptable will be crossed. The Agency will be out of the standard range of measures to be taken, the Business Continuity Plan (BCP) will take over.

The Business Continuity Plan enters in force when the working conditions in the Agency are out of limits. These limits are predefined, see the BCP.

1.3 Some explanation

The first task is to develop an understanding of the Agency to be assessed. You do not need to become an expert in the operation of the Agency, but you must get enough of an understanding on how the Agency operates to appreciate its complexities and nuances. When taking a decision you should give consideration to factors such as hours of operation; lay-out of the Agency, neighbours of the Agency, number and types of visitors; nature of the activities developed; types of services provided (internet, brochures lectures etc…); the competitive nature of the industry; the sensitivity of information in the Agency; the 'corporate' culture in the Agency and the hosting Member State; the perception of risk tolerance; and so on.

What means in this context (useful definitions):

Security:

The word security is derived from the Latin "Se-Cura" and literally translates to "without fear". 'Security' is therefore the state of being secure, or the actions employed to achieve that state, i.e. to be secure is to be without fear of harm.

Security takes into account the actions of people attempting to cause destruction. Security is about the integrity of the building.

Safety:

Safety is the ability to protect against harming events. Safety is about the integrity of the human being.

Probability

The chance, or in some cases, the mathematical certainty that a given event will occur; the ratio of the number of outcomes in an exhaustive set of equally likely outcomes that produce a given event to the total number of possible outcomes.

Threat

An intent of damage or injury; an indication of something impending

Risk

The possibility of loss resulting from a threat, security incident, or event

Cost/Benefit Analysis

A process in planning, related to the decision to commit funds or assets. This is a systematic attempt to measure or analyse the value of all the benefits that accrue from a particular expenditure. Usually, this process involves three steps:

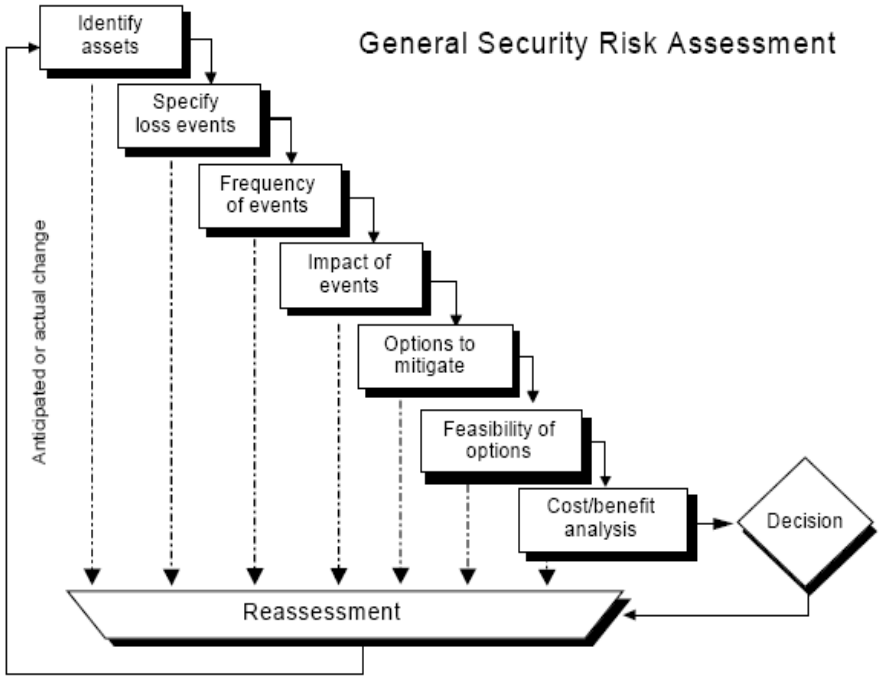
- Identification of all direct and indirect consequences of the expenditure.
- Assignment of a monetary value to all costs and benefits resulting from the expenditure.
- Discounting expected future costs and revenues accruing from the expenditure to express those costs and revenues in current monetary values.

Example: The meeting rooms were designed to receive and meet visitors; consideration of theft is part of the design process; things might get stolen. The investment to protect might exceed the costs invoked by the loss (theft) taking in account the probability of the threat occurring (or even re-occurring). When this balance changes revision of the situation is needed.

Consequential

A secondary result ensuing from an action or decision. From an insurance or security standpoint, costs, loss, or damage beyond the market value of the asset lost or damaged, including other indirect costs.

Chart



The Agency

Safety and security prevention through environmental design is based on the theory that action must be taken to counter the threat before it occurs. Architects, planners, and other security and safety professionals initially focussed on safety, security and prevention in terms of various physical-planning strategies to reduce threat opportunity.

Identifying high risk situations by noting certain factors as weak points as potential targets. The critical job is to identify specific areas concerning physical planning and design that can be responded to and actions can be taken against on the installation. In fact prevention can be built into almost every aspect of community planning.

As a result of these efforts, the following list of design concerns was developed: Building setbacks (front, side, and rear); Wall construction, interior and exterior; Door construction, setbacks and security (including carports, garages); Windows and skylights, setbacks, heights (from ground), show-window displays, and the type of frame or pane; Stairs (stairwells and staircases); Utility boxes; Fences, walls, hedges, screens, setbacks, heights, and louvers; Parking (private); Lighting; Streets, sidewalks, and walkways (locations, slopes, curvature, grades, and the length of a block; Alleys (blind and through alleys); Visibility of valuables (people, safes, and personal) Signs (street signs and signals, traffic signs and signals, and advertising signs); Accessibility; approach, entrance, and exit (pedestrian, vehicular, services,

residential, commercial); Public utilities and easements (gas, water, telephone, and electrical); Public areas and facilities; Street trees and shrubbery.

The Agency has standard two different security areas. These areas are designed in function of their use to maximise comfort when working.

We recognise:

The Public area

This area within the Agency is during normal opening hours free accessible to the public (Public area is identified by the Oval room in the Ground Floor of TR3 Building, the Round room on 14th Floor of TR3 building, the ACER Meeting Rooms in located in the 6th Floor of TR3 Building, kitchen and sanitary facilities which might be shared with other tenants). The Public area has an open informatics network connected to the public World Wide Web network via an isolated ADSL for example. There shall be under no circumstances outlets to the Secure Networks (eg. SNET and S-TESTA of the Agency and/or European Commission. The design and material used in the public area were such to limit safety and security risks.

The Administrative area

The access to this area is restricted to staff working for the Agency. Access to this area is granted on the basis of need to be. This area is only accessible via the SAS (Secure Access System).
The Administrative area is composed by the entire 1st Floor in TR3 Building, the entire 2nd Floor in TR3 Building, the ACER's rented area on 10th Floor in TR3 Building, the ACER's rented area on 12th Floor in TR3 Building.

Besides the offices restricted areas such as the computer room, archives and storages are located in this area. Storages might also be located outside this area in other parts of the building (in the basement and sometimes even outside the Agency) Some kitchen and sanitary facilities might be shared with other tenants; if shared, they are not part of the Administrative area.

This area is not open to any external invited persons.

All invited people must be kept in the Public area.

Access to the Administrative area is granted on the basis of need to be. This area is only accessible via the SAS (Secure Access System).

The safety and security systems

Each area in the Agency has its specific security and safety measures. The periphery of the Agency is protected against manual attacks and blasts. The walls, doors, windows and glass used are specially designed to give protection against aggression during demonstrations or in the event of an explosion. The internal partitioning walls and doors of the Agency have also been designed to assure maximum comfort.

Areas belonging to Head of Units, to the Market Monitoring Department and to the Director have additional sound insulation.

The Agency is further equipped with high quality door and window locking devices, a fire detection system and a closed television surveillance system. The restricted areas have on top an isolated access control system; the area is isolated through adoption of specific doors and walls from any kind of attack and intrusion.

SAS

The SAS is the Agency **S**ecure **A**ccess **S**ystem. It is installed in any floor and in any entrance to the Administrative area. The system is not located in Conference and Public areas. The SAS-doors are a highly protected, aggression proof tool to permit strict access control to the areas behind. **The doors are not attended, it is responsibility of Staff and in case of escorted guests, of accompanying staff, to check the correct closure of doors and to signal any problem to Facility Management and to the SOs in this respect**.

Fire detection

Fire detectors are adapted to the rooms or areas where they are located; they differ in shape and size. The fire detection system is present in all rooms and areas. It is activated 24hours. It will first advise the security staff on entrance floor of an existing problem. Only when the security staff has confirmed the presence of problem or when within a predefined timeframe no action was taken the alarm bell will ring to notify the staff of a problem. As the Agency is a part of a larger building the building wide fire detection system, the system will alarm when a part of the building will be alarmed.

CCTV

The closed circuit television system is setup conform local legislation and regulation 45/2001 (data protection). The system only registers images for safety and security reasons. Cameras are directed and programmed in such a manner that recording of unnecessary images is limited as much as possible. The principle is that images are reordered and stored for maximum 7 days. The images are only accessible to authorised staff (SO and Director).

No guard has access to life images of all cameras.

Access control

The access control is designed to record authorised and un-authorised use of badges on controlled access points. The system is only capable of identifying the place, time and badge used on card readers. It does not record the reason of presenting the badge to the reader. The owner, the person to whom the badge was issued (not always the holder) of the badge is responsible for the use of the badge. The system is capable of linking the badge identifier to the name of the owner of the card. Cards are to be used strictly personal. The system is designed to operate with

the limits of regulation 45/2001 (data protection). Data is only accessible to authorised staff.

