European Maritime Safety Agency

EMSA Security Rules for protecting EU classified information (EUCI)

Security Rules

Version: 3
Date: 1/12/2024

Document History

Version	Date	Changes	Prepared	Approved
1.0	30/09/2016	Note	A.2 & A.3	ED
1.1	15/10/2017	Annex 2 Standard Operational Procedures for RESTREINT UE/EU RESTRICTED handled by the Maritime Security Team – has been updated; Two new Annexes (3 and 4) have been added in order to provide Standard Operating Procedures of section 3 on Security Clearances. New Annex 5 Standard Operating Procedures for section 6.3 accreditation process has been added.	A.2 & A.3	ED
2.0	26/03/2019	Changes in the whole document following consultation with DG.HR.S in respect coherency with the Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information.	A.2	ED
2.1	01/08/2019	Section 1 has been updated to the effect of non-public disclosure of the Annexes. Annex 2 Standard Operational Procedures for RESTREINT UE/EU RESTRICTED handled by the Maritime Security Team as well as Annex 3 and 4 have been updated.	A.1, A.2, A.3, B.2	ED
2.2	20/11/2019	Annex 6 Standard Operational Procedures for the invacuation / evacuation / destruction of RESTREINT UE/EU RESTRICTED information in the event of an emergency has been added.	A.2	ED
2.3	01/05/2020	The Rules and Annexes have been updated in line with the new EMSA organisational chart	4.2	ED
3	1/12/2024	The Rules and Annexes have been updated in line with the new EMSA organisational chart and revised EMSA Security Rules Annex 2 SOP for MARSEC team revised (RUE-X)	4.2	ED

Table of Contents

List of Abbreviations

CCTV	Closed-circuit television
DG.HR.S	Directorate-General for Human Resources and Security
DSA	Designated Security Authority
EPR	EMSA Premises Rules
EUCI	EU classified information
FSC	Facility Security Clearances
IA	Information Assurance
ICT-S	Information and Communication Technology Systems
NSA	National Security Authority
PSI	Projects Security Instruction
PSC	Personnel Security Clearance
SAL	Security Aspects Letter

1. General Provisions

The EMSA Security Rules for protecting EU classified information (EUCI) lay down the basic principles and minimum standards of security for protecting EUCI.

The annexes to this document are an integral part of the EMSA Security Rules for protecting EU classified information:

Annex 1 - Equivalence of Security Classifications for EUCI *(not publicly available)*

Annex 2 - Standard Operating Procedures for RESTREINT UE/EU RESTRICTED handled by the Maritime Security Team *(not publicly available)*

Annex 3 - Standard Operating Procedures for obtaining Personnel Security Clearances *(not publicly available)*

Annex 4 - Authorisation and PSCC Template *(not publicly available)*

Annex 5 - Security Accreditation process for RESTREINT UE/EU RESTRICTED ICT-S *(not publicly available)*

Annex 6 - Standard Operational Procedures for the invacuation / evacuation / destruction of RESTREINT UE/EU RESTRICTED *(not publicly available)*

1.1 Scope

1. The EMSA Security Rules for protecting EU classified information encompass EUCI up to the level of SECRET UE/EU SECRET; EMSA currently handles EUCI only at the level RESTREINT UE/EU RESTRICTED in the Maritime Security team, therefore for the time being the Rules will be implemented on this level the Maritime Security team. These Rules are not applicable to maritime data from EMSA maritime applications, the protection of which is ensured by data access mechanisms.

2. The EMSA Security Rules for protecting EUCI shall apply to:

   A. EMSA staff;
   B. any individual with access to EMSA premises or other assets, or to information handled by EMSA.

1.2 Definitions

Accreditation means the formal authorisation and approval granted to an information and communication technology system (ICT-S) by the Executive Director to process EUCI in its operational environment, following the formal validation of the respective Security Plan and its correct implementation.

Accreditation Process means the necessary steps and tasks required prior to the accreditation by the Executive Director. These steps and tasks shall be specified in an Accreditation Process Standard.

Authorisation for access to EUCI means a decision by the Executive Director taken on the basis of an assurance given by a competent authority of a Member State that an EMSA staff member, 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; the individual thus described is said to be 'security authorised'.

Classified contract means a framework contract or contract, as referred to in Council Regulation (EC, Euratom) No 1605/2002.

Classified subcontract means a contract entered by a contractor of EMSA, with another contractor (i.e. the subcontractor) for the supply of movable or immovable assets, the execution of works or the provision of services, the performance of which requires or involves the creation, handling or storing of EUCI.

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

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.

EMSA staff means EMSA officials, temporary agents, contract agents, Seconded National Experts as well as personnel working intramuros such as interims, trainees, NEPTs, etc.

Handling of EUCI means all possible actions to which EUCI may be subject throughout its life-cycle. It comprises its creation, registration, processing, carriage, downgrading, declassification and destruction. In relation to information and communication technology systems (ICT-S) 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.

Information and Communication Technology Systems (ICT-S) means any system enabling the handling of information in electronic form. Such system shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources.

Material means any medium, data carrier or item of machinery or equipment, either manufactured or in the process of manufacture.

Originator means the Union institution, agency or body, 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 authorisation is the application of measures to ensure that access to EUCI is granted only to individuals who have:

- a need-to-know;
- been security authorised to the relevant level, where appropriate; and
- been briefed on their responsibilities.

