Ref.: EUSPA-SEC-AB-DEC-A22114
Version 1.0
AB decision no.: EUSPA-AB-08-23-01-09

EU Agency for the Space Programme

Administrative Board 8

Prague, 26 January 2023

Decision of the Administrative Board on the security rules for protecting EU Classified Information

DECISION OF THE ADMINISTRATIVE BOARD OF THE EUROPEAN UNION AGENCY FOR THE SPACE PROGRAMME OF 26 JANUARY 2023

adopting the European Union Agency for the Space Programme Decision on the security rules for protecting EU Classified Information

The Administrative Board of the European Agency for the Space Programme (hereinafter 'the Agency'),

Having regard to Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU (hereinafter the 'EUSPA Regulation'), and in particular Article 76, 77 and 96 thereof;

Having regard to the Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU Classified Information (hereinafter the 'EUCI');

Having regard to the European Union Agency for the Space Programme Decision on Security in the Agency (EUSPA-AB-07-22-10-06);

Whereas:

1) The Agency is required, subject to prior consultation of the Commission, adopt its own security rules equivalent to the Commission's security rules for protecting EUCI and sensitive non-classified information, including rules concerning the exchange, processing and storage of such information, in accordance with 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;
2) The objective of security within the Agency is to enable the Agency to operate in a safe and secure environment by establishing a coherent, integrated approach as regards its security, providing appropriate levels of protection for persons, assets and information commensurate with identified risks, and ensuring efficient and timely delivery of security. Security in the Agency shall be based on the principles of legality, transparency, proportionality and accountability;
3) It is important that the Agency is associated with the principles, standards and rules for protecting classified information which are necessary in order to protect the interests of the Union and its Member States;
4) Risk to EUCI should be managed as a process. This process should 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 these measures in line with the concept of defence in depth. The effectiveness of such measures should be continuously evaluated;
5) The Agency has consulted the Commission on these security rules;

6) The Administrative Board of the Agency has adopted the European Union Agency for the Space Programme Decision on Security in the Agency (EUSPA-AB-07-22-10-06).

HAS DECIDED AS FOLLOWS:

Article 1 – Adoption

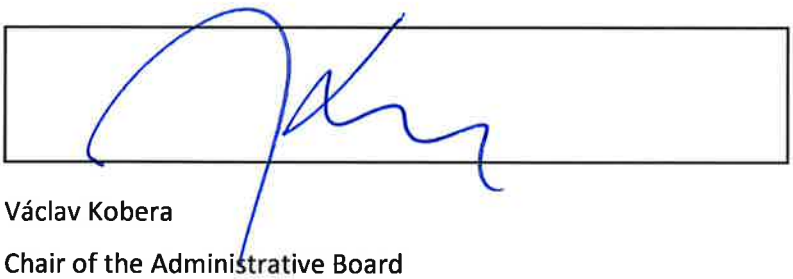
The European Union Agency for the Space Programme Decision on the security rules for protecting EU Classified Information, as set out in the Annex to this Decision, is hereby adopted.

Article 2- Entry into force

The present Decision enters into force on the day following its adoption.

Done in Prague, on 26 January 2023

For the EUSPA Administrative Board



Václav Kobera

Chair of the Administrative Board

Annexes:
Annex- European Union Agency for the Space Programme Decision on the security rules for protecting EU Classified Information.

ANNEX

European Union Agency for the Space Programme Decision on the security rules for protecting EU Classified Information

CHAPTER 1 – BASIC PRINCIPLES AND MINIMUM STANDARDS

Article 1 - Definitions

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

1. 'accreditation' means the formal authorisation and approval granted to a Communication and Information System (CIS) by the Security Accreditation Authority (SAA) to process EUCI in its operational environment, following the formal validation of the Security Plan and its correct implementation;
2. 'accreditation process' means the necessary steps and tasks required prior to the accreditation by the Security Accreditation Authority. These steps and tasks shall be specified in the Agency CIS Security Accreditation Policy;
3. 'Agency department' means any Agency department, including administrative and operational department, within the organisational structure of the Agency approved by the Administrative Board;
4. 'Agency staff members' means Agency officials and other servants including Seconded National Experts;
5. 'authorisation for access to EUCI' means a decision by the Security Authority of the Agency taken on the basis of an assurance given by a competent authority of a Member State that an Agency official, other servant or seconded national expert may, provided his/her 'need-to-know' has been determined and he/she has been appropriately briefed on his/her 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';
6. 'cryptographic (CRYPTO) material' means cryptographic algorithms, cryptographic hardware and software modules, and products including implementation details and associated documentation and keying material;
7. 'classified contract' means a framework contract or contract, as referred to in EU Regulation 2018/1046[1], entered into by the Agency or one of its departments, with a

[1] Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).

contractor for the supply of movable or immovable assets, the execution of works or the provision of services, the performance of which requires handling of EUCI;

8. 'classified subcontract' means a contract entered into by a contractor of the Agency or one of its departments, 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;
9. 'classified grant agreement' means an agreement whereby the Agency awards a grant, the performance of which requires or involves the creation, handling or storing of EUCI;
10. 'Communication and Information System' (CIS) means any systems enabling the handling of information in electronic form. A communication and information system shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources. 'Agency CIS' means CIS owned by the Agency (this definition excludes the systems of the Space Programme Components);
11. '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;
12. 'declassification' means the removal of any security classification;
13. 'defence in depth' means the application of a range of security measures organised as multiple layers of defence;
14. 'document' means any recorded information regardless of its physical form or characteristics;
15. 'downgrading' means a reduction in the level of security classification;
16. 'EU 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;
17. '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 Communication and Information Systems (CIS) it also comprises its collection, display, transmission and storage;
18. '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;
19. 'implementing rules' means any set of rules adopted by the Administrative Board of the Agency in accordance with Chapter 5 of the European Union Agency for the Space Programme Decision on Security in the Agency;
20. 'Information Assurance' (IA) in the field of Communication and Information Systems means 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;
21. 'material' means any medium, data carrier or item of machinery or equipment, either manufactured or in the process of manufacture;
22. 'originator' means the European 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;