Theft or lose of cards should be reported immediately to the Security Officer via E-Mail or phone call.

An access card is like a key, it gives the right to pass a controlled point. Sometimes access is only given when a card and a code is given. This is programmable per access point or in function of day-time (outside office hours for example).

The advantage of an access control system to a key is that it can be activated and de-activate in function of needs. When a key is lost the lock (or locks in case of a master key) must be replaced and all distributed keys must be replaced.

Keys

The Agency has high security window and door locking devices and cylinder locks installed on the perimeter windows and doors as well as in certain internal security doors. Other doors, like the office doors are equipped with good quality cylinder locks. A copy of these keys is kept in the key-cupboard in the Facility Manager room. **There are also master keys present in the Agency; these master keys shall never leave the Agency premises. They exist for emergency reasons only. You can find the master keys with the Security Officer.**

X-Ray

The Agency has at least one X-ray machine to check daily incoming mail and to control visitor's personal belongings during events that request an increased security level during or an increased security alert state.

Firefighting equipment

The Agency has fire blankets and fire extinguishers. The fire extinguishers are normally located near emergency exits and at least one at each floor within 30 meters distance from any point in the Agency on the floor. The standard fire extinguisher is a water-foam based type. You can use this extinguisher on all normal fires in the Agency. There are also CO^2 extinguishers in the Agency, their time of use is extremely short and the effect is limited if not used properly. Careful: do not use the CO^2 extinguisher on a person on fire, you can provoke cold burns with the CO^2. All fire extinguishers need to be tested at least once each year. A sticker indicates the last test date and / or next testing date.

The Agency has also fire-hoses. The vain of the fire hose shall only be opened when the hose was first completely unrolled. Careful: the water comes out under high to very high pressure. They should be used by trained personnel.

Fire and Panic buttons

- Emergency fire alert buttons are located near emergency exits. The idea is that in case of a fire you direct yourself to the emergency exit. There you can push the alert button and take an extinguisher in case you decide you can still control the fire.

- Emergency exit buttons are installed to release doors that normally should remain closed. They cut the power on the locking devices or mechanically override the locking device.

AED and FIRST AID

The Agency shall have an Automatic External Defibrillator. The AED shall be strategically installed, accessible from all point in the Agency. For example near the SAS on the public area side.

The First Aid kit shall also be wall mounted near the AED.

The Agency should provide the AED machine(s) within 18 months from entry into force of this "ACER Security Manual" subject to budget availability.

Systems Management

The security systems are maintained at least once per year or more often, if required by Slovene national legislation. The systems are managed by the Security Officer. He has access to the core of all systems and is capable of having the system programmed as requested.

You must inform the SO immediately of theft or loss of an access card of the access control system. The system operation codes shall be changed on a regular basis at least each time a member of staff leaves the Agency.

The SO can provide you with the necessary codes to manipulate security systems if and when you are authorised to do so.

The Facility Manager manages the keys in the Agency. Keys for the offices or for other rooms, can be requested to Facility Manager. Only keys for File Cabinets and drawers can be found in the office. A passe-partout can be requested and granted on request, after justifying the need. Facility manager will keep records of date, time and to whom keys have been provided and date and time of when they are returned to the Facility Manager. The SO must be able to have access to the register in order to perform his duties.

Harmonised policy for health and safety at work

Given the large number of locations of UE linked workplaces and their wide geographical spread both within and outside the Union, it is important that the

Commission's health and safety policy be harmonised and applied by analogy in a way that is suited to Agency's locations, for the benefit of all staff.

While local health and safety requirements may vary from country to country, it is the Commission's objective - based on a preventive approach - to attain a high level of protection everywhere, i.e. one which is at least as high as, and in many cases higher than, what is required by national law.

As an employer, the Agency is responsible for the health and safety of all staff and must implement an appropriate policy to protect them. The powers of the Agency in the area of the health and safety policy are delegated.

Since the Protocol on Privileges and Immunities exempts the Agency from being subject to the controlling authorities of the host country, this absence of external control has to be compensated for by the Agency's own internal control and audit scheme. The Directorate-General for HR of the European Commission is therefore also authorised to carry out additional health and safety checks and audits as and when necessary.

TASKS OF THE GUARDS

The guards in the Agency are unarmed. They assure the surveillance and access control of the Agency. The Agency has guards and receptionists (12th Floor). Their duties are different.

1.1 The Guard Company

The contracted guarding company does provide guarding to the building hosting the Agency.
Please, be aware that the guards on the ground floor are contracted by the landlord and not by the Agency.

The guard company will also assist staff during a crisis situation. With the exception of extreme urgency (fire or pursuit) the guard company will not enter the Agency outside office hours without the prior authorisation or in the presence of a member of staff (SO, Director or Head of Administration).

1.2 The guards

Often the guard is for a visitor the first contact with the Agency. The guard's uniform and his attitude shall be above reproach. The guard shall be discrete, courteous and helpful.

In the morning the guards will make an opening round in the Agency. In the evening the guards will make a closing round

The guard's position is next to the entrance of the 12th Fl., eventually in the guard room (located in K1). In the guard room some security systems can be controlled.

The guard shall primarily perform surveillance and access control tasks and alert designated staff of unusual situations. The guard will assist staff during an intervention, though this is not his first duty. He will only leave this room after having called for assistance.

Further:

- The guards had First-Aid training. They shall perform assistance in this context.
- The guards will assist in cases of emergency. He will help staff during an evacuation of the building. He will keep trace of the persons in the building that might need help during an evacuation (disabled persons, elderly persons or pregnant women). In case of an evacuation he will always keep eyesight on the building entrance. He will assist the SO counting staff evacuating the building and report about the situation to public forces (medical assistance fire-department or police)
- The guards will keep trace of the keys.

1.3 The receptionist

The receptionist's task is to survey and to guide visitors. He/she will actively intervene and interact with visitors. He/she is normally positioned on the 12th floor in the Agency's premises next to the elevators.

The Security systems and physical security

Prevention and protection are the two primary concerns of physical security. Physical security must integrate various capabilities; it must address an expanded range of threats that embraces not only traditional threat components but also non-traditional threats generated by natural or man-made disasters. Physical security is a central component of protection and provides an integrated venue to support for well-functioning of the representation.

Physical security is defined as that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard against espionage, sabotage, damage, and theft.

An overall site-security system is comprised of three major sub-elements detection, delay, and response. The detection sub-element includes intrusion detection, assessment, and entry control.

An electronic security system consists of sensors interfaced with electronic entry-control devices, CCTV, and security lighting. The situation is assessed by using CCTV. Digital and analogue data are transmitted from the detection devices, interior and exterior locations, to the security system for processing. Reliability and accuracy are important functional requirements of the cabling of the data-transmission system.

The response time is defined as the time it takes the security force to arrive at the scene after an initial alarm is received at the security centre. The total delay time is defined as the sum of all of the barriers' delay times, the time required to cross the areas between barriers after an intrusion alarm has been reported by the local guard, and the time required accomplishing the mission and leaving the protected area. An electronic security system basic function is to notify security personnel that an intruder is attempting to penetrate, or has penetrated, a protected area in sufficient time to allow the response force to intercept and apprehend him. To accomplish this, there must be sufficient physical delay between the point where the intruder is first detected and his objective. This provides delay time equal to or greater than the response time

Security and safety systems shall only be operated by trained staff.

1.4 The X-RAY machine

The Agency should provide an X-Ray machine within 18 months from entry into force of this "ACER Security Manual" subject to budget availability. The X-ray machine is maintained as prescribed by it's manufactory. It is tested at least once a year or more often if local legislation prescribes, on leaking of x-rays.

The X-ray machine shall **only** be operated by duly trained security staff. The machine shall be used to screen all incoming post.

Following instructions of the SO the guards will also use the X-ray machine to screen bags and other personal belongings of visitors and of staff in an increased alert state.

1.5 The CCTV system

The life images of the CCTV will be available to the SO in the IDF room.

The CCTV uses cameras that automatically switch the sensitivity between daytime and night-time recording. The CCTV is a digital system that records digitally the images.

Only the LSA, the IT Team, the Facility Manager, the SO or his deputy have access to the central system located in the IDF rooms of the Agency.

1.6 The access control system

The access control system is located in the computer room.

Agency officials have 24 hour access to the office areas. Further access is granted on the basis of need to be and following an internal decided timetable.

Only the LSA, , the IT Team, the Facility Manager, the SO or his deputy have access to the central system located in the computer room of the Agency.

OUTSIDE OFFICE HOURS INCIDENTS

Duty officer

The Agency will setup a duty roster of members of staff that will be contacted by the guard company outside office hours in case of the reception of an alarm by the guard company.

The SO will transmit the list and roster of duty officers to the guard company. Monthly this list will be verified by the SO and its accuracy will be checked by the guard company.

The hand-over between the duties officers will take place on Friday noon .

Outside office hours event

In case of an alarm received by the central desk, the Guard Company will inform the Agency duty officer of the nature of the incident / alarm. The duty officer will take a decision about interventions to be made by the guard company in case of an event.

In case the duty officer decides an intervention on site is necessary. The guarding contract provides an intervention service of at least two hours on site in case any emergency (during or outside office hours). After these two hours the duty officer will order if necessary extra services.

The guard company will not enter the Agency on its own initiative. The duty-officer will not enter the Agency alone. The duty-officer will wait for the guard service to be present. Entering the Agency after an alarm will only take place when more then one person is present. The deputy duty officer will follow up and be ready to act in case intervention delays are passed. The deputy duty officer will alert the police if delays are exceeded.