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, 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.

Personnel Security Clearance Certificate (PSCC) means a certificate issued by the EMSA Security Officer establishing that an individual holds a valid security clearance and a security authorisation issued by the Executive Director and which shows the level of EUCI to which that individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the period of validity of the relevant security clearance or authorisation and the date of expiry of the certificate itself.

Premises mean any immovable or assimilated property and possessions of EMSA.

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 user communities, informing the Executive Director of such risks and reporting them to operating units.

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

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

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 security clearance up to a specified level (CONFIDENTIEL UE/ EU CONFIDENTIAL or above).

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.

Standard Operating Procedures (SOP) means detailed, written instructions to implement these Rules on specific level of classification.

Staff Regulations means the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the European Union ('CEOS'), laid down by Council Regulation (EEC, Euratom, ECSC) No 259/68 as last amended by Regulation (EU, Euratom) No 1023/2013 of the European Parliament and the Council of 22 October 2013.

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.

1.3 Amendments of the EMSA Security Rules for protecting EU classified information (EUCI)

1. These Rules shall be reviewed on a regular basis.

2. The EMSA Security Manager supported by the EMSA Information Assurance Officer is responsible for preparing assessments of the need for revision and amendment for subsequent approval by the Executive Director.

2. Basic principles and minimum standards

2.1 Definition of EUCI, security classifications and markings

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

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. It may bear additional markings, which are not classification markings, but are intended to designate the field of activity to which it relates, identify the originator, limit distribution, restrict use or indicate releasability.

2.2 Classification management

1. All units in EMSA shall ensure that EUCI they create, is appropriately classified, clearly identified as EUCI and retains its classification level for only as long as necessary.

2. EUCI shall not be downgraded or declassified nor shall any of the security classification markings be modified or removed without the prior written consent of the originator.

3. In case EMSA handles EU classified information with a classification level higher than RESTREINT UE/EU RESTRICTED, Standard Operating Procedures on EUCI shall be developed on that specific level of classification.

4. EMSA shall not handle TRES SECRET UE/EU TOP SECRET information.

2.3 Protection of classified information

1. EUCI shall be protected in accordance with these Rules.

2. The holder of any item of EUCI shall be responsible for protecting it.

3. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of EMSA, EMSA 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 Annex I.

4. Where another body and/or organisation introduces classified information bearing a security classification marking into the structures or networks of EMSA, EMSA shall protect that information in accordance with the requirements applicable to EUCI at the equivalent level and in accordance with the Administrative Arrangements between EMSA and other body and/or organisation, as set out in the table of equivalence of security classifications contained in Annex I.

5. An aggregate of EUCI may warrant a level of protection corresponding to a higher classification than that of its individual components.

2.4 Security risk management

1. The 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 EMSA premises and the locally assessed threat of malicious and/or criminal activities, including espionage, sabotage and terrorism.

2. The 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.

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

2.5 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 these Rules.

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 EMSA Security Manager.

4. All appropriate measures shall be taken to:

   A. inform the originator;
   B. ensure that the case is verified 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 these Rules and/or for compromising or losing EUCI shall be liable to disciplinary and/or legal action in accordance with the applicable laws, rules and regulations.

3. Access to EUCI and security authorisations

3.1 Basic principles

1. An individual shall only be granted access to EUCI after:

   A. his need-to-know has been determined by the Executive Director;
   B. he has been briefed on the Security Rules for protecting EUCI and the relevant security standards and guidelines, and has acknowledged his responsibilities with regard to protecting such information;
   C. for information classified CONFIDENTIEL UE/EU CONFIDENTIAL and above, he has been security authorised to the relevant level or is otherwise duly authorised by virtue of his functions in accordance with national laws and regulations.

2. All individuals whose duties may require them to have access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be security authorised to the relevant level before being granted access to such EUCI. The individual concerned shall consent in writing to being submitted to the personnel security clearance procedure. Failure to do so shall mean that the individual cannot be assigned to a post, function or task which involves access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above.

3. 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.

4. 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 conducted by the competent authorities of a Member State in accordance with its national laws and regulations.

5. The EMSA Security Manager with the assistance of Unit 4.1 shall be responsible for liaising with the DG HR.S within the scope of the SLA between EMSA – DG.HR in the context of all security clearance issues.

3.2 Security authorisation procedure

1. The Executive Director of EMSA shall identify the positions within the Agency for which the holders need to access information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above to perform their duties and so need to be security authorised.

2. As soon as it is known that an individual will be appointed to a position requiring access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, the Executive Director shall inform the EMSA Security Manager, which shall liaise accordingly with the DG HR.S within the scope of the SLA between EMSA – DG.HR. The individual shall consent in writing to being submitted to the security clearance procedure and return the completed questionnaire within the shortest deadline in accordance with the instructions from DG HR.S.

3. The EMSA Security Manager shall forward the completed security clearance questionnaire to the DG HR.S within the scope of the SLA between EMSA – DG.HR in the context of all security clearance issues, requesting that a security investigation be undertaken for the level of EUCI to which the individual will require access.

4. Where information relevant to a security investigation is known to the EMSA Security Manager concerning an individual who has applied for a security clearance, the EMSA Security Manager, acting in accordance with the relevant rules and regulations, shall notify the DG HR.S within the scope of the SLA between EMSA – DG.HR in the context of all security clearance issues.