23. ‘personnel security authorisation’ 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 authorised to the relevant level, where appropriate; and
    c. been briefed on their responsibilities.
24. ‘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/her ‘need-to-know’ has been determined and he/she has been appropriately briefed on his/her responsibilities, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date;
25. ‘Personnel Security Clearance Certificate’ (PSCC) means a certificate issued by a competent authority establishing that an individual holds a valid security clearance or a security authorisation issued by the Agency Security Authority 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;
26. ‘premises’ means any immovable or assimilated property and possessions which the Agency is entitled to use on the basis of a hosting agreement, a lease or similar agreement;
27. ‘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;
28. ‘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;
29. ‘risk acceptance’ is the decision to agree to the further existence of a residual risk after risk treatment;
30. ‘risk assessment’ consists of identifying threats and vulnerabilities and conducting the related risk analysis, i.e. the analysis of probability and impact;
31. ‘risk communication’ consists of developing awareness of risks among CIS user communities, informing approval authorities of such risks and reporting them to operating authorities;
32. ‘risk treatment’ consists of mitigating, removing, reducing (through an appropriate combination of technical, physical, organisational or procedural measures), transferring or monitoring the risk;
33. ‘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);
34. ‘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;

35. 'sites' means the actual premises where the Agency is entrusted with responsibilities for its security, including where specified in the relevant hosting agreement, lease or similar agreement;
36. 'Staff Regulations' means the Staff Regulations of officials of the European Union and the Conditions of Employment of other servants of the European Union, as laid down by Regulation (EEC, Euratom, ECSC) No 259/68 of the Council[2];
37. '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;
38. '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.

Article 2 – Subject matter and scope

1. This Decision lays down the objectives, basic principles and minimum standards, roles and responsibilities regarding the Agency's security rules for protecting EUCI (´the Rules´).
2. This Decision shall apply to all Agency departments and in all premises and sites of the Agency.
3. Notwithstanding any specific indications concerning particular groups of staff, this Decision shall apply to Agency staff under the scope of the Staff Regulations and of the Conditions of Employment of other servants of the European Communities to national experts seconded to the Agency (SNEs), to service providers and their staff, to trainees and to any individual with access to Agency buildings or other assets, or to information handled by the Agency.

Article 3 – EUCI security classifications and markings

1. 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;

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

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.

2. EUCI shall bear a security classification marking in accordance with paragraph 1. 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.

Article 4 – Classification management

1. Each Agency department shall ensure that the EUCI it creates is appropriately classified, clearly identified as EUCI, and retains its classification level for only as long as necessary.
2. Without prejudice to Article 25 below, EUCI shall not be downgraded or declassified, nor shall any of the security classification markings referred to in Article 3(1) be modified or removed without the prior written consent of the originator.
3. Where appropriate, implementing rules on handling EUCI, including a practical classification guide, shall be adopted in accordance with Article 7 below.

Article 5 – Protection of classified information

1. EUCI shall be protected in accordance with this Decision and its implementing rules.
2. The holder of any item of EUCI shall be responsible for protecting it, in accordance with this Decision and its implementing rules, according to the rules laid out in Chapter 4 below.
3. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the Agency, 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 the Annex to the Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union[3], or to the Commission Decision (EU, Euratom) 2015/444[4], as latest updated.
4. An aggregate of EUCI may warrant a level of protection corresponding to a higher classification than that of its individual components.

[3] Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union (OJ 2011/C 202/05, 08.7.2011, p. 13).
[4] Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU Classified Information.

Article 6 – Security Risk management

1. 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.
2. 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.

Article 7 – Implementation of this Decision

1. Following the adoption by the Agency's Administrative Board of this Decision, the Security Authority of the Agency may develop any necessary implementing rules, security policies, processes, procedures, or notices setting out security guidelines and best practices within the scope of this Decision and its implementing rules.
2. The Agency departments shall take all necessary measures falling under their responsibility in order to ensure that, when handling or storing EUCI or any other classified information, this Decision and the relevant implementing rules are applied.
3. The security measures taken in implementation of this Decision shall be compliant with the principles for security in the Agency laid down in Article 3 of the European Union Agency for the Space Programme Decision on Security in the Agency, as adopted by the Administrative Board of the Agency.
4. The Executive Director of the Agency shall set up the Security Authority of the Agency. The Security Authority of the Agency shall have the responsibilities assigned to it by this Decision and its implementing rules.
5. Within each site (or premises, if needed) of the Agency, the Local Security Officer (LSO), as referred to in Article 20 of the European Union Agency for the Space Programme Decision on Security in the Agency, as adopted by the Administrative Board of the Agency, shall have the following overall responsibilities for protecting EUCI in accordance with this Decision, under the Security Authority's directives:
   a. managing requests for security authorisations for staff;
   b. contributing to security training and awareness briefings;
   c. supervising the site's Registry Control Officer (RCO);
   d. reporting on breaches of security and compromise of EUCI;
   e. holding spare keys and a written record of each combination setting;

f. assuming other tasks related to the protection of EUCI or defined by implementing rules.

6. The Security Authority shall be supported in its activities by the Agency Central Security Office which will be in charge of the Agency corporate security activities.

Article 8 – Breaches of security and compromise of EUCI

1. A breach of security occurs as a result of an act or omission by an individual which is contrary to the security rules laid down in this Decision and its implementing 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 Security Authority of the Agency.
4. Where it is known or where there are reasonable grounds to assume that EUCI has been compromised or lost, a security inquiry shall be conducted in accordance with Article 13 of the European Union Agency for the Space Programme Decision on Security in the Agency.
5. All appropriate measures shall be taken 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.
6. 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 Staff 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.

CHAPTER 2 – PERSONNEL SECURITY

Article 9 – Basic Principles

1. An individual shall only be granted access to EUCI after
   a. his/her need-to-know has been determined;
   b. he/she has been briefed on the security rules for protecting EUCI and the relevant security standards and guidelines, and has acknowledged his/her responsibilities with regard to protecting such information;

c. for information classified CONFIDENTIEL UE/EU CONFIDENTIAL and above, he/she has been security authorised to the relevant level.

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/her 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 Security Authority of the Agency shall be solely responsible for liaising with the national security authorities (NSAs) or other competent national authorities in the context of all security clearance issues. All contacts between the Agency services and their staff, and the NSAs and other competent authorities shall be conducted through the Security Authority services.

