

MANAGEMENT BOARD DECISION 45/2022

of 30 July 2022

**adopting Security Rules of the European Border and Coast Guard Agency
(Frontex)**

THE MANAGEMENT BOARD

Having regard to the European Border and Coast Guard Regulation¹ (hereinafter the 'Regulation'),
in particular Article 92(2) thereof,

Whereas:

- (1) Article 92(1) of the Regulation provides that the European Border and Coast Guard Agency ('Frontex') is to adopt its own security rules to be based on the principles and rules laid down in the Commission's security rules for protecting European Union classified information ('EUCI') and sensitive non-classified information including, inter alia, provisions for the exchange of such information with third countries, and processing and storage of such information as set out in Commission Decisions (EU, Euratom) 2015/4432 on Security in the Commission and (EU, Euratom) 2015/4443 on the security rules for protecting EU classified information.
- (2) Frontex security rules should cover the security of the information systems developed, deployed and operated by the Agency, which serve to exchange classified and sensitive non-classified information with the relevant actors as stipulated in Article 15(2) of the Regulation. The exchange of sensitive non-classified and classified information is to be carried out in a secure manner via the communication network that is established and maintained by Frontex in accordance with Article 14 of the Regulation. Frontex is to provide technical support for the information exchange and permanent availability of the communication network.
- (3) In order to be able to ensure the protection of EUCI and sensitive non-classified information, in the framework of various systems that are established and maintained by Frontex in accordance with Article 15, 18 and 67 of the Regulation, Frontex needs to operate in a safe and secure environment by establishing a coherent integrated approach to its security, providing appropriate levels of protection as concerns persons, including Frontex staff, assets and information, commensurate with any risk identified.
- (4) The security rules should therefore include general rules for the security of the environment where such information is being handled. The safety of Frontex staff and a high level of security in its premises is of paramount importance in order to ensure a safe exchange, processing and storage of sensitive non-classified and classified information. In this context, the Commission Decision (EU, Euratom) 2015/443, which sets out the objectives, basic principles, organization and responsibilities regarding security at the Commission, gives indications for adequate rules to be established by Frontex in this Decision.
- (5) In addition to Commission Decisions (EU, Euratom) 2015/443 and (EU, Euratom) 2015/444,

¹ Regulation (EU) 2019/1896 of 13 November 2019 on the European Border and Coast Guard (OJ L 295, 14.11.2019, p. 1).

Commission Decision (EU, Euratom) 2019/1961², Commission Decision (EU, Euratom) 2019/1962³, Commission Decision (EU, Euratom) 2019/1963⁴, Commission Decision (EU, Euratom) 2017/46⁵ and Commission Implementing Decision C(2018)6575⁶ also contain security rules that are applicable to the Commission and that should also constitute the basis for the security rules of Frontex in relation to the protection and handling of classified information.

- (6) EUROSUR is established by the Regulation as a framework for the European Border and Coast Guard to exchange information, including classified and sensitive non-classified information, and for the operational cooperation between Member States' national authorities and Frontex. It is necessary to ensure data security in EUROSUR in accordance with Chapter III Section 2 of Commission Implementing Regulation (EU) 2021/581⁷ (the "EUROSUR Implementing Regulation"). Due to the fact that Frontex is responsible for the establishment and maintenance of the European components of EUROSUR that are interconnected with national components of Member States, detailed rules should be established regarding the security of data and the technical components of EUROSUR. These detailed rules should be developed in a separate document, without prejudice to the provisions of this Decision.
- (7) This Decision should repeal and replace the Management Board Decision 4/2013 establishing measures for the application of the security principles relating to the processing of non-classified sensitive information.
- (8) In order to ensure that these security rules remain relevant and fit for purpose in the light of organisational, operational and technological developments within Frontex, these security rules should be reviewed regularly and, where necessary, updated.
- (9) In implementing this Decision, Frontex shall comply with the Treaties and in particular the Charter of Fundamental Rights⁸, Protocol No 7 to the Treaty on the Functioning of the European Union on the Privileges and Immunities of the European Union and any rules of national law applicable to the Agency having regard, in particular, to agreements entered into by the Agency pursuant to Articles 60 and 94 of the Regulation, and with the terms of the present Decision.
- (10) In accordance with Article 92(2) of the Regulation, the Commission has given its approval to the security rules on 30th June 2022,

HAS DECIDED AS FOLLOWS:

Article 1

Object

The security rules of the European Border and Coast Guard Agency (Frontex), as set out in the Annex to this Decision, are hereby adopted.

Article 2

Repeal

This Decision repeals and replaces Management Board Decision 4/2013 establishing measures for the application of the security principles relating to the processing of non-classified sensitive information.

² Commission Decision (EU, Euratom) 2019/1961 of 17 October 2019 on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information (OJ L 311, 2.12.2019, p. 1).

³ Commission Decision (EU, Euratom) 2019/1962 of 17 October 2019 on implementing rules for handling RESTREINT UE/EU RESTRICTED information (OJ L 311, 2.12.2019, p. 21).

⁴ Commission Decision (EU, Euratom) 2019/1963 of 17 October 2019 laying down implementing rules on industrial security with regard to classified procurement contracts (OJ L 311, 2.12.2019, p. 37).

⁵ Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission (OJ L 6, 11.1.2017, p. 40).

⁶ Commission Implementing Decision C(2018)6575, of 4.10.2018, on implementing rules for physical security measures aimed at protecting European Union Classified Information.

⁷ Commission Implementing Regulation (EU) 2021/581 of 9 April 2021 on the situational picture of the European Border Surveillance System (EUROSUR) (OJ L 124, 12.4.2021, p. 3).

⁸ OJ C 83, 30.2.2010, p. 389.

Article 3
Entry into Force

This Decision enters into force on the day following its adoption.

Done in written procedure, on 30 July 2022

For the Management Board

[signed]

Alexander Fritsch
Chairperson of the Management Board

Annexes:

Annex - Security Rules of the European Border and Coast Guard Agency (Frontex)

ANNEX

Security Rules of the European Border and Coast Guard Agency (Frontex)

CHAPTER 1 GENERAL PROVISIONS

Article 1 *Subject matter and scope*

1. This Decision lays down the basic principles and minimum standards of security within Frontex with a view to ensuring the protection of European Union classified information ('EUCI') and sensitive non-classified information including, inter alia, provisions for the exchange of such information with third countries, and processing and storage of such information.
2. The rules laid down in this Decision shall apply to all Frontex entities and in all Frontex premises.
3. Notwithstanding any specific rules concerning particular groups of staff, this Decision shall apply to all Frontex staff falling within the scope of the Staff Regulations of Officials of the European Union (the 'Staff Regulations') and of the Conditions of Employment of Other Servants of the European Union (the 'CEOS')⁹ to national experts seconded to Frontex¹⁰, to service providers and their staff, and to any individual with access to Frontex buildings or other assets, or to information handled by Frontex.