5. Following completion of the security investigation and notification from the relevant NSA of its overall assessment of the findings of the security investigation, and as soon as possible after the EMSA Security Manager has been informed by the EMSA – DG.HR.S with regard to the outcome of the security investigation, the Executive Director:

   A. may grant an authorisation for access to EUCI to the individual concerned and authorise access to EUCI up to the relevant level until a date specified by him but for a maximum of 5 years, 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;
   B. shall, where the security investigation does not result in such an assurance, in accordance with the relevant rules and regulations, notify the individual concerned, who may ask to be heard by the EMSA Security Manager. The competent NSA may be asked for any further clarification it can provide according to its national laws and regulations. If the outcome of the security investigation is confirmed, the authorisation for access to EUCI shall not be issued.

6. 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 Executive Director shall be subject to appeals in accordance with the Staff Regulations.

7. EMSA shall accept the authorisation for access to EUCI granted by any other EU bodies such as: Union institution or agency, provided it remains valid. Authorisations shall cover any assignment by the individual concerned within EMSA.

8. Where information becomes known to the EMSA Security Manager concerning a security risk posed by an individual who holds a valid security authorisation, Executive Director, acting in accordance with the relevant rules and regulations, shall ensure that the competent NSA is notified thereof.

9. More detailed provisions concerning the procedure for acquiring a security clearance and the internal division of tasks are described in the Annex 3 - Standard Operating Procedures for obtaining Personnel Security Clearances.

3.3 Access to EUCI for individuals duly authorised by virtue of their functions

The EMSA staff, who have access to EUCI by virtue of their functions, shall be briefed on their security obligations in respect of protecting EUCI.

3.4 Security clearance and security authorisation records

1. Records of security clearances and authorisations granted for access to EUCI shall be maintained by EMSA Security Manager in accordance with these Rules. These records shall contain as a minimum the level of EUCI to which an individual may be granted access, the date of issue of the security clearance and its period of validity.

2. The EMSA Security Manager 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 authorisation for access to EUCI and the date of expiry of the certificate itself.

3.5 Renewal of security authorisations

1. After the initial granting of security authorisations and provided that the individual has had uninterrupted service with EMSA and has a continuing need for access to EUCI, the security authorisation for access to EUCI shall be reviewed for renewal, as a general rule, every five years from the date of notification of the outcome of the last security investigation on which it was based.

2. The Executive Director may extend the validity of the existing security authorisation for a period of up to 12 months, if no adverse information has been received from the relevant NSA or other competent national authority within a period of two months from the date of transmission of the request for renewal and the corresponding security clearance questionnaire. If, at the end of this 12-month period, the relevant NSA or other competent national authority has not given its opinion, the individual shall be assigned to duties which do not require a security authorisation.

3. More detailed provisions concerning the procedure for the renewal of a security clearance and the internal division of tasks are described in the Annex 3 - Standard Operating Procedures for obtaining Personnel Security Clearances.

3.6 Security authorisation briefings

1. After participating in the mandatory security authorisation briefing organised by the EMSA Security Manager, all individuals who have been security authorised 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 EMSA Security Manager.

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

3. 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.

3.7 Temporary security authorisations

1. In exceptional circumstances, where duly justified in the interests of the service and pending completion of a full security investigation, the Executive Director may grant a temporary authorisation for individuals to access EUCI for a specific function, without prejudice to the provisions regarding renewal of security clearances. Such temporary authorisations for access to EUCI shall be valid for a single period not exceeding six months and shall not permit access to information classified TRES SECRET UE/EU TOP SECRET.

2. After they have been briefed, 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 EMSA Security Manager.

3.8 Attendance at classified meetings

1. EMSA staff responsible for organising meetings at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed shall, through the meeting organiser, inform the EMSA Security Manager well in advance of the dates, times, venue and participants of such meetings.

2. Individuals assigned to participate in meetings organised by EMSA at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed, may only do so upon confirmation of their security clearance or security authorisation status. Access to such classified meetings shall be denied to individuals for whom EMSA Security Manager has not seen a PSCC or other proof of security clearance, or to participants of EMSA who are not in possession of a security authorisation.

3. Before organising a classified meeting, the meeting organiser shall request external participants to provide the EMSA Security Manager well in advance with a PSCC or other proof of security clearance. The EMSA Security Manager shall inform the meeting organiser that a PSCC or other proof of PSC has been received. Where applicable, a consolidated list of names may be used, giving the relevant proof of security clearance.

4. Where the EMSA Security Manager is informed by the competent authorities that a PSC has been withdrawn from an individual whose duties require attendance at meetings organised by EMSA, the EMSA Security Manager shall notify the meeting organiser.

4. Physical security aimed at protecting classified information

4.1 Basic principles

1. 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, in accordance with these Rules and theirs Standard Operating Procedures, if applicable.

2. In particular, 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 authorisation;
   C. deterring, impeding and detecting unauthorised actions; and
   D. denying or delaying surreptitious or forced entry by intruders.

3. Physical security measures shall be put in place for EMSA premises, offices, rooms and other areas in which EUCI is handled or stored, including areas housing information and communication technology system (ICT-S).