Article 10 – Security authorisation procedure

1. Each Head of Department within the Agency shall identify the positions within his/her department 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 LSO of the Agency site or premises concerned shall inform the Security Authority of the Agency, which shall transmit to the individual the security clearance questionnaire issued by the NSA of the Member State under whose nationality the individual has been appointed as a staff member of the Agency. The individual shall consent in writing to being submitted to the security clearance procedure and return the completed questionnaire within the shortest deadline to the Security Authority of the Agency.
3. The Security Authority of the Agency shall forward the completed security clearance questionnaire to the NSA of the Member State under whose nationality the individual has been appointed as a staff member of the Agency, 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 Security Authority of the Agency concerning an individual who has applied for a security clearance, the Security Authority of the Agency, acting in accordance with the relevant rules and regulations, shall notify the competent NSA thereof.
5. Following completion of the security investigation, and as soon as possible after having been notified by the relevant NSA of its overall assessment of the findings of the security investigation, the Security Authority of the Agency:
   a. may grant authorisation for access to EUCI to the individual concerned and authorise access to EUCI up to the relevant level until a date specified by the Security Authority of the Agency 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 Security Authority of the Agency, who in turn may ask the competent NSA 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 authorisation to access EUCI for the Security Authority of the Agency is granted by the Executive Director.
7. 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 Security Authority of the Agency shall be subject to appeals in accordance with the Staff Regulations.
8. The Agency shall issue the authorisation for access to EUCI on the basis of the authorisation for access to EUCI granted by any Union institution, body or agency provided it remains valid. The Security Authority of the Agency will, upon the individual taking up the employment in the Agency, notify the relevant NSA of the change of employer.
9. 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 Security Authority of the Agency, or if there is a break of 12 months in an individual's service, during which time s/he has not been employed by the Agency or by a Union Institution, body or agency, or in a position with a national administration of a Member State, the Security Authority of the Agency shall refer the matter to the relevant NSA for confirmation that the security clearance remains valid and appropriate.
10. Where information becomes known to the Security Authority of the Agency concerning a security risk posed by an individual who holds a valid security authorisation, the Security

Authority of the Agency, acting in accordance with the relevant rules and regulations, shall notify the competent NSA thereof.

11. Where an NSA notifies the Security Authority of the Agency of the withdrawal of an assurance given in accordance with paragraph 5(a) for an individual who holds valid authorisation for access to EUCI, the Security Authority of the Agency may ask for any clarification the NSA can provide according to its national laws and regulations. If the adverse information is confirmed by the relevant NSA, the security 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/she might endanger security.
12. Any decision to withdraw or suspend authorisation for access to EUCI from any individual falling under the scope of this Decision, and, where appropriate, the reasons for doing so, shall be notified to the individual concerned, who may ask to be heard by the Security Authority of the Agency. Information provided by an NSA shall be subject to the relevant laws and regulations in force in the Member State concerned. Decisions made in this context by the Security Authority of the Agency shall be subject to appeals in accordance with the Staff Regulations.
13. Agency Departments shall make sure that national experts seconded to them for a position requiring security authorisation to access EUCI shall present, prior to taking up their assignment, a valid PSC or Personnel Security Clearance Certificate (PSCC), according to national law and regulations, to the Security Authority of the Agency, who, on the basis thereof, shall grant security authorisation for access to EUCI up to the level equivalent to that referred to in the national security clearance, with a maximum validity for the duration of their assignment.

Security clearance and security authorisation records

14. Records of security clearances and authorisations granted for access to EUCI shall be maintained by the Security Authority of the Agency in accordance with this Decision. These records shall contain as a minimum the level of EUCI to which the individual may be granted access, the date of issue of the security clearance and its period of validity.
15. The Security Authority of the Agency 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.

Renewal of security authorisations

16. After the initial granting of security authorisations and provided that the individual has had uninterrupted service with the Agency 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, until the expiration date of the PSC.
17. The Security Authority of the Agency may extend the validity of the existing security authorisation for a period of up to 12 months after the expiration of the PSC, if no adverse information has been received from the relevant NSA, DSA 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, DSA or other competent national authority has not notified the Security Authority of the Agency of its opinion, the individual shall be assigned to duties which do not require a security authorisation.

Article 11 – Security authorisation briefings

1. After having participated in the security authorisation briefing organised by the Security Authority of the Agency, all individuals to be security authorised shall acknowledge in writing that they have understood their obligations with respect to protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the Security Authority of the Agency.
2. 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 Security Authority of the Agency 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.

Article 12 – Temporary security authorisation

1. In exceptional circumstances, where duly justified in the interests of the service and pending completion of a full security investigation, the Security Authority of the Agency, may, after consulting the NSA of the Member State of which the individual is a national and subject to the outcome of preliminary checks to verify that no relevant adverse information is known, 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 having been briefed in accordance with Article 11(1), 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 Security Authority of the Agency.

Article 13 – Attendance at classified meetings organised by the Agency

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

2. Individuals assigned to participate in meetings organised by the Agency 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 the Security Authority of the Agency has not seen a PSCC or other proof of security clearance, or, to participants of the Agency who are not in possession of a security authorisation.
3. Before organising a classified meeting, the meeting organiser responsible or the LSO of the site or premises organising the meeting, shall request external participants to provide the Security Authority of the Agency with a PSCC or other proof of security clearance. The Security Authority of the Agency shall inform the LSO or the meeting organiser of PSCCs or other proof of PSC received. Where applicable, a consolidated list of names may be used, giving the relevant proof of security clearance.
4. Where the Security Authority of the Agency is informed by the competent authorities that a PSC has been withdrawn from an individual whose duties require attendance at meetings organised by the Agency, the Security Authority of the Agency shall notify the LSO of the site or premises where the meeting is organised.
5. The provisions above apply to any type of classified meeting, including, but not limited to, Security Accreditation Board meetings, or Administrative Board meetings, even in their restricted formation under Article 75(5) of the Space Regulation 2021/696[5].

Article 14 – Potential Access to EUCI

Couriers, guards and escorts shall be security authorised to the appropriate 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.

CHAPTER 3 – PHYSICAL SECURITY AIMED AT PROTECTING CLASSIFIED INFORMATION

Article 15 – 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 this Decision and its implementing rules.

[5] Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU

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 all premises, buildings, offices, rooms and other areas in which EUCI is handled or stored, including areas housing communication and information systems as referred to in Chapter 5.
4. Areas in which EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is stored shall be established as Secured Areas in accordance with this Chapter and accredited by the Security Accreditation Authority of the Agency.
5. Only equipment or devices approved by the Security Authority of the Agency shall be used for protecting EUCI at the level CONFIDENTIEL UE/EU CONFIDENTIAL or above. This approval shall be based on the Commission's rules on equipment or devices used for protecting EUCI.