Article 2 Definitions

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

- a) 'Accreditation' means the formal authorisation and approval granted to a communication and information system by the competent Security Accreditation Authority to process EUCI in its operational environment, following the formal validation of the Security Plan and its correct implementation.
- b) 'Accreditation Process' means the necessary steps and tasks required prior to the accreditation by the competent Security Accreditation Authority. These steps and tasks shall be specified in a Security Notice on the security accreditation of communication and information systems handling EUCI at Frontex.
- c) 'Assets' means all movable and immovable property and possessions of Frontex.
- d) 'Authorisation for access to EUCI' means a Decision by the Frontex Security Authority taken on the basis of an assurance given by a competent authority of a Member State that a Frontex statutory staff member or seconded national expert may, provided his or her 'need-to-know' has been determined and he or she has been appropriately briefed on his or 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'.
- e) 'Classified contract' means a contract entered into by Frontex with a contractor for the supply, the execution of works or the provision of services, the performance of which

⁹ Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community. OJ L 56, 4.3.1968, p. 1, as last amended by Regulation (EU, Euratom) No 1023/2013 of the European Parliament and of the Council of 22 October 2013, OJ L 287, 29.10.2013, p. 15.

¹⁰ 'National experts seconded to Frontex' means those experts referred to in Management Board Decision 25/2012 of 28 November 2012 laying down rules on national experts with tasks and powers of the guest officers to Frontex, Management Board Decision 12/2017 of 30 March 2017 on secondment of national experts to Frontex, and those seconded to Frontex in accordance with Article 56 of the Regulation.

- requires or involves the creation, handling or storing of EUCI.
- f) 'Classified subcontract' means a contract entered into by a Frontex contractor or grant beneficiary for a classified contract with a contractor (i.e. subcontractor), whose performance requires or involves the creation, handling or storing of EUCI.
 - g) 'Classified grant agreement' means an agreement whereby Frontex awards a grant, the performance of which requires or involves the creation, handling or storing of EUCI.
 - h) 'Communication and Information System' or 'CIS' means any system enabling the handling of information in electronic form, including all assets required for its operation, as well as the infrastructure, organisation, personnel and information resources. This definition includes business applications, shared IT services, outsourced systems, and end-user devices.
 - i) 'Crisis situation' means a circumstance, event, incident or emergency (or a succession or combination thereof) posing a major or an immediate threat to security in Frontex regardless of its origin.
 - j) 'Cryptographic (Crypto) material' means cryptographic algorithms, cryptographic hardware and software modules, and products including implementation details and associated documentation and keying material.
 - k) 'Cybersecurity' means the preservation of confidentiality, integrity and availability of Communication and Information Systems (CIS) and the data sets that they process; the application of technologies, processes and controls to protect ICT systems, networks, computer programmes and end user computing devices. It aims to reduce the risk of cyber-attacks and to protect against unauthorised exploitation.
 - l) 'Data' means information in a form that allows it to be communicated, recorded, processed or destroyed.
 - m) 'Declassification' means the removal of any security classification.
 - n) 'Defence in depth' means the application of a range of security measures organised as multiple layers of defence.
 - o) 'Downgrading' means a reduction in the level of security classification.
 - p) 'Document' means any recorded information regardless of its physical form or characteristics.
 - q) 'European Union classified information' (EUCI) means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.
 - r) 'EUROSUR' means the framework for information exchange and cooperation between the Member States and the European Border and Coast Guard Agency referred to in Article 2(9) of the Regulation.
 - s) 'EUROSUR Security Accreditation Board' refers to the EUROSUR Security Accreditation Board established pursuant to Article 35(1) of the EUROSUR Implementing Regulation.
 - t) 'Facility Security Clearance' ('FSC') means an administrative determination by a National Security Authority ('NSA'), Designated Security Authority ('DSA') or any other competent security authority in accordance with national laws and regulations regarding security, that a facility can afford an adequate level of protection to EUCI to a specified security classification level (CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET).
 - u) 'Frontex entities' means all entities of the Agency as defined by the Management Board Decision 43/2020 adopting the Agency's amended organisational structure¹¹ and the Frontex Internal Structure and Rules of Procedure based on that Decision.
 - v) 'Frontex Security Officer' means a staff member with general responsibility for security in Frontex under the authority and responsibility of the Frontex Security Authority and appointed by the Management Board¹².
 - w) 'Handling' of EUCI means all possible actions to which EUCI may be subject throughout its life-cycle. It comprises its creation, recording or registration, processing, carriage, downgrading, declassification and destruction. In relation to Communication and

¹¹ Management Board Decision 43/2020 of 9 December 2020 adopting the Agency's amended organisational structure

¹² Article 100(2)(ad) of the Regulation.

- Information Systems, it also comprises its collection, display, transmission and storage.
- x) '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.
 - y) 'Implementing rules' means any set of rules or security notices adopted in accordance with Article 70.
 - z) 'Local Informatics Security Officer' ('LISO') means the officer who is responsible for IT security policy awareness, liaises with and advises the Digital Services Unit on IT security policies, maintains and develops information security management processes and information system security plans, and reports on ICT security.
 - aa) 'Material' means any medium, data carrier or item of machinery or equipment, either manufactured or in the process of manufacture.
 - bb) 'Originator' means the Union institution, agency or body, Member State, third country or international organisation under whose authority classified information has been created and/or introduced into the Union's structures.
 - cc) 'Personal data' means personal data as defined in Article 3(1) of Regulation (EU) 2018/1725¹³ of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC;
 - dd) 'Personnel security authorisation' is the application of measures to ensure that access to EUCI is granted only to individuals who have:
 - i) a need-to-know;
 - ii) been security authorised to the relevant level, where appropriate; and
 - iii) been briefed on their responsibilities.
 - ee) '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 or her 'need- to-know' has been determined and he or she has been appropriately briefed on his or her responsibilities, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date;
 - ff) 'Personnel Security Clearance Certificate' ('PSCC') means a certificate issued by a competent authority establishing that an individual holds a valid security clearance 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.
 - gg) 'Premises' means any immovable or assimilated property and possessions of Frontex.
 - hh) 'Prevention of risk' means security measures that can reasonably be expected to impede, delay or stop a risk to security.
 - ii) 'Registry Control Officer' ('RCO') means a dedicated staff member executing registry control tasks related to the management and protection of EUCI in the Frontex EU Classified Information Registry ('Frontex EUCI Registry').
 - jj) '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.
 - kk) '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 causes 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.
 - ll) 'Risk acceptance' is the decision to agree to the further existence of a residual risk after risk treatment.
 - mm) 'Risk assessment' consists of identifying threats and vulnerabilities and conducting the related risk analysis, i.e. the analysis of probability and impact.
 - nn) 'Risk communication' consists of developing awareness of risks among CIS user communities, informing approval authorities of such risks and reporting them to

¹³ OJ L 295, 21.11.2018, p 39.