Presence in the Agency outside office hours

With the exception of opening and closing of the Agency by the guards **only staff is allowed to enter the Agency outside office hours**.

Staff will enlist in the register present near the main entrance with their name, date and entry time. When leaving the Agency staff will also indicate this time.

INCIDENTS

Staff working the in the Agency will be informed during regular briefings of general and specific Agency related risks.

1.1 Security threats to the Agency and its staff are:

- Verbal aggression
- Sabotage
- Drunken people
- Theft
- Manual attack aggression
- Breaking and climbing in
- Armed attack aggression
- Political and economical espionage
- Bombs

Safety threats to the Agency and its staff are:

- Fire
- Flooding
- Explosion
- Earthquake
- Air pollution
- Water pollution

Social threats to the Agency and its staff are:

- Demonstration
- Hunger strike in the Agency
- Occupation of the Agency
    - Non-violent by one person
    - By more persons and or non-peaceful

Technical threats to the Agency and its staff are:

- Failure of electricity supply
- Flooding, rupture of a conduct
- Failure of means of communication
- Failure in the structure of the building

In all cases staff is requested to follow the instructions given by the Director, Head of Administration or Security Officer.

The Alert state may be increased. The business continuity plan might be turned into in force.

EVACUATION

1.1 Evacuation guides

Each floor shall have at least one person designated to make one round on the floor before going to the meeting point. She/he shall report the situation on his floor to the Head of Administration or SO. (E.g. not all persons evacuated, disabled persons etc)

1.2 Evacuation instructions

KEEP CALM AND STRICTLY FOLLOW INSTRUCTIONS

There are several reasons for evacuation and resulting types of evacuation. Some are urgent some are less urgent.

The Agency has emergency routes. They are indicated on the floor plans that are displayed on each floor. **Familiarise yourself with these routes**.

The word emergency route is used since the routes use is two-fold:

1. To provide staff a route to a safe area, sometimes inside but often outside the Agency.
2. To provide the police and fire brigade a safe route inwards the Agency to come and assist you.

PLEASE KEEP THE EMERGENCY ROUTE DOORS CLOSED AND FREE FROM ANY OBSTACLE THEY MIGHT SAVE YOUR OR YOUR COLLEAGUE'S LIFE.

1.3 What is an evacuation route

An emergency route has fire resistant walls and doors that will protect you from a fire during a limited time (often about 60 minutes). Further the emergency routes have double entrance doors preventing smoke from entering in the route.

Once you enter in the emergency route stay calm and leave the emergency route at the exit do NOT enter at other floor levels, you do not know the situation behind the door.

Next to the emergency route entrance door you will find a fire extinguisher and or a fire alarm bell. In case of a fire and when you decide to evacuate make sure you push the fire alarm button.

1.4 Evacuation route standards

Following the normalisation standards there are two types of emergency exit doors in the Agency. Both lead into an emergency route to a safe area. The first type is the normal emergency exit door; in case of an emergency we do not expect panic in front of this door. These doors seem to have standard door opening devices; they are normally located in the Administrative where people are familiar with the situation. The second type of doors is where the possibility exists to have panic in front of the door; these doors are located in the public; people are not familiar with the situation. These doors are equipped with special opening devices, in particular with specific opening keys. Due to the particular nature of the building, the doors are re-enforced and need a specific key to be opened. The key is located next to the door. If a security door is an Emergency door, the key is located already next to the door on the emergency route.

There are also standards for:

- Pictograms that are often green (sometimes illuminated) signs
  - Indicating directions,
  - Indicating the exit
- Lights:
  - the emergency route lighting (1 lux minimum on the ground),
  - anti-panic lighting (0,5 lux horizontal),
  - workplaces with an increased safety risk.

The Meeting point

The meeting point is a place out of sight of the building in Šubičeva ulica in the garden next to the Slovenian Parliament entrance. It will be at least 300 meters distance of the building. You will go to the meeting point in case of a short term evacuation unless instructed differently.

Fire evacuation

In case of a fire the guard will be alerted by the fire detection system. Staff has also the possibility to alert the guard by using alert buttons present on the floors. Buttons are located in the public area.

A member of staff may attempt extinguishing a fire when the fire is small and controllable:

1. *after having alerted the guards,*
2. *having informed colleagues,*
3. *in the presence of another member of staff,*

The guard will confirm that there is a fire before sounding the evacuation bell. In case the evacuation bell is sounded staff will **immediately cease all activities and leave immediately the Agency**. You close but do not lock your office door. In case EU-

restricted information is handled, this shall be put back in the cupboard that will be locked or it shall be taken along concealed in a cover.

ALL STAFF and their visitors SHALL GATHER AT THE MEETING POINT.

A head count shall be performed. The Director, HoA or SO shall liaise with the firemen and policemen. You shall only re-join the building after authorisation by the police or firemen.

Bomb threat evacuation

In case a bomb threat was received or suspected object was discovered the Agency will be evacuated. See also items at chapter 17.19.

In a bomb threat situation do not touch anything, stop using your mobile phone and switch it off till you are at the meeting point. Do not use any radio-transmitting devices.

In case the evacuation bell is sounded you should immediately cease all work and go to the meeting point. You close but do not lock your office door. Though this is an urgent evacuation please have a look around you on your way out of the building and report at the meeting any abnormalities you might have observed.

In case the guard or member of staff makes a round through the building you will be asked to search your office without touching anything, leave your office observing all objects on your route out of the building and report any abnormalities at the meeting point.

Threat in the vicinity evacuation

In case of a threat of any kind in the vicinity of the Agency premises, the Director, HoA or SO can decide to evacuate the Agency.

This evacuation can be done by ringing the evacuation bell or by the guard or member of staff making a round through the building.

In case the evacuation bell is sounded you should immediately cease all work and go to the meeting point. You close but do not lock your office door.
In case the guard or member of staff the informed you, you will follow his instructions.

If you are instructed to evacuate via a particular route **(in particular you may be asked to leave the building using routes on the back of the building at K1)**, do so. The other routes might be obstructed!

After the evacuation

In all cases you will go to the meeting point and wait for further instructions. If there is a change in the meeting point, it will be communicated when leaving the building and you will be instructed how to reach the new point.

Long term evacuation

In case the evacuation is likely to take a longer period the Director, HoA or SO might decide to activate the Business Continuity Plan.

STANDARD PROCEDURES

There are seven main safety and security procedures

1. VIP's
2. The Agency opening procedure
3. The Agency closing procedure
4. The entrance surveillance procedures
5. Disrupting events procedures inside the Agency
    a. Security incidents in the Agency
    b. Safety incidents in the Agency
6. Disrupting events procedures outside the Agency
    a. Security incidents around the Agency
    b. Safety incidents around the Agency
7. Treatment of EUCI

1.1 VIP's

Staff organising activities inviting VIP's shall also inform the Director and SO who will inform the guard service of their presence.

In case of bigger events it is advised to inform also the Local Police Office. In this case, please, take the time to inform in due time the SO.

The 24 hours permanence service of the Security Office in Brussels can always be contacted in case of problems. They are also aware of travel schedules of commissioners.

Often the presence of the Commissioner or the President does require some special security arrangement. For practical reasons it is advisable to extend guard services during his stay in the Agency. Some members of the Commission have close protection; the Agency will be informed of any extra needs through the cabinet of the Commissioner.

1.2 The Agency opening procedure

What

Aggressors often use a vehicle, parked insight at some distance of the point of attack. A vehicle with a driver and a running engine is a typical 'get away' car. Aggressions on persons often take place in badly illuminated, calm and out of sight areas. A manual attack on the Agency often leaves traces.

The first person to arrive at the Agency, early in the morning at dawn when the streets are still calm is a relatively easy target. He has the access badge and eventually necessary code to unlock the Agency.

To do

Often the staff will be the first to enter and open the Agency; guards shall make an outside round before entering the premises. They will be vigilant and look for any traces of attempts to enter the Agency. It is not always easy to see the difference between simple vandalism and attempts to break in. In case he detects such traces, he will immediately inform his dispatch centre. The dispatch centre will send help and inform the duty officer week if outise office hours, the SO in all other cases.

Before opening the Agency he will look around for any suspicious person(s). **He will not open the Agency when he is in the presence of an unknown third person.**

The guard will close the main entrance after entering. He will then make an internal round in the building or in the floor. He will check the building surveillance systems.

At the normal opening hours on work days, the staff will unlock the public area for visitors at the foreseen time.

Incident

- In case the first person to arrive discovers traces of manual attack (breaking in) on the Agency premises (doors and windows), **he will not enter and call the police, SO, Guard Company and the duty officer. Do not touch anything, avoid destroying traces.**

  Staff is requested not to enter the Agency before the arrival of the Police. Staff will only enter when there is a guarantee no danger exists anymore and all traces have been examined by the police.

- In case the first person to arrive at the Agency is attacked just before opening the Agency he shall collaborate with the aggressors.

You will not take any initiative and strictly do what is asked from you.

Observe, listen try to remember details for recognition of subjects afterwards.

The Agency closing procedure

What

Quite some robberies or climbing-in are the result of opportunities created when not properly leaving the property; like windows not closed or rear doors and sometimes even front doors forgotten and left unlocked.

Armed aggression on the last person closing off the premises at dusk often happens when the person is alone.

To do

The last Staff Member on the floor finishing his duty in the evening will make a closing round.