Article 16 – Physical security requirements and measures

1. Physical security measures shall be selected on the basis of a threat assessment made by the Security Authority of the Agency, where appropriate in consultation with other departments of the Agency, Union institutions, agencies or bodies and/or competent authorities in the Member States. The Agency 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 Security Authority of the Agency, applying the concept of defence in depth, shall determine the appropriate combination of physical security measures to be implemented. To that effect, the Security Authority of the Agency shall develop minimum standards, norms and criteria, set out in implementing rules; those standards and norms shall be based on the minimum standards, norms and criteria developed by the Commission Security Authority.

3. The Security Authority of the Agency 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 premises.
4. When EUCI is at risk of being overlooked, even accidentally, the Agency departments concerned shall take the appropriate measures, as defined by the Security Authority of the Agency, to counter this risk.
5. For new facilities, physical security requirements and their functional specifications shall be defined with the consent of the Security Authority of the Agency as part of the planning and design of the facilities. For existing facilities, physical security requirements shall be implemented in accordance with the minimum standards, norms and criteria set out in implementing rules.

Article 17 – 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 Security Accreditation Authority of the Agency 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 and, where possible, vehicles to be checked;
   b. unescorted access shall be granted only to individuals who are duly authorised by the Security Authority of the Agency or any other competent authority; and
   c. all other individuals shall be escorted at all times or be subject to equivalent controls.
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. Any keys shall be managed in accordance with Article 19;
   b. all persons and material entering such areas shall be controlled;
   c. The Security Authority of the Agency shall ensure that such areas are regularly physically and/or technically inspected. 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 communications devices and electrical or electronic equipment shall first be examined by the Security Authority of the Agency 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. The LSO shall draw up Security Operating Procedures (SecOPs) for each Secured Area under his/her responsibility stipulating, in accordance with the provisions of this Decision and its implementing rules:
    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 Security Authority of the Agency and afford protection equivalent to a security container approved for the storage of EUCI of the same classification level.

Article 18 – 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 in accordance with Article 30 and has undertaken to comply with compensatory measures, set out in implementing 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 laid down in implementing rules.
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 and compensatory measures, set out in implementing rules, are complied with; or
   c. outside a Secured Area or an Administrative Area provided the holder:
      i. has undertaken to comply with compensatory measures, set out in implementing rules, to ensure the EUCI is protected from access by unauthorised persons;
      ii. keeps the EUCI at all times under his/her personal control; and
      iii. 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.
5. EUCI which is classified TRES SECRET UE/EU TOP SECRET shall be handled in a Secured Area, set up and maintained by the Security Authority of the Agency, and accredited to that level by the Security Accreditation Authority of the Agency.
6. EUCI which is classified TRES SECRET UE/EU TOP SECRET shall be stored in a Secured Area, accredited to that level by the Security Accreditation Authority of the Agency, under one of the following conditions:
   a. in a security container in accordance with the provisions of Article 17 with one or more of the following supplementary controls:
      i. continuous protection or verification by cleared security staff or duty personnel;
      ii. an approved IDS in combination with security response personnel; or
   b. in an IDS-equipped strong room in combination with security response personnel.

Article 19 – Management of keys and combinations used for protecting EUCI

1. Procedures for managing keys and combination settings for offices, rooms, strong rooms and security containers shall be laid down in implementing rules according to Article 7. Such procedures 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.

CHAPTER 4 – MANAGEMENT OF EU CLASSIFIED INFORMATION

Article 20 – Basic principles

1. All EUCI documents should be managed in compliance with the Agency's policy on document management and consequently should be registered, filed, preserved and finally eliminated, sampled or transferred to the Historical Archives in accordance with the common Agency-level retention list for the Agency files.
2. Information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be registered for security purposes prior to distribution and on receipt. Information classified TRES SECRET UE/EU TOP SECRET shall be registered in a designated registry.
3. Within the Agency, an EUCI registry system shall be set up in accordance with the provisions of Article 26.
4. Agency premises where EUCI is handled or stored shall be subject to regular inspection by the Security Authority of the Agency.
5. 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 Chapter 5;
   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 Chapter 5; or
      ii. in all other cases, as prescribed in implementing rules.

Article 21 – Classifications and markings

1. Information shall be classified where it requires protection with regard to its confidentiality, in accordance with Article 3(1).
2. The originator of EUCI shall be responsible for determining the security classification level, in accordance with the relevant implementing rules, standards and guidelines regarding classification, and for the initial dissemination of the information.
3. The classification level of EUCI shall be determined in accordance with the relevant implementing rules.
4. The security classification shall be clearly and correctly indicated, regardless of whether the EUCI is on paper, oral, electronic or in any other form.
5. 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.
6. 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.
7. 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.
8. 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

Article 22 – Markings

In addition to one of the security classification markings set out in Article 3(1), 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.

Article 23 – 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:

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

Article 24 – 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. documents classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall bear a registration number and all EUCI documents shall bear a subject, which is not itself classified information, unless it is marked as such;
   d. the document shall bear a date;
   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.
2. Where it is not possible to apply paragraph 1 to EUCI, other appropriate measures shall be taken in accordance with implementing rules.

Article 25 – 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. Each Agency department 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 the Agency no less frequently than every five years shall be established by implementing rules. 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 having originated in the Agency 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 1700/20036[5].

Article 26- EUCI registry system in the Agency

1. Without prejudice to Article 49 paragraph 5 below, in every Agency site where EUCI is handled or stored at the level of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET, a responsible local EUCI registry shall be identified to ensure that EUCI is handled in accordance with this Decision. The establishment of each local registry shall be authorised by the Security Authority of the Agency.
2. The EUCI registry established at the Agency headquarters shall act as:
   a. the local EUCI registry for the Agency's headquarters,
   b. the EUCI registry for sites or services which do not have a local EUCI registry,
   c. the main point of entry and exit for all information classified RESTREINT UE/EU RESTRICTED and up to and including SECRET UE/EU SECRET exchanged between the Agency and Member States, as well as third States and international organisations, and for Union institutions, agencies and bodies, unless specified differently in specific arrangements.
3. If information classified TRES SECRET UE/EU TOP SECRET has to be handled within the Agency, a registry shall be designated by the Security Authority of the Agency to act as the central receiving and dispatching authority for information classified TRES SECRET UE/EU TOP SECRET. Where necessary, local registries may be designated to handle that information for registration purposes.
4. The local registries may not transmit TRES SECRET UE/EU TOP SECRET documents directly to other local registries or externally without the express written approval of the central TRES SECRET UE/EU TOP SECRET registry.
5. EUCI registries shall be established as Secured Areas as defined in Chapter 3, and accredited by the Security Accreditation Authority (SAA) of the Agency.