- operating authorities.
- oo) 'Risk to security' means the combination of the threat level, the level of vulnerability and the possible impact of an event.
 - pp) 'Risk treatment' consists of mitigating, removing, reducing (through an appropriate combination of technical, physical, organisational or procedural measures), transferring or monitoring the risk.
 - qq) 'Security Authority' means the authority having the responsibilities assigned by this Decision and its implementing rules.
 - rr) 'Security Board' means a group advising the Frontex Security Authority, where appropriate, on matters relating to Frontex internal security policy and more particularly on protection of EUCI.
 - ss) 'Security in Frontex' means the security of persons, assets and information in Frontex, and in particular the physical integrity of persons and assets, the integrity, confidentiality and availability of information and communication and information systems, as well as the unobstructed functioning of Frontex operations.
 - tt) '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).
 - uu) 'Security measure' means any measure taken in accordance with this Decision for the purpose of controlling risks to security.
 - vv) '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.
 - ww) 'Sensitive non-classified information' is understood as all information or material restricted to a limited number of persons (on a need-to-know or need for access basis), whose disclosure to non- authorised persons would cause a moderate level of harm to Frontex, Union institutions and bodies, Member States or bodies and agencies that Frontex has entered into working relations with, but not to such a serious level as to merit EU security classification under Article 24. Frontex must protect this information or material because of its sensitivity.
 - xx) '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 No (EEC, Euratom, ECSC) No 259/68 of the Council¹⁴.
 - yy) '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.
 - zz) 'Threat to security' means an event or agent that can reasonably be expected to adversely affect security if not responded to and controlled. An 'Immediate threat to security' means a threat to security which occurs with no or with extremely short advance warning; and a 'Major threat to security' means a threat to security that can reasonably be expected to lead to loss of life, serious injury or harm, significant damage to property, compromise of highly sensitive information, disruption of IT systems or of essential operational capacities of Frontex.
 - aaa) '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.

¹⁴ See footnote 11.

Article 3

Principles for security measures applied within Frontex

1. In implementing this Decision, Frontex shall comply with the EU Treaties and in particular the Charter of Fundamental Rights¹⁵, Protocol No 7 to the Treaty on the Functioning of the European Union on the Privileges and Immunities of the European Union and any applicable rules of national law and with the terms of the present Decision. If necessary, a security notice providing guidance in this respect shall be adopted based on Article 70.
2. Security measures taken in accordance with this Decision shall be based on the principles of legality, transparency, proportionality and accountability.
3. Any security measure, including those on the protection and handling of EUCI and sensitive non-classified information, shall be taken overtly unless this can reasonably be expected to impair its effect. Addressees of a security measure shall be informed in advance of the reasons for and the impact of the measure, unless the effect of the measure can reasonably be expected to be impaired by providing such information. In this case, the addressee of the security measure shall be informed after the risk of impairing the effect of the security measure has ceased.
4. Frontex entities shall ensure that security issues are taken into account from the start of the development and implementation of Frontex policies, decisions, programmes, projects and activities for which they are responsible.
5. Frontex shall, where appropriate, seek cooperation with the competent authorities of the Member States hosting Frontex premises, of other Member States and of Union institutions, agencies or bodies, where feasible, taking account of the measures taken or planned by those authorities to address the risk to security concerned.
6. When taking security measures, Frontex shall in particular ensure so far as reasonably possible, that:
 - a) it shall only transmit personal data to external recipients in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council;
 - b) where an individual poses a threat to security, any security measure shall be directed against that individual, and that individual may be subjected to bearing the costs incurred. Those security measures may only be directed against other individuals if an immediate or major threat to security must be controlled and the following conditions are fulfilled:
 - i) the envisaged measures against the individual posing the threat to security cannot be taken or are not likely to be effective;
 - ii) Frontex cannot control the threat to security by its own actions or cannot do so in a timely manner;
 - iii) the measure does not constitute a disproportionate danger for the other individuals and their rights.

Article 4

Obligation to comply

1. This Decision, including, its implementing rules and the security notices as referred to in Article 70 and the instructions given by mandated staff as referred to in Article 9 shall be mandatory.
2. Non-compliance with this Decision may trigger disciplinary action in accordance with the Treaties and the Staff Regulations, contractual sanctions and/or legal actions under national laws and regulations.

¹⁵ OJ C 83, 30.3.2010, p. 389.

CHAPTER 3 **ORGANISATION**

Article 5 **Frontex Security Authority**

1. The Frontex Security Authority shall assume the following functions, within the meaning of Commission Decision (EU, Euratom) 2015/444¹⁶:
 - a) Information Assurance Authority ('IAA');
 - b) Crypto Distribution Authority ('CDA');
 - c) Security Accreditation Authority ('SAA').
2. The Frontex Security Authority shall have the responsibilities assigned to him or her by this Decision and its implementing rules.
3. The function of the Frontex Security Authority shall be exercised by the Executive Director of Frontex.

Such functions may be delegated to a staff member of Frontex in accordance with the Frontex Internal Structure and Rules of Procedure.

Article 6 **Frontex Security Board**

1. The Frontex Security Authority shall be assisted by the Frontex Security Board established pursuant to the Decision of the Executive Director of 31 October 2019¹⁷.
2. The Frontex Security Board shall provide support and guidance to the Frontex Security Authority to enhance holistic solutions in security matters, including the handling of EUCI and sensitive non-classified information.
3. The specific arrangements on roles and responsibilities of the members of the Frontex Security Board as regards cybersecurity shall be defined in the rules concerning the security of Communication and Information Systems ('CIS') in Frontex.

Article 7 **EUROSUR Security Accreditation Board**

Matters related to the security of data and to the security accreditation in EUROSUR shall be dealt with by the EUROSUR Security Accreditation Board in accordance with its role and responsibilities as laid down in Article 35 of Commission Implementing Regulation (EU) 2021/581.

Article 8 **Frontex Security Officer**

1. The Management Board shall appoint a Frontex Security Officer responsible for the operational day-to-day security within Frontex, who shall be the point of contact on security within Frontex, including for the protection of classified information and sensitive non-classified information¹⁸.
2. The Frontex Security Officer shall be a Temporary Agent.
3. The Frontex Security Officer shall be accountable to the Frontex Security Authority for fulfilling his or her tasks. In relation to his or her daily work, the Security Officer shall report to the Director of the Financial Digital and Security Division.
4. On matters dealt with in this Decision the Frontex Security Officer shall report directly to the

¹⁶ Articles 34 and 36(7) and 35(a) of Commission Decision (EU, Euratom) 2015/444 respectively.

¹⁷ Decision of the Executive Director No R-ED-2019-10 of 31/01/2019 establishing the Frontex Security Board.

¹⁸ Article 100, 2. (ad) of the Regulation.

Frontex Security Authority, while informing his or her direct hierarchy.

5. The Frontex Security Officer shall:

- a) be the contact point on security within the Agency;
- b) monitor the correct implementation of this Decision;
- c) monitor the alignment of this Decision with the European Commission's security rules;
- d) ensure security training and awareness activities addressing staff members, contractors and others working under the authority of Frontex;
- e) develop Operating Procedures ('SecOPs') within the meaning of Article 49(10) of this Decision;
- f) be responsible for Communication Security, including crypto distribution management;
- g) be responsible for handling and reporting breaches of security (any incident affecting security at Frontex, including suspected criminal offences) and compromise of sensitive non-classified information and EUCI;
- h) be responsible for key management, including holding spare keys and a written record of each combination setting;
- i) manage requests for personnel security clearances and act as the point of contact within Frontex in the context of vetting procedures;
- j) assist the Frontex Security Authority in the discharge of responsibility for EUCI, including preparation of accreditation of classified CIS, access rights management for classified CIS and supervision of the Frontex EUCI Registry;
- k) determine the appropriate combination of physical security measures for protecting EUCI and implement and develop minimum standards, norms and criteria to that effect;
- l) assume other tasks related to the protection of EUCI or defined by the implementing rules.