A common advice to staff is to avoid working alone in the Agency. If possible staff should in such case preferably continue to work from home using the teleworking facilities.

Incident

- In case you are alone and you hear suspicious voices or noises do not be the hero. Call from your office for help, a colleague or the guard at the entrance hall for assistance. Do not make an intervention on your own without out informing somebody. If you decide to go for a search, agree with the party you called on a time that you will call back to make sure they will call for help if anything happens.
- In case you are aggressed when closing the Agency, and you are forced to go in again, or in case you are hijacked:
    - Do not take any initiative and strictly do what is asked from you.
    - Observe, listen try to remember details for recognition of subjects afterwards.

The entrance surveillance procedures

The Public area is part of the Agency. This area is clearly separated from the Administrative area of the Agency.

The public area

The Agency public area is freely accessible to the public during the opening hours. The guard and receptionists (may be staff members) keep an eye on the public circulating in these areas. These areas are under camera surveillance. The presence of the CCTV is clearly indicated near every entrance.

The public areas shall be kept free of supply boxes and other objects where bombs could easily be hided. The setup of the public area is design such that the receptionist and guard shall have an easy view over the public and the area.

The administrative area

The Administrative area is located behind the SAS (Secure Access System). This highly protected interlocking door system provides a secure way of controlling access to the Administrative area.

Only the SAS shall be used to enter the Administrative area.

Alternative access ad exit points via controlled emergency exit doors are only permitted for staff and this only during security state WHITE. The alternative entry and exit routes shall also be avoided during demonstration or other activities in the vicinity of the Agency.

Visitors shall always enter and leave the Administrative area via the SAS, main entrance. Visitors shall never be guided by staff through the alternative access points, with the exception of an emergency evacuation.

Staff Access

Staff and other EU-officials shall use and dress their access badges to enter and leave the Agency.

Staff shall visibly wear their service badge

Visitors

- Visitors shall be enlisted at the security reception on the 12th Floor. (Date of entry, name, first name and person visited)
- Visitors shall receive a visitor tag with a printed number.
- The time of entry is noted.
- The visitor identify shall be verified against and official ID-document.
- The time of leaving shall be noted

- The visitor tag badge shall be returned at the security reception desk which will take care to destroy the tag after use and to annotate the time of exit

Contractor, Maintenance and Cleaning staff

This is staff which regularly returns to the Agency premises to execute contracted work.
Their personal badge shall be programmed such that they can execute their contracted work.

- Contractor, maintenance and cleaning staff shall be enlisted at the security reception. (Date of entry, name, first name and company name)
- Contractor, maintenance and cleaning staff shall receive their personal badge that is kept at the security reception desk.
- The time of entry is noted
- Contractor, maintenance and cleaning staff identify shall be verified against and official ID-document in case the guard does not know the person.
- The time of leaving shall be noted
- Contractor, maintenance and cleaning staff shall return their badge at the security reception desk, they shall not leave the Agency with the badge.

Disrupting events procedures inside the Agency

In case any local or international VIP's are present the local authorities, the SO will be informed immediately. The SO together with the local authorities will take all the necessary steps.

The goal of the security and safety instructions are to discourage people of acting against the Agency. The objective is to avoid active interventions by the application of the security and safety measures that are mainly preventive. The application of the security and safety rules will create an atmosphere of active protection.

Security incidents in the Agency

In the public area

Security incidents in the public area are often created by one person or a group of persons seeking publicity or attention. It is rare that these

people act violent, though it may not be excluded that a situation can develop in a violent situation.

A hunger strike or occupations of public meeting rooms are the most common events.

Remain calm. The first contact, listening and communication are important. Collect as much as possible information about the person(s) and the objectives. Do not act against the objective of the person(s). Collaborate with you own agenda in mind. Try to come to a common acceptable agreement. Remain neutral and do not take position. Create a situation of confidence.

- Inform the Director, Head of Administration or SO as soon as possible.
- Inform local authorities about the event, in case the situation is not violent avoid having police cars other actions that might attack attention to the case.
- Have the CCTV system in the public area register in continuous mode. Inform the person(s) in the information centre about this.

The guard will remain in the security reception area, and observe the situation and coordinate assistance with the guard dispatch centre and police. The guard will not leave his post to avoid to get mixed up in the situation and not being able to contact help forces anymore.

Do not invite the person or delegation of the group into the Administrative area of the Agency; use a meeting room in the public area for contacts.

A solution can be not to intervene, to give the person or group of persons free access to the public area and negotiate that they only occupy during opening hours. This has be done before and resulted in a satisfactory situation that was resolved in a couple of days.

In the Administrative area

If the internal security and safety rules are applied such a situation should not take place. An exception would be a visitor turning out to have a different agenda after all. An attack on the Agency with intrusion would be another possible situation.

In case of a security incident inside the Administrative area: **Clean your desk immediately. Put your paper work in your cupboard and switch off your computer. Remain calm, listen and communicate.**

Do not act unexpected provoking a reaction of fear by the aggressor. Try to call / get discretely assistance. In case the aggressor has a handheld weapon (gun, knife or other) do not resist.

The guard will remain in the security reception area, and observe the situation and coordinate assistance with the guard dispatch centre and police.

SO shall be informed immediately of such a situation, by a staff member or the guard.

In general

Wherever in the Agency; in case of a violent action or event that disrupts the function of the Agency (like an explosion) European Commission Headquarters will be informed immediately and all necessary preventive actions will be taken.

Instructions will be given by the Director, Head of Administration or SO who will liaise with the EC Head-Quarters.

Safety incidents in the Agency

In the public area

A safety and security incident in the public area could be something like a flooding, fire, a person getting hurt by an object in the public area, explosion or a bomb alert situation.

- When the Agency receives a bomb alert, or a fire takes place the standard procedures will be applied see point 0 above

  The visitors of the public area will be guided out of the Agency by the SO or by the Staff Members.

  The guard will remain in the security reception area, and observe the situation and coordinate assistance with the guard dispatch centre and police.

- When a person gets ill or hurt himself in the Agency the guard will alert staff with First Aid training. The receptionist will create a free space around the person in need of help.

  The guard will call for assistance, ambulance if necessary

- In case of a flooding or other Agency infrastructure related event, like a electrical supply or short circuit problem the maintenance company and landlord in case the building is leased) will be contacted and informed about the situation.

In the Administrative area

A safety and security incident in the public area could be something like fire, a person getting hurt by an object in the public area, explosion or a bomb alert situation.

- When the Agency receives a bomb alert, or a fire takes place the standard procedures will be applied see point 0 above

  The visitors of the public area will be guided out of the Agency by the Staff which is present in any event.

  The guard will remain in the security reception area, and observe the situation and coordinate assistance with the guard dispatch centre and police.

- When a person gets ill or hurt himself in the Agency the guard will alert staff with First Aid training.

  The guard will call for assistance, ambulance if necessary

In general

Wherever near the Agency, in case an event takes place that disrupts the function of the Agency, SO, HoA and Director will be informed immediately and all necessary preventive actions will be taken.

Instructions will be given by the Director, Head of Administration or SO.

Disrupting events procedures outside in the vicinity of the Agency

The visible implementation of security and safety measures will create an impression of active protection. The goal of the security and safety instructions are to discourage people of acting against the Agency. The objective is to avoid active interventions by the use of the security and safety measures that are mainly preventive.

Events happening outside the Agency can have an overwhelming effect and disrupt seriously the functioning of the Agency. In these cases the Business Continuity Plan might become in force.

Security incidents around the Agency

Security incidents outside are often man created. The Agency can be the target but although it is not necessary that the Agency is targeted the Agency could suffer from collateral effects.

Demonstrations are the most common events that take place outside an Agency. Sometimes the demonstrations are spontaneous and not announced; sometime they are announced.

Due to the proximity with the Slovenian Parliament, the local police station will in all cases immediately be informed about the manifestation taking place, they can prepare for if needed and keep a distant eye on the demonstration. Interventions or help will be requested if needed only.

Contact with the demonstrators will only take place via a spokesman or small group of representatives.

In case of a protest action outside the Agency:

1. The meeting rooms public access will be closed.
2. Staff will be informed of the event outside and requested to close windows and not to go near the windows at the building side of the demonstration.
3. Staff will be informed that in case they get in contact with the demonstrators not to provoke and to listen.
4. In case of a conference that is ongoing participants may be request to stay inside or to evacuate through an alternative exit.

Safety incidents around the Agency

Safety incidents outside can be of various natures, for example: meteorological, environmental or man created.

These incidents are rarely targeting the Agency only.

Events without prior notice:

Sometimes, like in cases of a big fire or large explosion with toxic smoke in the neighbourhood; the public forces will provide instructions like closing the windows or to evacuate the area.
Try to listen to the local radio station.

Events with prior notice:

In other cases, like the dismantling of a bomb, the area might be temporarily evacuated. This is often well in advanced notified to the local inhabitants.

Long term rain or earthquakes might seriously influence the functioning of the Agency. In case of flooding by rain the fire department shall be called for help, when necessary. The landlord shall be informed and asked for help.

Treatment of EUCI

The Agency is not equipped to handle European Union Classified Information (EUCI) of a higher level then RESTREINT UE/EU RESTRICTED.

For the handling of any EUCI and also RESTREINT UE/EU RESTRICTED see the security notices available at the security website.

The need-to-know principle applies to all EUCI and thus overlooking of documents by people (also colleagues) to whom the document was not addressed shall be prevented.

The RESTREINT UE/EU RESTRICTED documents shall be destructed in special crosscut shredders.