Article 27 – Registry Control Officer

1. Each EUCI registry shall be managed by a Registry Control Officer (RCO).
2. The RCO shall be appropriately security-cleared.
3. The RCO shall be subject to the supervision of the LSO within the Agency site, as far as the application of the provisions regarding the handling of EUCI documents and compliance with the relevant security rules, standards and guidelines is concerned.

[6] Council Regulation (EC, Euratom) No 1700/2003 of 22 September 2003 amending Regulation (EEC, Euratom) No 354/83 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community (OJ L 243, 27.9.2003, p. 1)

4. Within his/her responsibility for managing the EUCI Registry to which he/she has been assigned, the RCO shall assume the following overall tasks in accordance with this Decision and the relevant implementing rules, standards and guidelines:
   a. manage operations relating to the registration, preservation, reproduction, translation, transmission, dispatch and destruction of EUCI,
   b. verify periodically the need to maintain the classification of information,
   c. assume any other tasks related to the protection of EUCI defined in implementing rules.

Article 28 – Registration of EUCI for security purposes

1. For the purposes of this Decision, registration for security purposes (hereinafter referred to as 'registration') means the application of procedures which record the life-cycle of EUCI, including its dissemination.
2. All information or material classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be registered in designated registries when it is received in or dispatched from an organisational entity.
3. When EUCI is handled or stored using a Communication and Information System (CIS), registration procedures may be performed by processes within the CIS itself.
4. More detailed provisions concerning the registration of EUCI for security purposes shall be laid down in implementing rules.

Article 29 – Copying and translating EU classified documents

1. TRES SECRET UE/EU TOP SECRET documents shall not be copied or translated without the prior written consent of the originator.
2. 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.
3. The security measures applicable to the original document shall apply to copies and translations thereof.

Article 30 – 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 an Agency building or a self-contained group of Agency buildings,
      - between Agency buildings located in the same Member State,

- within the Union,
- from within the Union to the territory of a third State, and

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

3. These protective measures shall be laid down in detail in implementing rules, or, in case of projects and programmes referred to in Article 38, as an integral part of the relevant Programme or Project Security Instructions (PSI).
4. The implementing rules or PSI shall include provisions commensurate with the level of EUCI, regarding:
   a. the type of carriage, such as hand carriage, carriage by diplomatic or military courier, carriage by postal services or 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, and notwithstanding Article 20, paragraph 5, the protective measures set out in the relevant implementing rules may be supplemented by appropriate technical countermeasures approved by the Security Authority of the Agency so as to minimise the risk of loss or compromise.

Article 31 – Destruction of EUCI

1. EU classified documents which are no longer required may be destroyed, taking into account regulations on archives and the Agency's rules and regulations on document management and archiving.
2. EUCI of the level of CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be destroyed by the RCO of the responsible EUCI registry on instruction from the holder or from a competent authority. The RCO shall update the logbooks and other registration information accordingly.
3. For documents classified SECRET UE/EU SECRET or TRES SECRET UE/EU TOP SECRET, such destruction shall be performed by the RCO in the presence of a witness who shall be cleared to at least the classification level of the document being destroyed.
4. 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 RCO of the responsible EUCI registry shall keep destruction certificates of TRES SECRET UE/EU TOP SECRET documents for a period of at least ten years and 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 implementing rules and which shall meet relevant EU or equivalent standards.

6. Computer storage media used for EUCI shall be destroyed in accordance with procedures laid down in implementing rules.

Article 32 – Destruction of EUCI in emergencies

1. Agency premises holding EUCI 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 no circumstances adversely affect the safeguarding or destruction of TRES SECRET UE/EU TOP SECRET material, including the 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 laid down in implementing rules.

CHAPTER 5 – PROTECTION OF EU CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

Article 33 – Basic principles of Information Assurance

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.
2. Effective Information Assurance shall ensure appropriate levels of:
   a. Authenticity: the guarantee that information is genuine and from *bona fide* sources;
   b. Availability: the property of being accessible and usable upon request by an authorised entity;
   c. Confidentiality: the property that information is not disclosed to unauthorised individuals, entities or processes;
   d. Integrity: the property of safeguarding the accuracy and completeness of assets and information;
   e. 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. The Agency ICT Risk Management Methodology shall be specified in the Agency ICT Security Strategy.

Article 34 – CIS handling EUCI

1. CIS shall handle EUCI in accordance with the concept of IA.
2. For Agency CIS handling EUCI, compliance with the Agency's information systems security policy, also referred to as the Agency ICT Security Policy, implies that:
   a. the Plan-Do-Check-Act approach shall be applied for the implementation of the information systems security policy during the full life-cycle 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;
   d. all mandatory security measures as determined by the policy on security of information systems must be implemented;
   e. 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;
   f. 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 CIS handling EUCI shall notify to the SAA all potential security weaknesses, incidents, breaches of security or compromise which may have an impact on the protection of the CIS and/or the EUCI therein.
4. Where the protection of EUCI handled by Agency CIS is provided by cryptographic products, 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 shall be approved.
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 CAA.
6. Security measures shall be implemented to protect CIS 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.
7. The Security Authority of the Agency shall assume the following functions:
   a. IA Authority (IAA)
   b. Security Accreditation Authority (SAA)
   c. TEMPEST Authority (TA)
   d. Crypto Approval Authority (CAA)

e. Crypto Distribution Authority (CDA).

8. The Security Authority of the Agency shall appoint for each Agency CIS the IA Operational Authority (IAOA).
9. The responsibilities of the functions described in paragraphs 7 and 8 are defined in Chapter 4 of the European Union Agency for the Space Programme Decision on Security in the Agency.