- 6. The Frontex Security Officer shall at regular intervals, report to the Frontex Security Authority and to his or her direct hierarchy on security issues involving any Frontex entities and, immediately, on any security incidents.
- 7. The Frontex Security Officer shall be a designated secretary to the EUROSUR Security Accreditation Board.
- 8. The Frontex Security Authority may assign to the Frontex Security Officer additional specific tasks in cases of major or immediate risks to security or of emergencies.
- 9. The responsibilities of the Local Informatics Security Officer or any other function implying security or safety-related responsibilities shall be without prejudice to the role and responsibilities assigned to the Frontex Security Officer.
- 10. The Frontex Security Officer shall liaise with the Local Informatics Security Officer, in particular for matters related to the security of classified CIS, or with any other function implying security or safety-related responsibilities in order to ensure a coherent and consistent approach to security and an efficient flow of information on matters related to security at Frontex. The role and responsibilities of the Local Informatics Security Officer of Frontex shall be laid down in the applicable rules concerning the security of classified CIS in Frontex.
- 11. The Frontex Security Officer may request a contractor to carry out, under his or her direction and supervision, tasks relating to security, within the terms of the contract.

CHAPTER 4 DELIVERING SECURITY

Article 9 Mandated staff

- 1. Only staff authorised by a mandate conferred upon them by the Frontex Security Authority, given on the basis of their current duties, post or function, may be entrusted with the power to take one or several of the following measures:

- a) conduct security inquiries as referred to in Article 16;
 - b) take security measures as referred to in Article 15, and as specified in the mandate.
- 2. The mandates referred to in paragraph 1 shall be conferred for a duration which shall not exceed the period during which the persons concerned hold the post or function in respect of which the mandate has been conferred. Those mandates shall be conferred in compliance with the applicable provisions set out in Article 3(1).
- 3. As regards mandated staff, this Decision constitutes a service instruction within the meaning of Article 21 of the Staff Regulations.

Article 10 **Security measures regarding persons**

- 1. An appropriate level of protection shall be afforded to persons in the premises of Frontex, taking into account security and safety requirements.
- 2. In case of major risks to security, the Frontex Security Officer and the Frontex Security Board shall provide appropriate security measures for Frontex staff and other staff where a threat assessment has indicated that such protection is needed to ensure their safety and security.
- 3. In case of major risks to security, Frontex may order the evacuation or lockdown (invacuation) of its premises.
- 4. Victims of accidents or attacks within Frontex premises shall receive assistance.
- 5. In order to prevent and control risks to security, staff duly mandated for the specific task may carry out background checks of persons falling under the scope of this Decision, so as to determine whether giving such persons access to Frontex premises or information presents a threat to security. For that purpose, and in compliance with Regulation (EU) 2018/1725 and the provisions referred to under Article 3 of this Decision, the mandated staff concerned may:
 - a) use any source of information available to Frontex, taking into account the reliability of the source of information;
 - b) access the personnel file or data Frontex holds with regard to individuals it employs or intends to employ, or for contractors' staff when duly justified.

Article 11 **Security measures regarding physical security and assets**

- 1. Security of assets shall be ensured by applying appropriate physical and technical protective measures and corresponding procedures, hereinafter called 'physical security', creating a multi-layered system.
- 2. Measures may be adopted pursuant to this Article in order to protect persons or information in Frontex as well as to protect assets.
- 3. Physical security shall have the following objectives:
 - a) preventing acts of violence directed against persons falling within the scope of this Decision;
 - b) preventing espionage and eavesdropping on sensitive or classified information;
 - c) preventing theft, acts of vandalism, sabotage and other violent actions aimed at damaging or destroying Frontex buildings and assets;
 - d) enabling investigation and inquiry into security incidents including through checks on access and exit control log files, CCTV coverage, telephone call recordings and similar data as referred to in Article 15 and 16 and other information sources.
- 4. Physical security shall include:
 - a) an access policy applicable to any person or vehicle requiring access to Frontex premises, including the parking lots;

- b) an access control system comprising guards, technical equipment and measures, information systems or a combination of all of those elements;
5. In order to ensure physical security, the following actions may be taken:
- a) recording entry to and exit from Frontex premises of persons, vehicles, goods and equipment;
 - b) identity controls at its premises;
 - c) inspection of vehicles, goods and equipment by visual or technical means;
 - d) preventing unauthorised persons, vehicles and goods, from entering Frontex premises.

Article 12

Security measures regarding information

1. Security of information covers all information handled by Frontex.
2. Security of information, regardless of its form, shall balance transparency, proportionality, accountability and efficiency with the need to protect information from unauthorised access, use, disclosure, modification or destruction
3. Security of information shall be aimed at protecting confidentiality, integrity and availability.
4. Risk management processes shall therefore be used to categorise information assets and to develop proportionate security measures, procedures and standards, including mitigating measures.
5. These general principles underlying security of information shall be applied in particular as regards:
 - a) 'European Union classified information' as defined in Article 2(q);
 - b) 'Sensitive non-classified information' as defined in Article 2(ww).
6. Any individual who is responsible for compromising or losing EUCI or sensitive non-classified information, which is identified as such in the rules regarding its handling and storage, may be liable to disciplinary action in accordance with the Staff Regulations. That disciplinary action shall be without prejudice to any further legal or criminal proceedings by the competent national authorities of the Member States in accordance with their laws and regulations and to contractual remedies.

Article 13

Security measures regarding Communication and Information Systems

1. All Communication and Information Systems ('CIS') used by Frontex shall comply with the Frontex Information Systems Security Policy, as set out in the applicable rules concerning the security of communication and information systems in Frontex, its implementing rules and corresponding security standards in accordance with Article 15(2) of the Regulation.
2. Frontex entities which own, manage or operate CIS shall allow access to these systems only to those Union institutions, agencies and bodies or other organisations and authorities, which can provide reasonable assurance that their IT systems are protected at a level equivalent to the Commission's Information Systems Security Policy as set out in Commission Decision 2017/46, its implementing rules and corresponding security standards. Frontex shall monitor such compliance, and in case of serious non-compliance or continued failure to comply, be entitled to prohibit access.

Article 14

Forensic analysis regarding cybersecurity

The Frontex Security Officer shall in particular be responsible for advising forensic technical analysis in cooperation with the Digital Services Unit at Frontex in support of the security inquiries referred to in Article 16, related to counterintelligence, data leakage, cyberattacks and information systems security.