WHAT TO DO IN CASE OF:

1.1 Theft

Prevention is the key word. Staff working in the Public area of the Agency shall have an office in the administrative area. They should not take more than the strict necessary personal belongs with them when working the public area.

In the Administrative area "clean desk" should be the principle. You should never leave personal belongings or material with value open and insight in your office. Lock them in your cupboard when you leave your office.

When you were subject of a theft in the office inform your Director or Head of Administration. When you were subject of theft outside the office make a police declaration. Certain incidental evidence or re-occurrence of theft in an area might lead to the actor and you might thus help other to become victim of the thief.

Harassment

When you feel harassed speak about it with somebody you can take in confidence, your Director or Head of Administration. Do not stay alone with your feelings.

The Agency has Confidential Counsellors who are available to speak and support the staff in case of psychological and sexual harassment.

In case you feel you need help and you cannot find this in the Agency, have a look at the Administrative webpage for assistance in case of harassment.

Espionage

When you feel that you are being overlooked or overheard, please contact your SO, Director or Head of Administration. Continue acting as before and wait for further instruction. Do not speak with colleagues about your experience.

Be aware of people that seek contact with you or that previously had no interest and that suddenly become very friendly. Electronic files, like postcards or other files, which you receive via email from third persons, can be contaminated with executable files that via a "trigger" might started transmitting information you have stored in your files. This does not necessarily happen at work, it could also be the case at home.

Telephone threat

When receiving a telephonic threat, treat the call seriously. Often, an anonymous telephone call is made regarding a bomb or an IED. When an anonymous warning or threat is received, notify the SO and Director. A decision will be made to contact the police, SO, the guard dispatch centre for assistance immediately. The SO will determine subsequent actions. Immediate action may include a search without evacuation, the movement of personnel within the establishment, a partial evacuation, or a total evacuation.

The following criteria helps determine what immediate action to take:

- Factors favouring a search before the movement of personnel:—
    - There is a high incidence of hoax telephone threats.
    - Effective security arrangements have been established.
    - Information in the warning is imprecise or incorrect.
    - The caller sounded intoxicated, amused, or very young.
    - The prevailing threat of terrorist activity is low.
- Factors favouring movement of personnel before searching:
    - The Agency had already a serious bomb threat in the recent past.
    - Information in the warning is precise as to the matters of location, a description of the device, the timing, and the motive for the attack.
    - A prevailing threat of terrorist activity is high.

THE PPI

The Maastricht Treaty (formally, the Treaty on European Union, TEU) was signed on February 7, 1992 in Maastricht, the Netherlands after final negotiations on December

9, 1991 between the members of the European Community and entered into force on November 1, 1993 during the Delors' Commission. It led to the creation of the European Union. The seventh protocol of this treaty is the PPI.

1.1 Protocol Privileges and Immunities (Does apply to the Agency*)*

Article 1

The premises and buildings of the Union shall be inviolable. They shall be exempt from search, requisition, confiscation or expropriation. The property and assets of the Union shall not be the subject of any administrative or legal measure of constraint without the authorisation of the Court of Justice.

Article 2

The archives of the Union shall be inviolable.

GENERAL PROVISIONS

Article 17

Privileges, immunities and facilities shall be accorded to officials and other servants of the Union solely in the interests of the Union.
Each institution of the Union shall be required to waive the immunity accorded to an official or other servant wherever that institution considers that the waiver of such immunity is not contrary to the interests of the Union.

Article 18

The institutions of the Union shall, for the purpose of applying this Protocol, cooperate with the responsible authorities of the Member States concerned.

The Vienna Convention (Partially applicable to the Agency)

The Vienna Conventions on Diplomatic Relations is an international treaty on diplomatic intercourse and the privileges and immunities of a diplomatic mission. Adopted on April 18, 1961 by the United Nations Conference on Diplomatic Intercourse and Immunities

Diplomatic immunity is a form of legal immunity and a policy held between governments, which ensures that diplomats are given safe passage and are considered not susceptible to lawsuit or prosecution under the host country's laws (although they can be expelled). It was agreed as international law in the Vienna Convention on Diplomatic Relations (1961), though the concept and custom have a much longer history. Many principles of diplomatic immunity are now considered to be customary law. Diplomatic immunity as an institution developed to allow for the maintenance of government relations, including during periods of difficulties and even armed conflict. When receiving diplomats—formally, representatives of the sovereign (head of state)—the receiving head of state grants certain privileges and immunities

to ensure that they may effectively carry out their duties, on the understanding that these will be provided on a reciprocal basis.

Access to the Agency

In case the national authorities require access to the Agency, during office hours the first contact will be the SO or duty officer outside office hours; they shall be requested to wait in the public area. The Director and Head of Administration shall be immediately informed. European Commission Head Quarters (DG-ENER) shall be contracted, outside office hours the 24hours dispatch centre of the Security office shall be contacted. The warrant to enter the premises shall be transmitted to the persons contacted in HQ.

WHAT EVERYONE SHOULD KNOW

5 Make sure you know the following at your workplace

- **Location and use of fire extinguishers**
- **Location and use of first aid kits**
- **The exits and emergency exits**
- **How to call for help**

6 What to do in case of fire / accident / attack of illness / bomb threat / suspect letter / disturbed person

7 The meeting point

IF YOU DON'T KNOW
OR
YOU ARE UNCERTAIN ABOUT SOMETHING
=> ASK!

FLOOR PLANS

See Floor Plans as updated by Facility Manager and is published on the INTRANET of the Agency.

INSTITUTION SPECIFIC INSTRUCTIONS

Intentionally Blank

BOMB THREAT CHECK LIST

Most bomb threats are made by telephone to places of employment. When you are prepared for such a call, you can respond in a calm manner, ask for specific information about the bomb and listen for some identifying characteristics of the caller.

The following guide will help you record the details of a bomb threat made by telephone.

When a bomb threat is received:

1	Listen.
2	Be calm and courteous.
3	Do not interrupt the caller.
4	Obtain as much information as possible.
5	Complete the form provided below and give it to security.

Details of the bomb threat to be recorded:

Date:
Time (include a.m. or p.m.):
Duration of call:
Exact wording of threat:

Questions to ask:

What time will the bomb explode?
Where is it?
What does it look like?
Where are you calling from?
Why did you place the bomb?
What is your name?

Identifying characteristics of the caller:

Sex:	Male	Female	Not sure	
Estimated age (specify):				
Accent:	English	French	Other	
Voice:	Loud	Soft	Other	
Speech:	Fast	Slow	Other	
Diction:	Good	Nasal	Lisp	Other
Manner:	Emotional	Calm	Vulgar	Other
Background noise: (specify)				
Voice was familiar: (specify)				

Caller was familiar with the area: (specify)

GUARD INSTRUCTIONS

1.1 General

The security guards are not Police officers; their primary duty is prevention, surveillance and assuring assistance in case of an event NOT apprehension of a situation.

The guard's duty in crime prevention is the protection of persons, goods and property for whom they are employed or for whom their security company has a contract agreement.

The guard has no special powers or right conferred. They have the same powers as all other ordinary citizens.
The guard shall not accept any instructions directly coming from Agency staff. There is no hierarchical relation between the Agency staff and the guard. The guard receives his instructions from his employer or the Head of Administration or SO who is responsible for managing the contract.

All guards are shall operate under the national legislation and have then necessary diplomas and licences.

The Agency should provide a security guard service within 18 months from entry into force of this “ACER Security Manual” subject to budget availability.

Appearance and dress

The guard is constantly before the client, he is the image of his company but also the first impression a visitor gets of the Agency. The guard shall be correctly dressed and well groomed.

The guard is issued with uniforms and necessary equipment at his company's expense. The uniform is the emblem of an officer's authority distinguishing him from other persons in the area.

Uniform shirts (long or short sleeves), ties, belts are to worn in function of the working environment, countries habits and climate. Long sleeves shall be worn down and buttoned at the cuff. Ties shall be properly worn; cardigans or pullovers are to be compatible in colour with the company's uniform.

Identity cards, access cards

The guard shall always wear his company identity card clearly visible.

Access cards and key conferred by the Agency shall only be used in the context of the duties. Keys and access cards other than needed to open the Agency main entrance door through which the guard enters in the morning or leave the Agency in

the evening shall never be taken outside the Agency by the guard without prior approval of the Head of Administration or SO.

Keys and access cards etc. shall not be removed from the key ring.

The guard shall take great in their use. Keys must never be forced. If a key does not operate a lock easily, either the key or the lock may be faulty. Worn or cracked keys and faulty or defective locks should be reported to the Head of Administration or SO and reported in the guard's logbook for replacement or repair.

Guard post keys must be locked away on completion of duty and must never be taken home, unless specific permission is given through the Head of Administration or SO. Never leave guard post keys in a vehicle – the guard must carry them with him at all times.

Agency keys are in a key-box that is installed in the facility management room. The guard shall control the issue of keys to staff for various areas within the premises. This lockable key cabinet is provided for the safe storage of the keys. A key register is also provided for the daily recording of key issues and returns, some key boxes have an electronic logbook. Unless otherwise instructed the key for the key cabinet should be kept with the post keys.

Discipline and conduct

The use of alcohol and drugs on duty are not permitted. Guards are not to report for duty when under influence of drugs or alcohol, or with the smell of intoxicating liquor in their breath. Failure to comply with this requirement will result in the instant request by the Agency of dismissal of the guard and his permanent replacement.