Article 35 – Accreditation of CIS handling EUCI

1. All CIS 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 for Agency CIS shall include the formal validation by the Agency SAA of the Security Plan for the CIS concerned in order to obtain assurance that:
   a. the risk management process, as referenced in Article 34(2), has been properly carried out;
   b. the system owner has knowingly accepted the residual risk; and
   c. a sufficient level of protection of the CIS, and of the EUCI handled in it, has been achieved in accordance with this decision.
3. The SAA of the Agency shall issue an accreditation statement which determines the maximum classification level of the EUCI that may be handled in the Agency CIS as well as the corresponding terms and conditions for operation. This is without prejudice to the tasks entrusted to the Security Accreditation Board established in Chapter II of Regulation (EU) 2021/696 of the European Parliament and of the Council.
4. A joint Security Accreditation Board (SAB) shall be responsible for accrediting Agency CIS involving several parties. It shall be composed of a SAA representative of each party involved and be chaired by an SAA representative of the Agency.
5. The accreditation process shall consist of a series of tasks to be assumed by the parties involved. The responsibility for the preparation of the accreditation files and documentation shall rest entirely upon the CIS System Owner.
6. The accreditation of Agency CIS shall be the responsibility of the SAA of the Agency, who, at any moment in the life cycle of the CIS, shall have the right to:
   a. require that an accreditation process be applied;
   b. audit or inspect the CIS;
   c. where 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 CIS until conditions for operation are again satisfied.
7. The accreditation process shall be established in the Agency policy on the Accreditation Process for Agency CIS handling EUCI.

Article 36 – Emergency circumstances

1. Notwithstanding the provisions of this Chapter, 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 out in paragraph 1) 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.
4. A subsequent report shall be made to the competent authority as well as to the Security Authority of the European Commission.

CHAPTER 6 – INDUSTRIAL SECURITY

Article 37 – Basic principles

1. Industrial security is the application of measures to ensure the protection of EUCI
   a. within the framework of classified contracts, by:
      i. candidates or tenderers throughout the tendering and contracting procedure;
      ii. contractors or subcontractors throughout the life-cycle of classified contracts;
   b. within the framework of classified grant agreements, by
      i. applicants during grant award procedures;
      ii. grant beneficiaries or subcontractors throughout the life-cycle of classified grant agreements.
2. Such contracts or grant agreements shall not involve information classified TRES SECRET UE/EU TOP SECRET.
3. Unless stated otherwise, provisions in this Chapter referring to classified contracts or contractors shall be applicable also to classified subcontracts or subcontractors.

Article 38 – Procedure for classified contracts or grant agreements

1. The Agency, as contracting or granting authority, shall ensure that the minimum standards on industrial security set out in this Chapter, are referred to or incorporated in

the contract or grant agreement, and complied with when awarding classified contracts or classified grant agreements.

2. For the purposes of paragraph 1), the departments within the Agency shall seek the advice of the Security Authority and shall ensure that model contracts and subcontracts and model grant agreements include provisions reflecting the basic principles and minimum standards for protecting EUCI to be complied with by contractors and subcontractors within classified contracts, and respectively grant beneficiaries and subcontractors within the classified grant agreements.
3. The Agency shall closely cooperate with the NSAs, DSAs or any other competent authorities of the Member States concerned.
4. When a contracting or granting authority intends to launch a procedure aimed at concluding a classified contract or grant agreement, it shall seek the advice of the Security Authority of the Agency on issues regarding the classified nature and elements of the procedure, during all its stages.
5. Templates for and models of classified contracts and subcontracts, classified grant agreements, contract notices, guidance on the circumstances where Facility Security Clearances (FSCs) are required, Programme or Project Security Instructions (PSI), Security Aspects Letters (SALs), visits, transmission and carriage of EUCI under Classified Contracts or Classified Grant Agreements shall be laid down in Implementing Rules on industrial security.
6. The Agency may conclude classified contracts or grant agreements which entrust tasks involving or entailing access to or the Handling or storage of EUCI by economic operators registered in a Member State or in a third State with which an agreement or an administrative arrangement has been concluded in accordance with Chapter 7 of this Decision.

Article 39 – Security elements in a classified contract or grant agreement

1. Classified contracts or grant agreements shall include a Security Classification Guide and a Security Aspects Letter, and may additionally include a Programme or Project Security Instruction.

   Security Aspects Letter

   a. 'Security Aspects Letter' (SAL) means a set of special contractual conditions, issued by the contracting or granting authority, which forms an integral part of any classified contract or grant agreement involving access to or the creation of EUCI, that identifies the security requirements and those elements of the contract or grant agreement requiring security protection.
   b. The contract- or grant agreement-specific security requirements shall be described in a SAL. The SAL shall contain the Security Classification Guide (SCG) and shall be an integral part of a classified contract or sub-contract, or grant agreement.

c. The SAL shall contain the provisions requiring the contractor or grant beneficiary to comply with the minimum standards laid down in this Decision. The contracting or granting authority shall ensure the SAL indicates that non-compliance with these minimum standards may constitute sufficient grounds for the contract or the grant agreement to be terminated.

Programme or Project Security Instruction

a. 'Programme or Project Security Instruction' (PSI) means a list of security procedures which are applied to a specific programme or project in order to standardise security procedures. It may be revised throughout the programme or project.
b. The Security Authority shall develop a generic PSI. The Agency Departments responsible for programmes or projects involving handling or storage of EUCI may develop, where appropriate, specific PSIs, which shall be based upon the generic PSI.
c. A specific PSI shall be developed in particular for programmes and projects characterised by their considerable scope, scale or complexity, or by the multitude and/or the diversity of contractors, grant beneficiaries and other partners and stakeholders involved, for instance as regards their legal status. The specific PSI shall be developed by the Agency department(s) managing the programme or project, in close cooperation with the Security Authority.
d. The Security Authority shall submit both the generic and specific PSIs for advice to the Commission.
e. The Agency shall use and implement specific PSI issued by the Commission for specific programmes or projects.

2. The SALs shall include a SCG as a mandatory security element:
   a. 'Security Classification Guide' (SCG) means a document which describes the elements of a programme, project, contract or grant agreement which are classified, specifying the applicable security classification levels. The SCG may be expanded throughout the life of the programme, project, contract or grant agreement and the elements of information may be re-classified or downgraded.
   b. Prior to launching a call for tender or letting a classified contract, or launching a call for proposals or signing a grant agreement, the Agency, as contracting or granting authority, shall determine the security classification of any information to be provided to candidates, tenderers or contractors, or applicants or grant beneficiaries, as well as the security classification of any information to be created by the contractor or grant beneficiary. For that purpose, it shall prepare an SCG to be used for the performance of the contract or grant agreement, in accordance with this Decision and its implementing rules, after consulting the Security Authority of the Agency.
   c. In order to determine the security classification of the various elements of a classified contract or grant agreement, the following principles shall apply:

i. in preparing a SCG, the Agency, as the contracting or granting authority, shall take into account all relevant security aspects, including the security classification assigned to information provided and approved to be used for the contract or grant agreement by the originator of the information;
ii. the overall level of classification of the contract or grant agreement may not be lower than the highest classification of any of its elements; and
iii. where relevant, the contracting or granting authority shall liaise, through the Security Authority of the Agency, with the Member States' NSAs or any other competent security authority concerned in the event of any changes regarding the classification of information created by or provided to contractors or grant beneficiaries in the performance of a contract or grant agreement and when making any subsequent changes to the SCG.