Article 15

Security measures regarding persons, objects and CIS in case of immediate risk or a crisis situation

1. In order to ensure security in Frontex and to prevent and control risks, staff mandated in accordance with Article 9 may, in compliance with the principles set out in Article 3, take inter alia one or more of the following security measures:
 - a) securing of scenes and evidence, including access and exit control log files, CCTV images, in case of incidents or conduct that may lead to administrative, disciplinary, civil or criminal procedures;
 - b) limited measures concerning persons posing a threat to security, including ordering persons to leave Frontex premises, escorting persons from Frontex premises, banning persons from the Frontex premises for a period of time, the latter defined in accordance with criteria to be defined in implementing rules;
 - c) limited measures concerning objects posing a threat to security including the removal, seizure and disposal of objects;
 - d) searching of Frontex premises, including of offices, within such premises;
 - e) searching of CIS and equipment, telephone and telecommunications traffic data, log files, user accounts, etc.;
 - f) other specific security measures with similar effect in order to prevent or control risks to security, in particular in the context of Frontex rights as a tenant or as an employer in accordance with the applicable national laws;
 - g) interviewing those who could provide useful information with regard to the security inquiries in accordance with Article 16.
2. Under exceptional circumstances, security staff mandated in accordance with Article 9 may take any urgent measures needed, in strict compliance with the principles laid down in Article 3. As soon as possible after having taken those measures, they shall request the Frontex Security Authority to confirm the measures taken and authorise further necessary actions and shall liaise, where appropriate with the competent national authorities.
3. Security measures pursuant to this Article shall be documented at the time they are taken or, in the event of an immediate risk or a crisis situation, as soon as reasonably possible after they have been taken. In the latter case, the documentation must also include the elements on which the assessment regarding the existence of an immediate risk or a crisis situation was based. The documentation can be concise, but should be constituted in such a way as to allow the person subjected to the measure to exercise his or her rights of defence and of protection of personal data in accordance with Regulation (EU) 2018/1725 and to allow scrutiny as to the legality of the measure. No information about specific security measures addressed to a member of staff shall be part of the person's personnel file.
4. When taking security measures pursuant to point (a) and (b) of paragraph 1 of this article, Frontex shall in addition guarantee that the individual concerned is given the opportunity to contact a lawyer or a person of his or her confidence.
5. In line with Regulation 2018/1725 and the applicable rules on the protection of natural persons in relation to the processing of personal data in Frontex, individuals concerned by security measures pursuant to point (a) and (b) of paragraph 1 of this article shall be able to exercise their right to have recourse to the European Data Protection Supervisor.

Article 16

Inquiries

1. Security inquiries may be conducted:
 - a) in case of an incident that might be affecting security at Frontex, including suspected criminal offences;
 - b) in case of potential leakage, mishandling or compromise of sensitive non-classified

- information, or EUCI;
- c) in the context of counter-intelligence and counter-terrorism;
 - d) in case of cyber-incidents classified as serious.
2. Without prejudice to paragraph 1, Article 86 and Annex IX of the Staff Regulations, applicable to temporary and contract staff pursuant to Articles 50a and 119 CEOS, apply and security enquiries may be conducted in parallel with other inquiries.
 3. The decision to conduct a security inquiry shall be taken by the Frontex Security Authority who will also be the recipient of the inquiry report.
 4. Security inquiries shall be conducted only by dedicated members of staff of the Security Sector acting duly mandated in accordance with Article 9 under the responsibility of the Frontex Security Officer and supervision of his or her hierarchical superiors. Where the security inquiries relate to a member of the Security Sector, the Frontex Security Officer will be directly mandated by the Frontex Security Authority to perform the inquiries. Where the security inquiries relate to the Frontex Security Officer, independent competent security staff from outside Frontex will be mandated by the Frontex Security Authority to perform the inquiries under the supervision of the Frontex Security Authority.
 5. In accordance with their mandate, mandated staff shall exercise their powers of security inquiry independently and shall have the powers provided for in Article 15 and 16.
 6. Mandated staff having the competence to conduct security inquiries may gather information from all available sources related to any administrative or criminal offences committed within Frontex premises or involving persons referred to in Article 1(3) either as the victim or the perpetrator of such offences. Mandated staff shall inform and cooperate with the Frontex Data Protection Officer whenever an inquiry involves accessing personal data of an individual, in order to ensure fair and proportionate treatment of the data necessary for conducting the investigation.
 7. The Frontex Security Officer shall inform the competent authorities of the host Member State or any other Member State concerned, where appropriate, and in particular if the inquiry has given rise to indications of criminal acts having been perpetrated. In this context, the Frontex Security Officer may, where appropriate or required, provide support to these aforementioned authorities. Before informing the authorities, the Frontex Security Officer shall report on the facts to the Frontex Security Authority.
 8. In the case of cyber-incidents classified as serious, the Frontex Digital Services Unit shall collaborate closely with the Frontex Security Officer to provide support on all technical matters. In line with relevant regulations and national legislation, the Frontex Security Authority shall decide, in consultation with the Head of the Digital Services Unit, when it is appropriate to inform the competent authorities of the host country, or any other Member State concerned. The incident coordination services of the Computer Emergency Response Team for the Union institutions, bodies and agencies ('CERT-EU') will be used as regards support to Union institutions and other agencies that may be affected.
 9. Security inquiries shall be documented in accordance with the relevant implementing rules.
 10. As soon as security inquiries, as referred to in the first paragraph of this article, reveal information which falls within the competence of the Frontex Inspection and Control Office (ICO), the Frontex Security Officer shall inform the ICO at once in order, in particular, not to compromise later steps taken within the frame of administrative inquiries.

Article 17 **Cooperation with OLAF**

1. Where dedicated members of staff of the Security Sector under the responsibility of the Frontex Security Officer conduct security inquiries, as referred to in Article 16, and if aspects of these enquiries fall within the competences of the European Anti-Fraud Office ('OLAF'), the dedicated members of staff shall liaise with OLAF at once in order, in particular, not to compromise later

steps by OLAF. Where appropriate, the Frontex Security Authority shall invite OLAF to be involved in the investigation.

2. The security inquiries, as referred to in Article 16, shall be without prejudice to the powers of OLAF as laid down in the rules governing this body. The members of the Security Sector or the members of ICT Security may be requested to provide technical assistance for inquiries initiated by OLAF.
3. The Frontex Security Officer may be asked to assist staff members of OLAF when they access Frontex premises in accordance with Articles 3(5) and 4(4) of Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council¹⁹, in order to facilitate their tasks.
4. Where a case may fall within the competence of both the Frontex Security Officer and OLAF, the Frontex Security Officer shall report to the hierarchical superiors and the Frontex Security Authority that shall inform the Director-General of OLAF at the earliest possible stage.

Article 18

Alert states and management of crisis situations

1. The Frontex Security Authority shall be responsible for putting in place appropriate alert state measures in anticipation of or in response to threats and incidents affecting security at Frontex, and for measures required for managing the security related aspects of crisis situations.
2. The alert state measures referred to in paragraph 1 shall be commensurate with the level of threat to security. The alert state levels shall be defined in close cooperation with the competent services of Union institutions, agencies and bodies, and of the hosting Member State hosting Frontex premises.
3. The Frontex Security Officer shall advise the Frontex Security Authority on alert states and organisation of security related aspects of crisis situations and implementation of the Frontex Security Authority decisions.

CHAPTER 5

MANAGEMENT OF SENSITIVE NON-CLASSIFIED INFORMATION

Article 19

Sensitive non-classified information and Article 339 TFEU

Sensitive non-classified information as defined in Article 2 (49) includes, but is not limited to, information or material covered by the obligation of professional secrecy, as referred to in Article 339 TFEU, information covered by the interests protected in Article 4 of Regulation (EC) No 1049/2001²⁰ of the European Parliament and of the Council read in conjunction with the relevant case-law of the Court of Justice of the European Union or personal data within the scope of Regulation (EU) 2018/1725.