4. Areas in which EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is stored shall be established as Secured Areas in accordance with this section and accredited by the Executive Director.

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

4.2 Physical security requirements and measures

1. Physical security measures shall be selected on the basis of a threat assessment made by the EMSA Security Manager supported by the EMSA Information Assurance Officer where appropriate in consultation with other EMSA Units and/or competent authorities in the Member State. EMSA shall apply a risk management process

for protecting EUCI on its 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, its institutions, bodies or agencies, or the Member States and from sabotage, terrorist, subversive or other criminal activities.

2. The EMSA Security Manager, applying the concept of defence in depth, shall determine the appropriate combination of physical security measures to be implemented. To that effect, the EMSA Security Manager shall develop minimum standards, norms and criteria, set out in the Standard Operating Procedures, if applicable.

3. The EMSA Security Manager is 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 EMSA premises or buildings.

4. When EUCI is at risk of being overlooked, even accidentally, the EMSA Units concerned shall take the appropriate measures, as defined by the EMSA Security Manager, to counter this risk.

4.3 Equipment for the physical protection of EUCI

1. Two types of physically protected areas shall be established for the physical protection of EUCI:

A. Administrative Areas; and
B. Secured Areas (including technically Secured Areas).

2. The Executive Director shall establish that an area meets the requirements to be designated as an Administrative Area, a Secured Area or a technically Secured Area.

3. For Administrative Areas:

A. a visibly defined perimeter shall be established which allows individuals to be checked;
B. unescorted access shall be granted only to individuals in accordance with the EMSA Premises Rules; and
C. all other individuals shall be escorted at all times or be subject to equivalent controls in accordance with the EMSA Premises Rules.

4. For Secured Areas:

A. a visibly defined and protected perimeter shall be established through which all entry and exit is 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;
C. all other individuals shall be escorted at all times or be subject to equivalent controls.

5. 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.

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

A. such areas shall be equipped with an Intrusion Detection System (IDS), be locked when not occupied and be guarded when occupied;
B. all persons and material entering such areas shall be controlled;

C. such areas shall be regularly physically and/or technically inspected by the EMSA Security Manager. 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.

7. 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 communication devices and electrical or electronic equipment shall first be examined by the EMSA Information Assurance Officer to ensure that no intelligible information can be inadvertently or illicitly transmitted by such equipment beyond the perimeter of the Secured Area.

8. 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.

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

10. Security Operating Procedures shall be prepared for a 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 authorisation;
D. where appropriate, the procedures for escorts or for protecting EUCI when authorising any other individuals to access the area;
E. any other relevant measures and procedures.

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

4.4 Physical protective measures for handling and storing EUCI

1. 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 with compensatory measures to ensure that EUCI is protected from access by unauthorised persons.

2. 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 an Administrative Area or a Secured Area provided the holder has undertaken to comply with compensatory measures.

3. 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:

- has undertaken to comply with compensatory measures, set out in implementing rules, to ensure the EUCI is protected from access by unauthorised persons;
- keeps the EUCI at all times under his personal control; and
- in the case of documents in paper form, has notified the relevant registry of the fact.

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

4.5 Management of keys and combinations used for protecting EUCI

1. Procedures for managing keys and combination settings for offices and security containers shall be intended to guard against unauthorised access.

2. 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.

5. Management of EU Classified information

5.1 Basic principles

1. EUCI shall be managed in accordance with these Rules. However, any EUCI that is declassified shall from the moment of its declassification be managed in accordance with the EMSA Records Management Policy.

2. RESTREINT UE/EU RESTRICTED information shall be managed in accordance with the Annex 2 - Standard Operating Procedures for RESTREINT UE/EU RESTRICTED handled by the Maritime Security Team.

3. Information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be registered for security purposes prior to distribution and upon receipt.

4. A EUCI registry system shall be set up by the EMSA Security Manager for information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above.

5. EMSA premises where EUCI is handled or stored shall be subject to regular inspection by the EMSA Information Assurance Officer.

6. EUCI shall be conveyed between EMSA and other bodies outside physically protected areas as follows:

   A. as a general rule, EUCI shall be transmitted by electronic means protected by approved cryptographic products;
   B. when the means referred to in point (a) are not used, EUCI shall be carried either:

      - on electronic media (e.g. USB sticks, CDs, hard drives) protected by EU approved cryptographic products or other approved mechanisms.
      - In all other cases, as prescribed in the Annex 2 - Standard Operation Procedures for RESTREINT UE/EU RESTRICTED handled by the Maritime Security Team, if applicable.

5.2 Classifications

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

2. The originator of EUCI shall be responsible for determining the security classification level, in accordance with standards and guidelines regarding classification, and for the initial dissemination of the information.

3. The security classification shall be clearly and correctly indicated, regardless of whether the EUCI is in paper, oral, electronic or any other form.

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

5. 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.

6. 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.

7. 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

5.3 Markings

1. In addition to the security classification marking, 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;
   D. where applicable, the date or specific event after which it may be downgraded or declassified.

5.4 Abbreviated classification markings

1. 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.

2. 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:

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

5.5 Accreditation of ICT-S handling EUCI

1. All ICT-S handling EUCI shall undergo an accreditation process, based upon the principles of IA, whose level of detail must be commensurate with the level of protection required.