Article 40 – Access to EUCI for contractors' and grant beneficiaries' staff

The contracting or granting authority, shall ensure that the classified contract or classified grant agreement includes provisions indicating that staff of a contractor, subcontractor or grant beneficiary who, for the performance of the classified contract, subcontract or grant agreement, require access to EUCI, shall be granted such access only if:

a. they have been security authorised to the relevant level and their need-to-know has been determined;
b. they have been briefed on the applicable security rules for protecting EUCI, and have acknowledged 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.

Article 41 – Facility security clearance

1. 'Facility Security Clearance' (FSC) means an administrative determination by an NSA, DSA or any other competent security authority that, from the security viewpoint, a facility can afford an adequate level of protection to EUCI to a specified security classification level.
2. A FSC granted by the NSA, DSA or any other competent security authority of a Member State to indicate, in accordance with national laws and regulations, that an economic operator can protect EUCI at the appropriate classification level (CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET) within its facilities, shall be presented to the Security Authority of the Agency, which will forward it to the Agency department acting as the contracting or granting authority, before a candidate, tenderer or contractor, or grant applicant or beneficiary may be provided with or granted access to EUCI.
3. Where relevant, the contracting or granting authority shall notify, through the Security Authority of the Agency, the appropriate NSA, DSA or any other competent security

authority that an FSC is required for performing the contract or grant agreement. An FSC or PSC shall be required where EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has to be provided in the course of the procurement or grant award procedure.

4. The contracting or granting authority shall not sign a classified contract or a grant agreement before receiving confirmation from the NSA, DSA or any other competent security authority of the Member State in which the contractor or grant beneficiary concerned is registered that, where required, an appropriate FSC has been issued.
5. When the Security Authority of the Agency has been notified by the NSA, DSA or any other competent security authority which has issued an FSC about changes affecting the FSC, it shall inform the Agency department acting as contracting or granting authority. In the case of a sub-contract, the NSA, DSA or any other competent security authority shall be informed accordingly.
6. Withdrawal of an FSC by the relevant NSA, DSA or any other competent security authority shall constitute sufficient grounds for the contracting or granting authority, to terminate a classified contract or exclude a candidate, tenderer or applicant from the competition. A provision to that effect shall be included in the model contracts and grant agreements to be developed.

Article 42 – Provision for classified and grant agreements

1. Where EUCI is provided to a candidate, tenderer or applicant during the procurement procedure, the call for tender or call for proposal shall contain a provision obliging the candidate, tenderer or applicant failing to submit a tender or proposal or who is not selected, to return all classified documents within a specified period of time.
2. The contracting or granting authority, shall notify, through the Security Authority of the Agency, the competent NSA, DSA or any other competent security authority of the fact that a Classified Contract or grant agreement has been awarded, and of the relevant data, such as the name of the contractor(s) or grant beneficiaries, the duration of the contract and the maximum level of classification.
3. When such contracts or grant agreements are terminated, the contracting or granting authority, shall promptly notify, through the Security Authority of the Agency, the NSA, DSA or any other competent security authority of the Member State in which the contractor or grant beneficiary is registered.
4. As a general rule, the contractor or grant beneficiary shall be required to return to the contracting or granting authority, upon termination of the classified contract or the grant agreement, or of the participation of a grant beneficiary, any EUCI held by it.
5. Specific provisions for the disposal of EUCI during the performance of the classified contract or the classified grant agreement or upon its termination shall be laid down in the SAL.

6. Where the contractor or grant beneficiary is authorised to retain EUCI after termination of a classified contract or grant agreement, 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 the grant beneficiary.

Article 43 – Specific provisions for classified contracts

1. The conditions relevant for the protection of EUCI under which the contractor or grant beneficiary may subcontract shall be defined in the call for tender or call for proposals, and in the classified contract or grant agreement.
2. A contractor or grant beneficiary shall obtain permission from the contracting or granting authority, before sub-contracting any parts of a classified contract or grant agreement. No subcontract involving access to EUCI may be awarded to subcontractors registered in a third country, unless there is a regulatory framework for the security of information as provided for in Chapter 7.
3. The contractor or grant beneficiary 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 or granting authority.
4. With regard to EUCI created or handled by the contractor or grant beneficiary, the Agency shall be considered to be the originator, and save provided otherwise by the Union Space Programme, the rights incumbent on the originator shall be exercised by the contracting or granting authority.

Article 44 – Visits in connection with classified contracts or grant agreements

1. Where an Agency staff member or contractors' or grant beneficiaries' 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 or grant agreement, visits shall be arranged in liaison with the NSAs or any other competent security authority concerned. The Security Authority of the Agency shall be informed of such visits. However, in the context of specific programmes or projects, the NSAs or any other competent security authority may also agree on a procedure whereby such visits can be arranged directly.
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 or grant agreement.
3. Visitors shall be given access only to EUCI related to the purpose of the visit.
4. More detailed provisions shall be set out in implementing rules.
5. Compliance with the provisions regarding visits in connection with classified contracts or grant agreements, set out in this Decision and in the implementing rules referred to in paragraph 4), shall be mandatory.

Article 45 – Transmission and carriage of EUCI in connection with classified contracts or classified grant agreements

1. With regard to the transmission of EUCI by electronic means, the relevant provisions of Chapter 5 of this Decision shall apply.
2. With regard to the carriage of EUCI, the relevant provisions of Chapter 4 of this Decision and its implementing rules 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.

Article 46 – Transfer of EUCI to contractors or grant beneficiaries located in third States

EUCI shall be transferred to contractors or grant beneficiaries located in third States in accordance with security measures agreed between the Security Authority of the Agency, the contracting or granting authority, and the NSA, DSA or other competent security authority of the concerned third country where the contractor or grant beneficiary is registered.