Sleeping in duty is not permitted. Failure to comply with this requirement will result in the instant request by the Agency of dismissal of the guard and his permanent replacement.

Guard must give undivided attention to his duties. Unnecessary private conversations are not allowed. Long unnecessary conversations must be courteously be avoided.

The Agency is a non smoking work environment. The guard shall not smoke whilst on duty. Smoking in view of public or in front of the Agency is not permitted. The guard shall conform to the particular Agency smoking policy if he needs to smoke.

Guards are required to be courteous. They must reply to inquiries in a polite manner.

The security guard shall never leave his post unless properly relieved or upon instructions or permission of the Head of Administration or SO. They may leave their post after having called for assistance by informed their dispatching, or Agency staff to pursue a criminal offender, to assist another guard, to assist an injured person or in case of a fire or other similar emergency or extenuating circumstance.

The guard shall not accept gifts of any kind other than those given or authorised by the Head of Administration of SO which might result in compromising his position.

Confidentiality of Information

Information concerning the Agency affairs or staff may come to the attention of the guard. Such information must be treated as strictly confidential and shall under no circumstances be disclosed to third persons, even after the termination of employment.

The guard will immediately inform the Head of Administration or SO in case he sees or is confronted with sensitive information or Agency's Classified Information.

Granting access to the Agency Premises

The guard shall never let police enter in the Agency premises. The guard shall immediately inform the Director, Head of Administration, SO or in absence of these the highest in rank official about a request of national authorities requesting to enter the Agency.

The guard shall request the Police or other national authority to wait in the public area. The guard shall remain on his post during the presence of the police or national authorities and continue his normal duties.

The guards are not allowed access to the Agency outside their duties hours. In exceptional case access may be granted: The Agency premises are open to the public or specific permission was granted by the Head of Administration or SO.

Conduct offences

The guard shall during his duties be prohibited from participating in any gambling activities.

The removal of any document, article, item or good from the Agency premises is forbidden. Failure to comply with this requirement will result in the instant request by the Agency of dismissal of the guard and his permanent replacement. The Agency will report this act to the national authorities and police.

Any criminal act against the Agency or wilfully damaging or defacing of the Agency by the guard, during duty or off duty will result in an official complaint by the national authorities or police.

No arms, firearms and/or dogs are allowed in the Agency unless specifically authorised.

No television sets or radios are to be taken in the Agency. The use of the Agency television sets or radios are not allowed.

The Agency telephone and other communication means shall not be used for personal nature.

Tasks

The guards are not to permit the entry of unauthorised persons into the Agency

The Agency instructions handbook issued to all guards is to be read and understood by the guard. In case the guard does not understand an instruction he shall ask his superior or the Head of Administration or SO. The guard is required to comply with the instructions.

Knowing the premises

In order to carry out his protection and prevention duties efficiently, the guard shall be thoroughly familiar with the premises. It is the guard's responsibility to acquire all of the necessary information as soon as they assume duty.

"OK"-calls

In order to maintain contact and to be assured of the guard's well being at the start and end of his duties on normal workdays, outside normal Agency operating hours on weekdays and on weekends and public holidays the guard shall be contacted at specific times and the guard shall report on specific times with his dispatch centre.

The building

The security guard protects the assigned building, including the occupants and installations. The guard must be alert to anything which may cause injury to persons or loss or damage to the Agency property. Their duty includes:

- Protecting life and property from fire, accident, theft, damage and trespass.
- Making assigned patrol rounds according to instructions.
- Reporting evidence of and taking prompt action against fire or similar emergency.
- Permitting only persons with proper identification to enter the different guarded areas.
- Directing traffic in buildings and on building grounds.
- Making written reports on their daily duties and on unusual happenings and hazardous conditions, including potential security risks observed whilst on patrol.
- Reporting security and safety lighting which is not functioning.
- Physically checking doors and windows to ensure that they are secure.

- Reporting on building or equipment failures. (not to neglect taps).
- Reporting fire hazards. The guard must be alert and recognise and report fire hazards and be totally familiar with emergency procedures.
- Carrying out additional duties which may be necessary in order to successfully complete the assignment.

Entrance control

The guard stationed at the Agency entrance must have regard for the interests and needs of the employees and visitors. The guards shall:

- Ensure that only authorized persons are permitted to enter.
- Ensure that entrances and exits are clear and unobstructed.
- Look out for theft of the Agency property.
- Generally, departure from recognised routines, abnormal conduct, mannerism and appearance should be viewed with suspicion. An officer should be suspicious of the people who:

    - Becomes over friendly, or having been friendly, becomes obviously indifferent.
    - Arrives at the entrance in a nonchalant manner, perhaps whistling as they approach.
    - Approaches quickly, then slows down perceptibly; or approaches slowly and then increases pace.
    - Tries to deliberately avoid the officer.
    - Tries to engage them in needless conversation.
    - Is over-anxious to show a package or any other article they may be carrying.
    - Approaches the gate at an unusual time.
    - Approaches the gate walking unnaturally with a marked stoop; or an unnaturally stiff leg or arm.
    - Loiters around the gate or fence.
    - Is not dressed for the surrounding or prevailing conditions.

- Check vehicle loadings to invoices and/or delivery dockets as required.
- Ensure that each entrant, personnel or vehicle, is properly checked. The guard shall never simply sit and wave to entrants as they pass.
- Conduct bag and vehicle inspections if it is established practice to do so.
- Maintain Log Books as required.

It is the guard's responsibility to ensure the guard room area (located in K1) is tidy and free of litter. He shall ask cleaning to staff to help him keep the area clean.

Reports must be completed until the end of the service.

Cups, bottles and cans etc. must not be left lying around on the top of desks or cabinets. Any additional uniform items such as jackets, raincoats etc. should, where practicable, be stored out of sight.

No staff of other then the Head of Administration, the duty officer or SO should be permitted access to the guard room.

Patrol procedures

The most important patrol rounds the guards makes are the FIRST patrol and the LAST during his shift.

These are usually the longest one and must be carried out efficiently and with extra vigilance. It is on these patrol rounds that a guard might find objects left behind; a piece of machinery left running and unattended; or a security door left unlocked.

An effective first patrol round gives the guard prior warning during the next patrols should anything untoward be observed. The guard must know the route and follow a set plan. This plan should be varied on each patrol in order to deter any would be offender from knowing your exact routine.

The guard shall ensure that guard room is locked before commencing patrols.

The guard must he constantly on the alert and be on the lookout for any unusual conditions and listen for any unusual sounds, both of which should be investigated.
The security guard should:

- Make certain that no equipment which should have been turned off has been left running (coffee machine etc…). If equipment cannot be turned off notify an official of the Agency. (Office machines such as computers and facsimiles are generally left on and should not be turned off by the guard).
- Check heaters and furnaces for overheating.
- Check that fire-fighting equipment is in order.
- Check that no unnecessary lights are left burning or water faucets are left running.
- Check that no flammables such as waste materials, rags etc. are left close to stoves, heaters or hot pipes.
- Be suspicious of items placed near perimeter fences or under windows which might assist unauthorised access.
- Inspect fences, windows and doors or signs of forced or attempted entry, or the need for maintenance.

(Guards are not to use photo-copiers, computers etc- unless specific permission has been given).

The guards shall not look in drawers or read papers or do anything which would likely bring discredit. Courtesy is to be shown at all times to the staff working late. The

guard should not waste time by engaging in needless conversations or discuss any of the security business with them.

The guards should remember to patrol in a random, irregular pattern and be thorough in their search routine; to be alert and be careful, particularly at night, or in poorly lit or isolated areas -carry an efficient torch day or night; that all incidents, unusual conditions, damage etc. must be reported.

Search

In coming mail

The guard shall pass all incoming mail through the X-ray machine and check the mail for unwanted objects.
In case such abject are found the guard shall immediately contact the Head of Administration or SO of the Agency for further instructions.

Visitor

There is NO right of search on suspicion by anyone (other than a police officer in certain legislated circumstances) unless the person required to be searched agrees to do so voluntarily.

Legislation in most member states in this particular matter is perfectly clear, neither is an employer or his agent is entitled to conduct a search of any bag or parcel carried by a person, unless that person agrees.

In some cases the Agency may forbid customers bringing their own bags into the public area and provide lockers. There is no particular problem with this arrangement, provided the customer co-operates.

If the visitor refuses to submit to the search, we need to have proof beyond all reasonable doubt. The guard shall immediately call the Head of Administration or SO and who shall immediately call for police assistance. The guard is allowed to stop the visitor for the time for the police to come.

Bag and Vehicle Inspections

The legal right of any employer to search bags, parcels or vehicles of staff, even if necessary to combat theft, is not possible without the consent of the staff. Consent can only be given when the staff voluntarily agree to submit to the search.

The conclusion here is simple in both cases:
UNDER NO CIRCUMSTANCES SEARCH A BAG, PARCEL OR VEHICLE UNLESS IT IS AN ESTABLISHED PRACTICE TO DO SO AND WITH CONSENT OF THE PERSON.

Staff working late

It is the guard's clear responsibility to identify any staff (including senior management) who may be working after-hours, in order to establish that their presence is properly authorised. The guard shall assure that the presence board at the entrance of the Agency is up-to-date after making his last round.

The fact that the staff or management may be known to the officer does not negate this important security requirement. The by-passing of Agency's staff working after-hours does not constitute a check unless contact is made.

The guard shall record the time, date and person's name on his duty log.