2. The accreditation process shall include formal validation by the Executive Director of the Security Plan of the ICT-S concerned in order to obtain assurance that:

   A. the risk management process has been properly carried out;
   B. the System Owner has knowingly accepted the residual risk; and
   C. a sufficient level of protection of the ICT-S, and of the EUCI handled in it, has been achieved in accordance with these Rules.

3. The Executive Director shall issue an accreditation statement which determines the maximum classification level of the EUCI that may be handled in the ICT-S as well as the corresponding terms and conditions for its operation.

4. The accreditation process shall consist of a series of tasks to be assumed by the parties involved. Responsibility for the preparation of the accreditation files and documentation shall rest entirely upon the ICT-S System Owner.

5. The accreditation shall be the responsibility of the Executive Director who, at any moment in the life cycle of the ICT-S, shall have the right to:

   A. require that an accreditation process is carried out;
   B. audit or inspect the ICT-S;
   C. where the conditions for operation are no any longer satisfied, require the definition and effective implementation of a security improvement plan within a well-defined timescale, potentially withdrawing permission to operate the ICT-S until the conditions for its operation are satisfied.

6. More detailed provisions concerning the accreditation process are described in Annex 5 - The Security Accreditation Process.

5.6 Creation of EUCI

1. 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 registration number and a subject, which is not itself classified information, unless it is marked as such;
   D. the document shall be dated;
   E. documents classified SECRET UE/EU SECRET shall bear a copy number on every page, if they are to be distributed in several copies.

2. Where it is not possible to apply paragraph 1 to EUCI, other appropriate measures shall be taken in accordance with the Standard Operation Procedures, if applicable.

5.7 Downgrading and declassification of EUCI

1. At the time of its creation, the originator shall indicate, where possible, whether EUCI can be downgraded or declassified on a given date or following a specific event.

2. EMSA shall regularly review EUCI for which it is the originator to ascertain whether the classification level still applies. A system to review the classification level of registered EUCI which has originated in EMSA no less frequently than every five years shall be established by SOP. 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.

3. Information classified RESTREINT UE/EU RESTRICTED originated in EMSA will be considered to be automatically declassified after thirty years, in accordance with Regulation (EEC, Euratom) No 354/83 as amended by Council Regulation (EC, Euratom) No 1700/2003.

5.8 EUCI registry system in EMSA

1. A EUCI registry system shall be set up and managed by the EMSA Security Manager for information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above.

2. A record of all information classified RESTREINT UE/EU RESTRICTED shall be set up and managed by each Unit handling such information.

3. The EMSA Security Manager shall act as the central receiving and dispatching authority for information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above.

4. The EUCI register for information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be established as a Secured Area as defined in section 4 and accredited by the EMSA Executive Director.

5.9 Registration of EUCI for security purposes

1. For the purposes of these Rules, registration for security purposes (hereinafter referred to as 'registration') means the application of procedures which record the lifecycle of EUCI, including its dissemination. All information or material classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be registered in EMSA EUCI registry when it is received in or dispatched from an organisational entity.

2. When EUCI is handled or stored using an Information and Communication Technology Systems, registration procedures may be performed by processes within the Information and Communication Technology Systems itself.

3. More detailed provisions concerning the registration of EUCI for security purposes shall be laid down in the Standard Operating Procedures.

5.10 Copying and translating EU classified documents

1. Where the originator has not imposed caveats on their copying or translation, such documents may be copied or translated on instruction from the holder.

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

5.11 Carriage of EUCI

1. EUCI shall be carried in such a way as to protect it from unauthorised disclosure during its carriage.

2. Carriage of EUCI shall be subject to the protective measures, which shall:

   A. be commensurate with the level of classification of the EUCI carried, and
   B. be adapted to the specific conditions of its carriage, in particular depending on whether EUCI is carried:

      - within the EMSA building
      - between EU buildings located in the same Member State,
      - within the Union,

   C. be adapted to the nature and form of the EUCI.

3. These protective measures shall be laid down in detail in the Standard Operating Procedures, when applicable.

4. Standard Operating Procedures shall include provisions commensurate with the level of EUCI, regarding:

   A. the type of carriage, such as by hand, by diplomatic bag, by postal services or by commercial courier services,
   B. packaging of EUCI,
   C. technical countermeasures for EUCI carried on electronic media,
   D. any other procedural, physical or electronic measure,
   E. registration procedures,
   F. use of security authorised personnel.

5. When EUCI is carried on electronic media, the protective measures set out may be supplemented by appropriate technical countermeasures approved by the Executive Director on recommendation of the EMSA Information Assurance Officer so as to minimise the risk of loss or compromise.

5.12 Destruction of EUCI

1. EU classified documents which are no longer required may be destroyed, in accordance with EMSA Records Management Policy and Procedures.

2. EUCI of the level of CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be destroyed by the EMSA Security Manager of the responsible EUCI registry on instruction from the holder or from a competent authority. The EMSA Security Manager shall update the logbooks and other registration information accordingly.

3. For documents classified SECRET UE/EU SECRET, such destruction shall be performed by the EMSA Security Manager in the presence of a witness who shall be cleared to at least the classification level of the document being destroyed.

4. The EMSA Security Manager and the witness, where the presence of the latter is required, shall sign a destruction certificate, which shall be filed in the registry. The EMSA Security Manager shall keep destruction certificates for documents classified CONFIDENTIEL UE/EU; CONFIDENTIAL or SECRET UE/EU SECRET for a period of at least five years.