Article 20

Protection, handling and storage of sensitive non-classified information

1. Sensitive non-classified information must be protected by appropriate security measures.
2. The handling, storage and protection of sensitive non-classified information shall be laid down in a security notice adopted on the basis of Article 70 of this Decision.
3. Sensitive non-classified information shall only be released to those individuals who have a 'need-

¹⁹ Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.9.2013, p 1).

²⁰ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

to-know'. When deemed necessary for the effective protection of its confidentiality, it shall be identified by a security marking and corresponding handling instructions. When handled or stored on CIS, such information shall be protected in compliance with applicable rules on the security of CIS in Frontex, its implementing rules and corresponding standards.

4. If it is necessary for Frontex to exchange sensitive non-classified information with certain authorities of a third country, of an international organisation, with an EU Executive agency, or with an EU decentralised agency, an arrangement shall be drawn up between Frontex and the relevant authorities of the third country, international organisation, EU Executive agency or EU decentralised agency in accordance with Articles 73(4) and 68(2) of the Regulation, respectively. The arrangement shall set out the handling instructions for all such information exchanged between the parties. The Commission shall give its prior approval to the conclusion of any such arrangements and the European Parliament shall be provided with detailed information on the parties and the content of the arrangement. Each party shall remain responsible for the compliance of its own staff handling the information exchanged.

CHAPTER 6

MANAGEMENT OF EU CLASSIFIED INFORMATION

Article 21

Classification management

1. The originator shall ensure that EUCI created is appropriately classified, clearly identified as EUCI and retains its classification level for only as long as necessary.
2. Without prejudice to Article 37(4), EUCI shall not be downgraded or declassified nor shall the security classification marking referred to in Article 25 be modified or removed without the prior written consent of the originator.

Article 22

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 entities' business continuity plans.

Article 23

Breaches of security and compromise of EUCI

1. A breach of security occurs as the result of an act or omission by an individual which is contrary to the security rules laid down in this Decision and its implementing rules.
2. Compromise of EUCI occurs when, as a result of a breach of security, it has been disclosed wholly or in part to unauthorised persons.
3. Any breach or suspected breach of security shall be reported immediately to the Frontex Security Authority via the Frontex Security Officer while keeping informed his hierarchical superiors.
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 16.
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 Frontex, of the Union or of the Member States or party which may be involved on the basis of a signed arrangement;
 - d) take appropriate measures to prevent a recurrence; and 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, regulations and arrangements.

Article 24 **Basic principles**

1. All EUCI documents shall be managed in compliance with the applicable rules on document management in Frontex and consequently should be registered, filed, preserved and finally eliminated, sampled or transferred in accordance with the common Frontex retention list.
2. Frontex entities and premises where EUCI is handled or stored shall be subject to regular inspection by the Frontex Security Officer.
3. Information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be registered for security purposes prior to distribution and on receipt.
4. The Frontex Classified Information Registry shall act as the central point for receiving and dispatching EUCI. It shall act as the main point of entry and exit for all information classified RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET, which are exchanged between Frontex and Member States, or Union institutions, agencies and bodies, international organisations and Schengen Associated Countries²¹, according to the relevant specific arrangements.
5. When EUCI is handled or stored using a CIS, registration procedures may be performed by processes within the CIS itself.
6. More detailed provisions concerning the registration of EUCI for security purposes shall be laid down in implementing rules.

Article 25 **EUCI Classification levels**

1. EUCI at Frontex shall be classified at one of the following levels:
 - a) 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;
 - b) 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;
 - c) 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. 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

²¹ 'Schengen Associated Countries' means Iceland, Liechtenstein, Norway and Switzerland, which are non-EU countries participating in Schengen that have signed an Association Agreement in order to be associated with the implementation, application and development of the Schengen acquis.

of activity to which it relates, identify the originator, limit distribution, restrict use or indicate releasability.

Article 26
Maximum level of EUCI

The level of EUCI that Frontex may handle is up to the level of SECRET UE/EU SECRET. Frontex shall not handle EUCI at the level TRES SECRET UE/EU TOP SECRET.

Article 27
Classification principles

1. Information shall be classified where it requires protection with regard to its confidentiality in accordance with Article 25(1).
2. The originator of EUCI shall be responsible for classifying a document in accordance with the relevant implementing rules, standards and guidelines regarding classification, and for the initial dissemination of the information. The Frontex Security Authority may decide to attribute a standard classification level to certain types of information that Frontex creates on a regular basis, based on its nature, category and parameters as prescribed in the implementing rules.
3. The Decision to classify shall be taken in accordance with Article 25(1) and 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. The EUCI marking shall be in accordance with provisions of Article 28(2).
5. Individual parts of a given document (i.e. pages, paragraphs, sections, annexes, appendices, attachments and enclosures) may or may not require classification and shall be marked accordingly, including when stored in electronic form.
6. The complete document or file shall be classified if it contains any classified components.
7. The overall classification level of a document or file shall be at least as high as that of its most highly classified component. When information from various sources is collated, the final product shall be reviewed to determine its overall security classification level, since it may warrant a higher classification than its component parts.
8. To the extent possible, documents containing parts with different classification levels shall be structured so that parts with a different classification level may be easily identified and detached if necessary.
9. The classification of a letter or note covering enclosures shall be as high as the highest classification of its enclosures.

Article 28
Markings

1. In addition to the security classification marking set out in Article 25(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.

2. The EUCI marking shall be in upper case, with no spaces either side of the forward slash, in French and English (French first) and shall never be translated.
3. The originator shall indicate clearly at which level the letter or note covering 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 29
Abbreviated classification marking

1. A standardised abbreviated classification marking may be used to indicate the classification level of individual paragraphs of a text. The abbreviation may be used where the full classification marking cannot be inserted, for example on a small portable device. The abbreviation shall not replace the full classification marking at the top and bottom of the page.
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:

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

Article 30
Creation of EUCI

1. When creating an EU classified document:
 - a) each page shall be marked clearly with the classification level;
 - b) each page shall be numbered;
 - c) the document shall bear a registration number and a subject, which itself shall not be classified information, unless it is marked as such;
 - d) the document shall have the date of its creation on it;
 - e) documents classified SECRET UE/EU SECRET shall bear a copy number on every page, if they are to be distributed in several copies.
2. An aggregate of EUCI may warrant a level of protection corresponding to a higher classification than that of its individual components.
3. Where it is not possible to apply paragraph 1 to EUCI, other appropriate measures shall be taken in accordance with implementing rules.

Article 31
EU Classified Information Registry in Frontex

1. Within Frontex, a registry shall be designated by the Frontex Security Authority to act as the central receiving and dispatching authority for EUCI. This registry shall be the Central Frontex EUCI Registry. It shall act as the main point of entry and exit for all information classified RESTREINT UE/EU RESTRICTED and up to including SECRET UE/EU SECRET exchanged between Frontex and, when provided for in specific arrangements according to the provisions of CHAPTER 10, third countries and international organisations, and for other Union institutions, agencies and bodies.
2. Frontex EUCI registry shall be established as a Secured Area as defined in Article 49.