Offends

The Agency is a premise like any other which is susceptible to break-ins, it is important that the guard makes careful physical checks at his first and last post round. Should a break-in be discovered the guard shall report this immediately during working hours to the Head of Administration or SO and outside Agency working hours to his dispatch centre and to the duty officer. He shall stand by if requested to do so and wait for the arrival of the Head of Administration, Agency duty officer outside office hours and police. The guard shall not touch anything as it may disturb or destroy vital evidence such as fingerprints etc. Preserve the crime scene as indicated.

If offenders are discovered in the Agency premises, the guard shall immediately contact the Head of Administration or SO and outside Agency working hours to his dispatch centre, who will notify the Police. The guard shall not attempt to capture the offenders when alone and on his own. Whilst waiting for assistance to attend, the guard shall leave the premises normally and observe from a remote position. The guard shall assist the Police as required when they arrive but don't be a hindrance.

Fire

In case a fire is observed or discovered by a security guard this must be immediately reported to the Head of Administration or SO and outside Agency working hours to his dispatch centre and to the duty officer.

All noticed fires must be reported whether in the Agency or not.

Lights

During the last internal inspection the guard shall ensure that all lights are switched off as instructed by the Head of Administration or SO.

In case unusual lights are left on, particularly when external contractors were working; this shall be treated as an occurrence. The guard shall make a thorough check of the premises to ensure that there are no intruders and report the incident to

the SO during working hours and to Agency duty officer outside working hours and make a report.
In case the guard finds security lights not to be functioning this shall be reported in the guard's logbook.

Outside working hours rounds

A patrol send by the dispatch centre shall make at least twice an outside patrol round when the Agency is closed. The patrol shall when security risks or hazards are observed send an alert to the dispatch centre which will inform the Agency duty officer if necessary.
This shall include damaged fencing; insecure gates or windows; accumulation of rubbish outside against the Agency perimeter; unusual lights switched on.

The patrols must be physical and not merely drive pass. Variation of inspection patterns, continual vigilance and careful observation are essential to good security checking procedures.

The patrol must not stay near the Agency any longer than is necessary. Following a thorough inspection and correction of any irregularities, the officer must leave.

The patrol must not forget when checking the Agency external that people could be watching. Therefore, do not hesitate to report any occurrences.

Outside working hours interventions

When a patrol is directed by the dispatch to attend the Agency that has gone into alarm, the patrol shall verify that the Agency duty officer has been contacted.

The patrol will go on site and make an external check. In case any suspect traces are noticed the dispatch will contract the Agency duty officer again. The Duty officer will decide to go to the Agency and enter the premises with the patrol.

The Police will be contacted by the dispatch centre after contact with the Agency duty officer. In case the Agency duty officer can not be reached the Head of Administration or SO will be contacted. When neither can be reached the European Commission HQ security office will be contacted and the local police, where such notification is appropriate.
In case the patrol holds keys to the premises; the patrol shall only enter if so instructed to investigate before the Agency duty officer or Police arrive. The patrol shall this procedure:

- Thoroughly check the exterior of the premises for any sign of entry.
- Notify the dispatch centre and enter with extreme caution
- Thoroughly investigate the entire complex after arrival of the Agency duty officer unless instructed differently.

- Advise the dispatch of the full and precise details of the investigation, be it the result of a genuine or false alarm.
- The patrol shall leave a record of the intervention in the guard logbook or designated place, advising the next guard on duty of the date, time and sector(s) the patrol attended.
- Close the premises properly.

Incident reporting

One of the main aims of recording data on incidents which have occurred is to keep both management and authorised staff informed of the problems and events which are transpiring, and which are affecting or may affect staff and the normal running of the Agency, and / or which could possibly lead to a major crisis occurring or a damages claim against the organisation.

What is an incident

Firstly, an incident is any happening, occurrence, event, experience, hazard encounter, adventure of circumstances which might have an effect on the Agency and which either represents a risk or harm to visitors or persons working in the Agency and does or could affect the normal routine or operation of the Agency.

Reporting

If the guard hesitates he should report incidents by telephone or two-way radio. In case he seeks for authority guidance for a particular situation he shall be very precise in the provision of details.
It is important that great care is taken in providing full description of premises and facts. This will enhance the accuracy and the effectiveness of the guidance sought.

When making reports on the telephone give:
The correct name of the Agency.
The correct and full address of the Agency.
Time and Occurrence of the incident
Accurate and descriptive area of occurrence on premises.
The guard name and Agency contact and particulars.

NOTE: Where Client Codes (coding for names and addresses) are provided they must be used, particularly over the two-way radio.

Two-Way Radio
The two-way radio should only be used in emergencies in these circumstances if there is no telephone communication available. Any information should be brief and concise and if you are asked to "Stand By', do just that - STAND BY.

Report writting

The written report is the permanent record of a security organisation. It focuses attention on fire, accident, hazards and other conditions which need to be corrected.

It provides facts and dates for special reports and investigations. It also plays an important part in criminal actions, civil suits, claims and complaints which may develop.

Format

The written report, must be submitted as soon as circumstances permit.
The report needs to be as brief as possible, omitting nothing of importance, but avoiding information which is irrelevant and has no real bearing on the incident or situation.
A good report should be complete in all of the necessary details. As an example the report can be formatted in response to the following interrogative words:

- WHO?

WHO ARE THE PERSONS CONCERNED?
The names, ages, place of residence, telephone numbers and any other information which could be helpful in positively identifying the persons concerned and any witnesses to the incident should be provided.

- WHAT?

WHAT HAPPENED?
Describe exactly what took place in such detail as may be necessary and in the order in which the events occurred.
Accuracy is vitally important and only the facts should be stated. Conjecture and / or personal opinions are not to be included.

- WHEN?

WHEN DID THE INCIDENT OCCUR?
The time, day, month and year is to be given. Example - "2300 hours, Monday, 15th August 2008"
WHEN WAS THE INCIDENT DISCOVERED?
Detail as to when the incident was discovered and by whom it was discovered should also be given.
WHEN WAS THE INCIDENT REPORTED?
Detail as to when and by whom the incident was brought to your attention should also be included where applicable.
WHEN WAS THE SITUATION RETURNED TO NORMAL?

- WHY?

WHY Dro THE INCIDENT HAPPEN?
If the reason is known, full details should be given. (This question may not always be applicable).

- HOW?

HOW DID THE EVENT TAKE PLACE?
All of the information that has been obtained and which shows exactly how the event took place should be given.

Presentation

The report shall be written in the guard logbook.
In case the dispatch centre will provide a report this shall be send to the Head of Administration and to the SO of the Agency.

Crime scene management

The crime scene is the focal point of the criminal investigation. The success or failure of an investigation not only depends upon the thoroughness and immediacy of the preliminary police investigation, but what the Guards and staff do or fail to do upon arrival at the crime scene.

The scene

The crime scene is the location in which a crime occurred and is the central location of a crime from which subsequent investigative efforts will commence. The crime scene is the source of the most productive evidence. Physical evidence in the form of weapons, tool marks, fingerprints, tyres marks, fibres etc. may be present.
The value of the crime scene can deteriorate rapidly. For example, the victim may die or rain or wind could destroy traces of the criminal. Affirmative action can mean the difference between gathering overwhelming evidence or frustration for the police.
The protection and preservation of the crime scene then becomes the responsibility of the first person / guard on the scene (unless of course the police are already present). Appropriate action by that person may prevent the destruction or contamination of physical evidence, prevent further injury or loss of life, or prevent the loss of witnesses.

Guidelines

The following basic guidelines should be observed by the first person on the scene, provided that the police are not already in attendance.

- Do not touch anything, remember what you touched.
- Render any first aid to the best of your ability, if required.
- Notify the guard dispatch centre, duty officer, and request attendance of the police.
- Preserve the crime scene.
- Keep possible witnesses and suspects apart. Advise witnesses not to discuss the incident.
- Do not undertake any lengthy questioning of witnesses, but ensure that you obtain their names and addresses. Do not discuss the incident, you might influence the witnesses.
- Be alert and listen attentively as important or vital information can be obtained.
- Request that witnesses and any suspects remain at the scene until the police arrive.

- Start an incident report, record all times starting when the incident occurred, the time the dispatch centre and Police were notified and where applicable, the identity of the complainant or informant.

Preserving the scene

Keep all unauthorised persons out of the crime scene area. This includes other security personnel and Agency staff, however if there is an injured victim it would be necessary to allow ambulance officers or First Aiders entry to administer first-aid.

Attempt to fully identify all persons who were present prior to the arrival of the police. This is regardless of whether they were witnesses, victims, suspects or onlookers. These persons have one thing in common and that is they saw the scene before the incident and any changes that may have been made can be identified.

Record all conditions found at the scene. This may include, for example:

- Were the doors and/or windows open or closed;
- Were the doors locked or unlocked;
- Were the lights in each room on or off;
- Were there any distinctive or unusual odours.

Note any change that has been made. For example, if the lights were off when you arrived and were switched on, the fact must be mentioned.

Do not smoke or allow other persons to smoke at the crime scene. If matches or butts etc. are discarded, the police might carefully gather them up for examination.

Avoid using the telephone or other similar equipment at the scene. It is not uncommon for an offender to use a telephone at the scene. Latent (hidden or not visible) fingerprints are one of the most valuable pieces of evidence and the easiest to destroy, particularly through carelessness or stupidity.

Never use a handkerchief or similar item thinking that it will preserve latent fingerprints. It won't.

Pass on all of the information that you have recorded and noted to the police immediately they arrive at the scene.