5. Classified documents, including those classified RESTREINT UE/EU RESTRICTED, shall be destroyed by methods which shall be defined in the Standard Operating Procedures and which shall meet relevant EU or equivalent standards.

6. Electronic storage media used for EUCI shall be destroyed in accordance with the Standard Operating Procedures.

5.13 Destruction of EUCI in emergencies

1. The EMSA Security Manager supported by the system owner(s) and the EMSA Information Assurance Officer (for the digital security dimension) shall prepare plans based on local conditions for the safeguarding of EU classified material in a crisis including if necessary emergency destruction and evacuation plans. They shall promulgate instructions deemed necessary to prevent EUCI from falling into unauthorised hands.

2. The arrangements for the safeguarding and/or destruction of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/ EU SECRET material in a crisis shall under not adversely affect the safeguarding or destruction of enciphering equipment, whose treatment shall take priority over all other tasks.

3. 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.

4. More detailed provisions for destruction of EUCI shall be in the Standard Operating Procedures. Annex 6 Standard Operational Procedures for the invacuation / evacuation / destruction of RESTREINT UE/EU RESTRICTED information in a crisis, is kept by the EMSA Security Manager and distributed for attention of Head of Department 2, Marsec team and Facilities and Logistic team, when necessary.

6. Protection of EU Classified information in Information and Communication Technology Systems (ICT-S)

6.1 Basic principles of Information Assurance

1. Information Assurance (IA) in the field of information and communication technology system (ICT-S) 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.

2. Effective Information Assurance shall ensure appropriate levels of:

   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 assets and information;

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

3. IA shall be based on a risk management process.

6.2 ICT-S handling EUCI

1. ICT-S shall handle EUCI in accordance with the concept of IA.

2. For ICT-S handling EUCI implies that:

   A. the Plan-Do-Check-Act approach shall be applied for the implementation of the information systems security policy during the full lifecycle of the information system;
   B. the security needs must be identified through a business impact assessment;
   C. the information system and the data therein must undergo a formal asset classification; all mandatory security measures as determined by the policy on security of information systems must be implemented;
   D. a risk management process must be applied, consisting of the following steps: threat and vulnerability identification, risk assessment, risk treatment, risk acceptance and risk communication;
   E. a security plan, including the Security Policy and the Security Operating Procedures, is defined, implemented, checked and reviewed.

3. All staff involved in the design, development, testing, operation, management or usage of ICT-S handling EUCI shall notify to the Executive Director all potential security weaknesses, incidents, breaches of security or compromise which may have an impact on the protection of the ICT-S and/or the EUCI therein.

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

   A. preference shall be given to products which have been approved by the Council or by the Secretary-General of the Council in its function as crypto approval authority of the Council;
   B. where warranted on specific operational grounds, the Executive Director may waive the requirements referred to under a) and grant an interim approval for a specific period.

5. During transmission, processing and storage of EUCI by electronic means, approved cryptographic products shall be used. Notwithstanding this requirement, specific procedures may be applied under emergency circumstances or in specific technical configurations after approval by the Executive Director.

6. Security measures shall be implemented to protect ICT-S handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL or 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.

6.3 Emergency circumstances

1. Notwithstanding the provisions of this section, 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.

2. 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; and
   B. the classified material cannot be conveyed in time by other means.

3. Classified information transmitted under the circumstances set shall not bear any markings or indications distinguishing it from information which is unclassified, or which can be protected by an available crypto-graphic product. Recipients shall be notified of the classification level, without delay, by other means.

4. A subsequent report shall be made to the Executive Director.

7. Industrial security

7.1 Basic principles

1. Industrial security is the application of measures to ensure the protection of EUCI within the framework of classified contracts, by:

   A. candidates or tenderers throughout the tendering and contracting procedure;
   B. contractors or subcontractors throughout the lifecycle of classified contracts.

2. Unless stated otherwise, provisions in this section referring to classified contracts or contractors shall be applicable also to classified subcontracts or subcontractors.

7.2 Procedure for classified contracts

1. EMSA shall ensure that the minimum standards on industrial security set out in this section are referred to or incorporated in the contract and complied with when awarding classified contracts.

2. The EMSA Security Manager may seek the advice of the DG HR.S and shall ensure that model contracts and subcontracts include provisions reflecting the basic principles and minimum standards for protecting EUCI to be complied with by contractors and subcontractors.

3. When an EMSA Unit intends to launch a procedure aimed at concluding a classified contract, it shall seek the advice of the EMSA Security Manager on issues regarding the classified nature and elements of the procedure, during all its stages.

4. For models of classified contracts and subcontracts, contract notices, Project Security Instructions (PSI) and/or Security Aspects Letters (SAL), as applicable, the templates in the implementing rules for Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information shall be used.

7.3 Access to EUCI for contractors' staff

EMSA shall ensure that the classified contract includes provisions indicating that staff of a contractor or subcontractor who, for the performance of the classified contract or subcontract, requires access to EUCI, shall be granted such access only if:

   A. they have been security authorised to the relevant level or are otherwise duly authorised by their need-to-know has been determined;
   B. they have been briefed on the applicable security rules for protecting EUCI, and have acknowledged in writing their responsibilities with regard to protecting such information;
   C. they have been security cleared at the relevant level for information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET by the respective NSA, DSA or any other competent authority.