Article 32
Registry Control Officer

1. The EUCI registry shall be managed by the Registry Control Officer ('RCO') and Deputy Registry Control Officers ('DRCOs').
2. The RCO and DRCOs shall be appointed by the Frontex Security Authority.
3. The RCO and DRCOs shall be appropriately security-cleared.
4. The function of Registry Control Officer shall be exercised by designated and duly trained personnel. The RCO and DRCOs shall be subject to the supervision of the Frontex Security Officer, 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.
5. The Frontex EUCI Registry shall be subject to audit by the Frontex Security Officer via random checks concerning the application of the provisions regarding the handling of EUCI and compliance with the relevant security rules, standards and guidelines.
6. Within his or her responsibility for managing the EUCI Registry, 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 or transfer to the historical archives service 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 33
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 the Frontex EUCI Registry when it is received in or dispatched from an organisational entity.
3. When EUCI is handled or stored using a 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 34
Copying and translating EU classified documents

1. Information classified up to SECRET UE/EU SECRET may be copied or translated on instruction from the holder, provided the originator has not imposed any caveats.
2. The security measures applicable to the original document shall apply to copies and translations thereof. Extracts shall be classified at the same level as the original full document, unless the originator has explicitly specified otherwise.

Article 35
Carriage of EUCI

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

2. Carriage of EUCI shall be subject to 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:
 - i) within a Frontex building;
 - ii) within the Union;
 - iii) from within the Union to the territory of a third country; and
 - c) be adapted to the nature and form of the EUCI.
3. The implementing rules or, in case of projects and programmes referred to in Article 63 as an integral part of the relevant Programme or Project Security Instructions ('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 and use of security personnel.
4. EUCI shall be conveyed between entities and premises outside physically protected areas as follows:
 - a) as a general rule, EUCI shall be transmitted electronically by duly accredited means and/or protected by cryptographic products approved in accordance with CHAPTER 9;
 - b) when the means referred to in point (a) of this paragraph are not used, EUCI shall be exceptionally carried either:
 - i) on removable storage media (e.g. USB sticks, CDs, hard drives) protected by cryptographic products approved in accordance with CHAPTER 9 and marked with the appropriate classification marking; or
 - ii) as prescribed in implementing rules.

Article 36 **Classified Meetings**

1. Management of EUCI at any classification level during a meeting shall be detailed in the implementing rules on classified meetings. These rules shall include provisions commensurate with the level of EUCI, regarding:
 - a) procedures on preparing classified meetings, handling EUCI during classified meetings and actions required after classified meetings;
 - b) electronic equipment authorised for classified meetings;
 - c) access to meetings by participants, interpreters and translators.
2. In accordance with the provisions of this Decision, individuals assigned to participate in meetings organised by Frontex 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 Frontex Security Officer has not received confirmation of the required security clearance, or to participants from Frontex who are not in possession of a security authorisation.
3. For meetings at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed, the Frontex meeting organiser shall inform the Frontex Security Officer well in advance of the dates, times, venue and participants of such meetings. For meetings at which information is classified RESTREINT UE/EU RESTRICTED, the Frontex meeting organiser may consult the Frontex Security Officer for advice.

Article 37 **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 entity at Frontex 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 Frontex 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 declassified and the information has been marked accordingly.
3. When review of the document results in a decision to declassify, consideration shall be given as to whether the document should be made public or bear a sensitive non-classified information distribution marking within the meaning of Chapter V of this Decision.
4. Information classified RESTREINT UE/EU RESTRICTED having originated in Frontex will be considered to be automatically declassified after thirty years, in accordance with Regulation (EEC, Euratom) No 354/83 as amended by Council Regulations (EC, Euratom) No 1700/2003 and 496/2015²².

Article 38

Indication of downgrading or declassification of a document

1. The original classification marking at the top and bottom of every page shall be visibly crossed out (not removed) either using the "strikethrough" functionality for electronic formats, or manually for print-outs.
2. The first (cover) page shall be stamped as downgraded or declassified and completed with the reference of the authority responsible for downgrading or declassifying and the corresponding date.
3. The original recipients of the EUCI shall receive a copy of declassified documents for information, and shall be informed of any downgraded documents. These initial recipients shall be responsible for informing any subsequent addressees to whom they have sent or copied the original EUCI.
4. All translations of classified information shall be subject to the same declassification procedures as the original language version.

Article 39

Partial declassification of EUCI

1. Partial declassification ("sanitising") shall also be possible (e.g. annexes, a few paragraphs). The procedure shall be identical to that of full declassification.
2. Upon sanitising EUCI, a declassified extract shall be produced.
3. The omitted text representing the non-declassified parts shall be replaced by:

PART NOT TO BE DECLASSIFIED

either in the body of the text itself (if the non-declassified part is a part of a paragraph), or as a paragraph (if the non-declassified part is a specific paragraph or more than one paragraph).

4. Specific mention shall be made in the text if a complete annex cannot be declassified and has hence been withheld from the extract.

²² 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).

Article 40
Destruction of EUCI

1. EU classified documents which are no longer required shall be destroyed by the Frontex EUCI Registry, taking account of the applicable rules on document management and archiving in Frontex.
2. EU classified documents, including those classified as 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.
3. EUCI of the level of CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be destroyed by the Frontex RCO on instruction from the holder or from a competent authority. The Frontex EUCI Registry shall update the logbooks and other registration information accordingly.
4. For documents classified as SECRET UE/EU SECRET such destruction shall be performed by the Frontex RCO in the presence of a witness who shall be cleared to at least SECRET UE/EU SECRET level.
5. 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 Frontex EUCI Registry shall keep destruction certificates of documents classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET for a period of at least five years.
6. Removable computer storage media used for EUCI shall be destroyed in accordance with procedures to be laid down in implementing rules.

Article 41
Destruction of EUCI in emergencies

1. The Frontex Security Officer shall prepare plans for all Frontex entities holding EUCI based on local conditions for the safeguarding of EU classified material in a crisis including if necessary emergency destruction and evacuation plans. The Frontex Security Officer 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 material in a crisis shall under no circumstances adversely affect the safeguarding or destruction of SECRET UE/EU SECRET material, including the enciphering equipment, the treatment of which 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 in emergencies shall be laid down in implementing rules.

CHAPTER 7
PERSONNEL SECURITY

Article 42
Basic Principles

1. An individual shall only be granted access to EUCI after:
 - a) his or her need-to-know has been determined;
 - b) he or she has been briefed on the security rules for protecting EUCI and the relevant security standards and guidelines, and has acknowledged his or her responsibilities with regard to protecting such information;
 - c) for information classified CONFIDENTIEL UE/EU CONFIDENTIAL and above, he or 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 vetting 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 vetting procedures shall be conducted to determine whether an individual, taking into account his or 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. Security investigations shall be requested from the national security authorities ('NSAs') or other competent national authorities in the context of security clearance request procedures. Frontex may accordingly seek a Service Level Agreement with the Commission to act as a liaison point with NSAs for clearances.