Conclusion

Remember that as the first guard to arrive at the scene, is responsible for the scene management until the arrival of the police. The success or failure of the police investigation, to a large extent could well depend upon the action that guard undertook at the scene.

Fire safety and emergency procedures

Fire safety

Because of the ever present threat of fire, the Agency took precaution to equip its premises with adequate fire protection. The guard has a role to play in both fire safety and fire prevention.

The guard must be able to recognise fire hazards and know how to summon assistance and use fire-fighting equipment. The Agency expects this to be part of the guard's basic training. In case the guard did not receive such training he is to report this immediately to the Head of Administration or SO. The guard accepts this trust when commencing duty.

Fire Hazards

Some examples of fire hazards that the guard should be alert for are the following.

- Smoking and the careless disposal of smoking materials is one of the major fire hazards. Employees smoking near flammable liquids or materials and in contravention of "No Smoking" rules is an example.
- Electrical hazards could include frayed cords on appliances, wiring nailed or tacked to walls, or faulty or overloaded appliances.
- Flammable Liquids spillage, use in a closed room or use near open flames is a major concern. Many liquids have low flash points and are easily ignited. All flammable liquid vapours are heavier than air and flies vapours can flow along the floor to an ignition source and flash back to the container. Flammable and combustible liquids should be stored in according local environment legislation and approved lidded metal containers.
- Obstructed Stairways and Aisles; stairways and aisles must be free of obstructions to allow for clear exit in the event of a fire or other emergency.
- Housekeeping; Rags impregnated with oil, paint, flammable liquids etc. are subject to spontaneous combustion and should be stored in lidded metal containers. Rubbish is a common source of fuel for a fire. Closets, aisles, storerooms and basements etc. should be free of rubbish accumulation.
- Open flames should never be used near flammable liquids or gases or explosive materials. Be aware of open flames in offices in the Christmas period, this is forbidden.
- Unattended machinery left running unattended should never be allowed unless authorised by the client. Motors can easily overheat and catch fire.

Fire emergency procedures

The Agency has in place, for the particular areas in the premises, procedures relating to the action required in the event of emergencies such as FIRE; see the Agency

safety and security guidelines manual. At these particular areas the security guard will have a role to play within those procedures. It is therefore incumbent upon the guard to ensure that they are familiar with the duties and responsibilities which may be required of them in relation to fire emergency. Some Agencies may not have procedures in place, and in these situations it is important for the guard to have an appreciation of what action should be taken when faced with a particular type of emergency.

Action in the event of a Fire

The security guard Officer must remain calm and not panic if confronted with a fire situation.

Raise the Alarm. In most case the security guard will receive a message on the fire detection system that there is a problem. Most fire detection systems in the Agency are addressable system, and do identify the detector that went in alarm. The guard shall familiarize himself with the system in the Agency.

The guard will call the person occupying the office next to the room with detector in alarm and try to identify if the alarm is genuine.

- In case the alarm is not genuine he will reset the alarm system. And closely observe the system for other alarms to occur. He will in all cases immediately inform his dispatch centre, the Head of Administration or SO (during working hours) or Agency duty officer (outside working hours) of the incident. Attention in case the guard does not reset the fire alarm, the evacuation system will sound the evacuation sign automatically within about 90 seconds after the detector went into alarm.
- In case the alarm is genuine and outside office hours the guard will call the fire brigade immediately by telephone, using the 112 emergency number and inform his dispatch centre, and Agency duty officer. In case no guard is present the evacuation system will sound the evacuation sign automatically within about 90 seconds after the detector went into alarm.
- In case the alarm is genuine and during office hours the guard will call the Head of Administration or SO, by telephone. The Head of Administration or SO will decide upon the action to take. The Guard will sound the evacuation bell if so decided and call the fire brigade immediately by telephone, using the 112 emergency number. Attention in case the guard does not reset the fire alarm, the evacuation system will sound the evacuation sign automatically within about 90 seconds after the detector went into alarm.

In case the guard detects a fire also during a security round he shall use a manual call point (break-glass fire alarm) that is nearest to his position available.

The guard shall not take the chance of delaying too long by first faying to extinguish the fire. He shall raise the alarm first. The guard may try and extinguish or contain the fire using available fire-fighting equipment, but do not take any unnecessary risks and only after calling for help and informing his dispatch centre.

The guard shall use the correct type of extinguisher for the particular fire.

The guard shall always consider his own personal safety and that of other staff at all times and make certain that he leave an escape route available should the fire become too large or the smoke too intense.

The guards must also consider the safety of others in and around the premises and where possible have these persons advised of the situation in a calm manner in order to avoid panic.

Persons evacuating the Agency MUST NOT USE LIFTS under any circumstances. Personnel should evacuate by using the fire stairs and do so in a quiet and orderly manner. In a high-rise building, evacuation normally commences with the fire affected floor, then the floor above and the floor below, and so on in that order.

The fire brigade should be met at the entrance to the premises so that they can be guided to the exact location. The guard shall allocate this task to someone else if he is undertaking other more important tasks such as helping to evacuate the premises or fighting the fire.

The fire brigade, upon arrival at the scene, have complete authority. The guard should remain in close proximity to assist the fire brigade with any relevant information or assistance that they may require.

Evacuees should remain in the allocated evacuation assembly area and no persons should be allowed to re-enter the premises without the permission of the senior fire officer present.

Bomb threat and emergency procedures

If a threat is received by telephone, the security guard should adopt the following procedures in the event established procedures for the premises are not in place.

- Record as accurately as possible the words used by the caller; note:
    - Repetitious Language Speech impediments
    - Tone Inflection Any Idiosyncrasies
    - Accent Grammar Obscene Language
- Remain calm and do not terminate the conversation.
- Endeavour to engage the caller in conversation for as long as possible.
- Try to assess the caller's mental stability - also their familiarity with the premises or the device location.

Ask questions:

- How does the bomb look like
- Where is the bomb, the building or site, the floor, the room
- The type of bomb, the type of package, the size of the bomb

  - The type of explosive The bane of detonation
  - The reason for the bomb
- Listen for any background noises and take note of:
  - Conversation or laughter
  - Vehicle noise
  - Machinery or equipment noise
- Establish the sex and try to estimate the age of the caller.
- Try to determine the motive. Any information gained from the caller may provide useful clues in assessing the motive or sincerity of the caller, or their possible identity.

After the conversation is terminated

After the conversartion is terminated the security guard shall:

- Record the time and duration of the call
- Notify the during office hours the Head of Administration of SO and police on the Emergency Telephone Number 112

OR

- Notify the designated Agency duty officer outside office hours, his dispatch centre and the police.
- If possible, complete a written record of the whole conversation. If a Bomb Threat, pro-forma is provided, complete that also.
- Arrange for the police to be met. Upon their arrival, hand over all of the information gathered. In the event of a subsequent call, advise the police.

Subsequent actions

Actions which might follow will normally be outside the responsibility of the security guard. Nevertheless, the guard will no doubt have an important role to perform, either as a result of these procedures, or acting upon the instruction of the supervising police.
The security guard is to be prepared to assist in any way. This may include search procedures, control of individuals evacuating the area, or guarding the area in general.

Evacuation

The problem may arise as to whether the premises should be evacuated. If any "time" is nominated in the threat as the "time of explosion" and that time is merely minutes away, the responsibility for issuing the evacuation order would rest with the Director, Head of Administration or SO at the threatened the Agency.

If there is sufficient time lapse to enable the attendance of police at the premises, it will be the police with the Director who will be responsible for issuing the order for evacuation. If an evacuation is ordered it would proceed according to a pre-determined plan. The safety and security guidelines for the Agency have more information on this.

Search of the premises

A search for an explosive device must be orderly, complete and thorough. The number of searchers are generally kept to a minimum for the area to be searched. Ideally each group would include individuals who are familiar with the premises or area to be searched. They could be the Security Officer, cleaners, maintenance workers, gardeners etc. and it would be easier for them to readily observe any foreign objects or disturbance to any fittings etc. within the area.

A search must be systematic and cover corridors, landings, archives, computer rooms, storage areas, locker rooms, waste containers, electrical panels, telephone booths, offices, equipment cures, furnishings, etc. in the area.

The use of two-way radios and mobile phones during the search should be avoided and searchers should not smoke. All unnecessary pedestrian and vehicular traffic should be diverted from the area.

Finding a device

If any actual or suspected explosive device or suspicious object is discovered **DO NOT TOUCH OR DISTURB** the device or object in any way. Do not immerse the object in water.

Only a qualified explosive expert should approach the object.

NOTIFY THE POLICE IMMEDIATELY
AND
EVACUATE THE BUILDING and AREA.

Occupational Health and Safety

Safety policy

The Agency safety policy is to:

- Provide and maintain a safe work environment, including work conditions, practices and procedures for all personnel working in the Agency.
- Develop safety awareness throughout all Agency staff.
- Do its utmost to minimize hazards within the work place in order to prevent accidents from occurring.
- Set responsible standards of safety for all personnel and visitors to follow.

The use of Agency operational systems

The guard shall only operate equipment provide to him by his employer or present in the Agency after having received adequate training.

The guard shall contact the Head of Administration or SO if he feels he has not the adequate training to fulfil his job or use any of the equipment in the Agency he is asked to operate.

The Agency requires the guards to:

- Follow the safety and security instructions at all times.
- Maintain a safe and tidy work area.
- Ensure that they know exactly how to do their tasks safely before they start work.
- Report any hazards and make suggestions on how to improve safety to the Head of Administration or SO.