7.4 Provision for classified contracts

1. Where EUCI is provided to a candidate or tenderer during the procurement procedure, the call for tender shall contain a provision obliging the candidate or tenderer failing to submit a tender or who is not selected, to return all classified documents within a specified period of time.

2. The contracting authority, shall notify, through the DG HR.S, the competent NSA, DSA or any other competent security authority of the fact that a classified contract has been awarded, and of the relevant data, such as the name of the contractor(s) or beneficiaries, the duration of the contract and the maximum level of classification.

3. When such contracts are terminated, the contracting authority, shall promptly notify, through DG HR.S, the NSA, DSA or any other competent security authority of the Member State in which the contractor is registered.

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

5. Specific provisions for the disposal of EUCI during the performance of the classified contract or upon its termination shall be laid down in the Security Aspect Letter.

6. Where the contractor is authorised to retain EUCI after termination of a classified contract, the minimum standards contained in these Rules shall continue to be complied with and the confidentiality of EUCI shall be protected by the contractor.

7.5 Specific provisions for classified contracts

1. The conditions relevant for the protection of EUCI under which the contractor may subcontract shall be defined in the call for tender and in the classified contract.

2. A contractor shall obtain permission from the contracting authority, before sub-contracting any parts of a classified contract. No subcontract involving access to EUCI may be awarded to subcontractors registered in a third country, which has not entered into the security of information agreement with the European Union.

3. 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.

4. With regard to EUCI created or handled by the contractor, EMSA shall be considered to be the originator, and the rights incumbent on the originator shall be exercised by the contracting authority.

7.6 Visits in connection with classified contracts

1. Where EMSA staff members or contractors' personnel require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET for the performance of a classified contract, visits shall be arranged in liaison with the NSAs, DSAs or any other security authority concerned. The EMSA Security Manager and the Commission Security Authority shall be informed of such visits.

2. All visitors shall hold an appropriate security clearance and have a ‘need-to-know’ for access to the EUCI related to the classified contract.

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

4. More detailed provisions on such visits shall be adopted in line with the implementing rules for Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information.

5. Compliance with the provisions regarding visits in connection with classified contracts, set out in these Rules and the Commission’s implementing rules on industrial security shall be mandatory.

7.7 Transmission and carriage of EUCI in connection with classified contracts

1. With regard to the transmission of EUCI by electronic means, the relevant provisions of section 6 of these Rules shall apply.

2. With regard to the carriage of EUCI, the relevant provisions of section 5 of these Rules and the implementing rules on industrial security of Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information shall apply, in accordance with national laws and regulations.

3. 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. 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, DSA or any other competent security authority concerned;
D. journeys shall be point –to- point to the extent possible, and shall be completed as quickly as circumstances permit;
E. 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.

7.8 Transfer of EUCI to contractors or grant beneficiaries located in third State

EUCI shall be transferred to contractors located in third States in accordance with security measures agreed between the DG.HR.S, EMSA, as the contracting authority, and the NSA, DSA or other competent security authority of the concerned third country where the contractor is registered.

7.9 Handling of information classified RESTREINT UE/EU RESTRICTED in the context of classified contracts

1. Protection of information classified RESTREINT UE/EU RESTRICTED handled or stored under classified contracts shall be based on the principles of proportionality and cost-effectiveness.

2. No FSC or PSC shall be required in the context of classified contracts involving the handling of information classified at the level of RESTREINT UE/EU RESTRICTED.

3. Where a contract involves handling of information classified RESTREINT UE/EU RESTRICTED in an ICT-S operated by a contractor, the contracting authority shall ensure, after consulting the EMSA Security Manager supported by the system owner(s) and the EMSA Information Assurance Officer, that the contract specifies the necessary technical and administrative requirements regarding accreditation or approval of the ICT-S commensurate with the assessed risk, taking account of all relevant factors. The scope of accreditation or approval of such ICT-S shall be agreed between the Executive Director and the relevant NSA or DSA.

8. Exchange of classified information

8.1 Basic principles

1. Where EMSA determines that there is a need to exchange EUCI with another Union Institution, agency, body or office, or international organisation, the necessary steps shall be undertaken to establish an appropriate legal or administrative framework to that effect, which may include administrative arrangements concluded in accordance with the relevant regulations.

2. EUCI shall only be exchanged with a Union Institution, agency, body or office, or international organisation, provided such an appropriate legal or administrative framework is in place, and that there are sufficient guarantees that the Union Institution, agency, body or office or international organisation concerned applies equivalent basic principles and minimum standards for the protection of classified information.

8.2 Exchange of EUCI with Union institutions, agencies, bodies and offices

1. Before entering into an administrative arrangement for the exchange of EUCI with another Union Institution, agency, body or office, EMSA shall seek assurance that the Union Institution, agency, body or office concerned:

A. has a regulatory framework for the protection of EUCI in place, which lays down basic principles and minimum standards equivalent to those laid down in these Rules and its Standard Operating Procedures.
B. applies security standards and guidelines regarding personnel security, physical security, management of EUCI and security of ICT-S, which guarantee an equivalent level of protection of EUCI as that afforded in EMSA.
C. marks classified information which it creates as EUCI.