Article 47 – Handling of information classified RESTREINT UE/EU RESTRICTED in the context of Classified Contracts or Classified Grant Agreements

1. Protection of information classified RESTREINT UE/EU RESTRICTED handled or stored under classified contracts or grant agreements 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 or classified grant agreements involving the handling of information classified at the level of RESTREINT UE/EU RESTRICTED.

3. Where a contract or grant agreement involves handling of information classified RESTREINT UE/EU RESTRICTED in a CIS operated by a contractor or grant beneficiary, the contracting or granting authority shall ensure, after consulting the Security Authority of the Agency, that the contract or grant agreement specifies the necessary technical and administrative requirements regarding accreditation or approval of the CIS commensurate with the assessed risk, taking account of all relevant factors. The scope of accreditation or approval of such CIS shall be agreed between the Security Authority of the Agency and the relevant NSA or DSA.

CHAPTER 7 - EXCHANGE OF CLASSIFIED INFORMATION WITH OTHER UNION INSTITUTIONS, AGENCIES, BODIES AND OFFICES, WITH MEMBER STATES, AND WITH THIRD STATES AND INTERNATIONAL ORGANISATIONS

Article 48 – Basic principles

1. Working arrangements involving access to EUCI may only be concluded with the relevant authorities of third States or international organisations with which the Commission has already entered into an Administrative Arrangement[7] or a Security of Information Agreement within the meaning of Chapter 7 of Commission Decision 2015/444 has already been concluded.
2. Where in the absence of an administrative or working arrangement the Agency or one of its departments determines there is an exceptional need in the context of a Union political or legal framework to release EUCI to a third State or an international organisation, the Agency Security Authority shall consult the Commission and receive its prior approval before the Executive Director can decide to proceed to any ad hoc release of EUCI to such authorities.
3. EUCI may only be shared with a Union institution, agency, body or office which has equivalent basic principles and minimum standards for protecting EUCI in place and if there is an appropriate legal or administrative framework to that effect, which may include administrative arrangements concluded in accordance with the relevant regulations.
4. The decision to release EUCI originating in the Agency shall be taken by the Agency department, as originator of this EUCI within the Agency, 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 the Agency,

[7] In accordance with Article 56 of Commission Decision 2015/444, as a general rule Administrative Arrangements with third States and international organisations allow the exchange of classified information no higher than RESTREINT UE/EU RESTRICTED.

the Agency department which holds this classified information, shall first seek the originator's written consent to release. If the originator cannot be established, the Agency department, which holds this classified information, shall assume the former's responsibility after consulting the Commission.

Article 49 – Sharing of EUCI with Union institutions, agencies, bodies and offices

1. Before entering into an administrative arrangement for sharing EUCI with a Union Institution, agency, body or office, the Agency 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 this Decision and its implementing rules;
   b. applies security standards and guidelines regarding personnel security, physical security, management of EUCI and security of Communication and Information Systems (CIS), which guarantee an equivalent level of protection of EUCI as that afforded in the Agency.
   c. marks classified information which it creates as EUCI.
2. The Agency Security Authority shall, in close cooperation with the Directorate-General Human Resources and Security of the Commission, be the lead service within the Agency for the preparation of administrative arrangements referred to in paragraph 1.
3. Administrative arrangements shall as a general rule take the form of an exchange of letters, signed by the Executive Director on behalf of the Agency.
4. Before entering into an administrative arrangement on sharing EUCI, the Agency Security Authority shall ensure that an assessment visit has been conducted aimed at assessing the regulatory framework for protecting EUCI and ascertaining the effectiveness of measures implemented for protecting EUCI. The administrative arrangement shall enter into force, and EUCI shall be shared, only if the outcome of this assessment visit is satisfactory and the recommendations made further to the visit have been complied with. Regular follow-up assessment visits 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.
5. Within the Agency, the EUCI registry established in headquarters shall be the main point of entry and exit for classified information shared with Union institutions, agencies, bodies and offices. However, owing to security, organisational or operational grounds it may be more appropriate, with a view to protecting EUCI, for local EUCI registries to operate as the point of entry and exit for classified information regarding matters within the competence of the Agency's sites concerned.
6. The Executive Director shall be informed of the process of concluding administrative arrangements pursuant to paragraph 2.

Article 50 –Sharing of EUCI with Member States

1. EUCI may be shared with 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 1 of the Inter-Governmental Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union (2011/C 202/05) or Annex I of Commission Decision (EU, Euratom) 2015/444, as latest updated.
2. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the European 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 Annex 1 of the Inter-Governmental Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union (2011/C 202/05) or Annex I of Commission Decision (EU, Euratom) 2015/444, as latest updated.

Article 51 – Exchange of EUCI with third States and international organisations

1. Any administrative arrangements established by the Agency within the meaning of Article 48 (1) shall ensure, by means of an onsite visit conducted prior to the conclusion of the arrangement, that EUCI is given protection appropriate to its classification level and according to minimum standards which are laid down in this Decision.
2. The Agency Security Authority shall, in close cooperation with the Directorate-General Human Resources and Security of the Commission, be the lead service within the Agency for the preparation of administrative arrangements referred to in paragraph 1.
3. The Agency Security Authority shall seek the Commission's prior approval for the conclusion of administrative arrangements established under the conditions of Article 48(1).

Article 52 – Exceptional ad hoc release of EUCI

1. In the absence of an administrative or working arrangement, and where appropriate, the decision to release EUCI to an authority or a body of a third State or an international organisation concerned, shall, after prior approval of the Commission, be taken by the Executive Director on the basis of a proposal by the Agency Security Authority.
2. Following the Executive Director's decision to release EUCI and subject to prior written consent of the originator, including the originators of source material it may contain, the competent Agency registry shall forward the information concerned, which shall bear a

releasability marking indicating the authority of the body of the third State or international organisation to which it has been 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 this Decision.

CHAPTER 8 – FINAL PROVISIONS

Article 53 – Classified information created before the entry into force of this Decision

All EUCI classified in accordance with Decision 2015/444, or any other previous Decision regarding the protection of EUCI, applied by the Agency before the entry into force of this Decision, shall continue to be protected in accordance with the relevant provisions of this Decision.

Article 54- Transparency

This Decision and its implementing rules shall be brought to the attention of Agency staff and to all individuals to whom they apply.