2. Before entering into an administrative arrangement on the exchange of EUCI, the EMSA Information Assurance Officer shall conduct an assessment aimed at assessing the regulatory framework put in place by the corresponding Union Institution, agency, body or office in order to protect EUCI and ascertaining the effectiveness of related measures implemented for protecting EUCI. The administrative arrangement shall enter into force, and EUCI shall be exchanged, only if the outcome of this assessment is satisfactory and the recommendations made further have been complied with. Regular follow-up assessment shall be conducted to verify that the administrative arrangement is complied with and the security measures in place continue to meet the basic principles and minimum standards agreed.

3. Within EMSA, the EUCI registry managed by the EMSA Security Manager shall, as a general rule, be the main point of entry and exit for classified information exchanges with Union institutions, agencies, bodies and offices.

8.3 Exchange of EUCI with Member States

1. EUCI may be exchanged with and released to Member States provided that they protect that information in accordance with the requirements applicable to classified information bearing a national security classification at the equivalent level as set out in the table of equivalence of security classifications contained in Annex I.

2. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the European Union, EMSA 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 Annex I.

8.4 Exchange of EUCI with international organisations

1. Where EMSA determines that it has a long-term need to exchange classified information with international organisations, the necessary steps shall be undertaken to establish an appropriate legal or administrative framework to that effect, which may include administrative arrangements concluded in accordance with the relevant regulations.

2. Such administrative arrangements shall contain provisions to ensure that when third States or international organisations receive EUCI, such information is given protection appropriate to its classification level and according to minimum standards which are equivalent to those laid down in these Rules.

3. The decision to release EUCI originating in EMSA to international organisation shall be taken by the Executive Director, as originator of this EUCI within EMSA, 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, or of the source material it may contain, is not EMSA, EMSA which holds this classified information, shall first seek the originator's written consent to release. If the originator cannot be established, EMSA, which holds this classified information, shall assume the former's responsibility.

8.5 Administrative arrangements

1. An administrative arrangement shall:

   A. establish the basic principles and minimum standards governing the exchange of classified information between the EMSA and international organisation;
   B. provide for technical implementing arrangements to be agreed between EMSA and the competent security authority of the international organisation in question. Such arrangements shall take account of the level of protection provided by the security regulations, structures and procedures in place in international organisation concerned;
   C. provide that, prior to the exchange of classified information under the agreement, it shall be ascertained that the receiving party is able to protect and safeguard classified information provided to it in an appropriate manner;
   D. established following EMSA Administrative Arrangements Rules.

2. No EUCI shall be exchanged by electronic means unless explicitly provided for in the security of information agreement or technical implementing arrangements.

3. Within EMSA, the EUCI registry managed by the EMSA Security Manager shall, as a general rule, be the main point of entry and exit for classified information exchanges with third States and international organisations. However, for information classified RESTREINT UE/EU RESTRICTED, the respective Unit handling such information shall operate as the point of entry and exit for classified information regarding matters within its competence.

4. In order to assess the effectiveness of the security regulations, structures and procedures in international organisation concerned, EMSA may seek advice from the DG.HR.S.

5. In order to assess the effectiveness of the security regulations, structures and procedures in international organisation concerned, EMSA may, in collaboration with other Union institutions, agencies or bodies, participate in assessments and/or assessment visits, in mutual agreement with the international organisation concerned. Such assessment visits shall evaluate:

   A. the regulatory framework applicable for protecting classified information;
   B. any specific features of the security policy and the way in which security is organised in international organisation which may have an impact on the level of classified information that may be exchanged;
   C. the security measures and procedures actually in place; and
   D. security clearance procedures for the level of EUCI to be released.

8.6 Exceptional ad hoc release of EUCI

1. Where no administrative arrangement is in place, and where EMSA determines that there is an exceptional need in the context of a Union political or legal framework to release EUCI to a Union institution, agency, body or office, or to a specific body or department within international organisation, EUCI may be released under the exceptional ad hoc release procedure. The decision to release shall be taken, after consultation of the DG.HR.S by the Executive Director on the basis of a proposal by the EMSA Security Manager.

2. Following the Executive Director's decision to release the EUCI and subject to prior written consent of the originator, including the originators of source material it may contain, the competent EMSA Unit shall forward the information concerned. The information shall bear a releasability marking indicating the Union institution, agency, body of office or the specific body or department within the third State or international organisation to which it is being released. Prior to or upon actual release, the third party in question shall undertake in writing to protect the EUCI it receives in accordance with the basic principles and minimum standards set out in these Rules.

List of Annexes

Annex 1	Equivalence of security classifications
Annex 2	Standard operating procedures for RESTREINT UE/EU RESTRICTED handled by the Maritime security team
Annex 3	Standard operating procedures for obtaining personnel security clearances
Annex 4	Authorisation to access European Union classified information and PSCC template
Annex 5	Security Accreditation Process for RESTREINT UE/EU RESTRICTED ICT-S
Annex 6	Standard Operational Procedures for the invacuation / evacuation / destruction of RESTREINT UE/EU RESTRICTED information in the event of an emergency

European Maritime Safety Agency
Praça Europa 4
1249-206 Lisbon, Portugal
Tel +351 21 1209 200
Fax +351 21 1209 210
emsa.europa.eu