Article 43 **Security authorisation procedure**

1. The Frontex Security Authority shall identify the positions within Frontex 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 security vetting procedure should be initiated by the Security Officer. The individual shall consent in writing to being submitted to the security vetting procedure and shall complete and return the relevant NSA's vetting questionnaire to Security Officer without delay.
3. The Security Officer will transfer the completed security vetting questionnaire to the competent authority and request 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 Officer, he or she shall ensure that the relevant NSA is notified thereof.
5. Following completion of the security investigation, and as soon as possible after having been notified of the overall assessment of the findings of the security investigation, the Frontex Security Authority:
 - a) may grant an authorisation for access to EUCI to the individual concerned and authorise access to EUCI up to the relevant level until a date specified by him or her 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 Frontex Security Authority who in turn via the Security Officer 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 security investigation and 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 Frontex shall be subject to appeals in accordance with the Staff Regulations.

7. Frontex shall accept the authorisation for access to EUCI of equivalent level granted by any Union institution, body or agency provided it remains valid. Authorisations shall cover any assignment by the individual concerned within Frontex. The relevant NSA shall be notified of the change of employer.
8. If an individual's period of service does not commence within 12 months of the notification of the outcome of the security investigation, or if there is a break of 12 months in an individual's service, during which time he or she has not been employed by Frontex or by a Union Institution, body or agency, or in a position with a national administration of a Member State, the Security Officer shall refer the matter to the relevant NSA for confirmation that the security clearance remains valid and appropriate for access to EUCI.
9. Where information becomes known to the Security Officer concerning a security risk posed by an individual who holds a valid security authorisation, the Security Officer, acting in accordance with the relevant rules and regulations, shall ensure that the competent NSA is notified thereof.
10. Where an NSA notifies the withdrawal of an assurance given in accordance with paragraph 5(a) for an individual who holds a valid authorisation for access to EUCI, Frontex 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 individual shall be excluded from access to EUCI and from positions where such access is possible or where he or she might endanger security; where this is not possible the employment contract shall be terminated.
11. Any decision to withdraw or suspend an 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 Frontex Security Authority. 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 Frontex Security Authority shall be subject to appeals in accordance with the Staff Regulations.
12. Frontex shall make sure that national experts seconded to it 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 Frontex Security Authority, that, on the basis thereof, will grant a security authorisation for access to EUCI up to the level equivalent to the one referred to in the national security clearance, with a maximum validity for the duration of their assignment.
13. Records of security clearances and authorisations granted for access to EUCI shall be maintained by the Security Officer. 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.
14. After the initial granting of security authorisations and provided that the individual has had uninterrupted service with Frontex, a Union Institution, body or 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, every five years from the date of notification of the outcome of the last security investigation on which it was based.
15. The Frontex Security Authority may grant access to EUCI for a period of up to 12 months after the validity of the existing security authorisation expires, if no adverse information has been received from the relevant NSA or other competent national authority within a period of two months from the date of transmission of the request for renewal and the corresponding security clearance questionnaire. If, at the end of this 12-months period, the relevant NSA has not communicated its opinion, the individual shall be assigned to duties which do not require a security authorisation or employment contract shall be terminated as and when such clause is contractually foreseen.

Article 44
Security briefings

1. After having participated in the mandatory security briefing organised by the Frontex Security Officer, all individuals shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the Frontex Security Officer.
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 Officer 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 accordance with Article 17(2) of the Staff Regulations, applicable to temporary and contract staff pursuant to Articles 11 and 81 CEOS, in respect of the continued protection of EUCI.

Article 45
Temporary security authorisations

1. In exceptional circumstances, where duly justified in the interests of the service and pending completion of a full security investigation, the Frontex Security Authority may, after the competent NSA has been consulted, 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.
2. After having been briefed in accordance with Article 44, 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 written acknowledgements shall be kept by the Security Officer.

Article 46
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, and shall be briefed on security procedures for protecting EUCI and be instructed on their duties for protecting such information entrusted to them.

CHAPTER 8
PHYSICAL SECURITY AIMED AT PROTECTING CLASSIFIED INFORMATION

Article 47
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 designed based on a risk management process, in accordance with this Decision and its implementing rules.

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 clearance authorisation;
- c) deterring, impeding and detecting unauthorised actions; and

- d) denying or delaying surreptitious or forced entry by intruders.
- 2. Physical security measures shall be put in place for all Frontex premises, buildings, offices, rooms and other areas in which EUCI is handled or stored, including areas housing CIS as referred to in CHAPTER 9.
- 3. 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 Frontex Security Accreditation Authority.
- 4. Only equipment or devices approved by the relevant Security Authority shall be used for protecting EUCI at the level CONFIDENTIEL UE/EU CONFIDENTIAL or above.

Article 48

Physical security requirements and measures

- 1. Physical security measures shall be selected on the basis of a threat assessment made by the Frontex Security Officer, approved by Frontex Security Authority, where appropriate in consultation with Frontex entities, Union institutions, agencies or bodies and/or competent authorities in the Member States. Frontex shall apply a risk management process for protecting EUCI in 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 Frontex 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 Officer, applying the concept of defence in depth, shall determine the appropriate combination of physical security measures to be implemented. These physical security measures shall be based on Commission Implementing Decision C(2018)6575, of 4.10.2018, on implementing rules for physical security measures aimed at protecting European Union Classified Information.
- 3. The Security Officer and staff of the Security Sector are authorised to conduct entry and exit searches to act as a deterrent to the unauthorised introduction of material or the unauthorised removal of EUCI from premises or buildings.
- 4. When EUCI is at risk of being accessed without authorisation, even accidentally, the Frontex entities concerned shall take the appropriate measures as defined by the Frontex Security Officer to counter this risk.
- 5. For new facilities, physical security requirements and their functional specifications shall be defined in consent with the Frontex Security Authority, 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 the implementing rules.

Article 49

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 Frontex Security Accreditation Authority shall establish that an area meets the requirements

of 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 Officer and in compliance with the relevant internal Frontex access policy;
- 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 a 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. For Secured Areas which are protected against eavesdropping and designated as 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, keys shall be managed in accordance with Article 51;
- b) all persons and material entering such areas shall be controlled;
- c) such areas shall be regularly physically and/or technically inspected by the Security Officer. 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. Notwithstanding point (d) of paragraph 6, before being used in areas where meetings are held or work is being performed involving information classified SECRET UE/EU SECRET, and where the threat to EUCI is assessed as high, any communications devices and electrical or electronic equipment shall first be examined by the Frontex Security Officer to ensure that no intelligible information can be inadvertently or illicitly transmitted by such equipment beyond the perimeter of the Secured Area.

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

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

10. The Security Officer shall develop Security Operating Procedures ('SecOPs') for each Secured Area 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 Officer and afford protection equivalent to a security container approved for the storage of EUCI of the same classification level.

Article 50

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 35 and has undertaken to comply with compensatory measures, set out in implementing rules, 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 the provisions as prescribed by the implementing rules.
3. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL or as SECRET UE/EU SECRET may be handled:
 - a) in a Secured Area;
 - b) in an Administrative Area, provided the EUCI is protected from access by unauthorised individuals; or
 - c) outside a Secured Area or an Administrative Area provided the holder has undertaken to comply with the provisions as prescribed by the implementing rules.
4. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be stored in a Secured Area in a security container or a strong room.

Article 51

Management of keys and any combinations used for protecting EUCI

1. Procedures for managing keys and any combination settings for offices, rooms, strong rooms and security containers shall be laid down in implementing rules adopted in accordance to Article 70. 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 9
PROTECTION OF EU CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS

Article 52
Basic principles of Information Assurance

1. Information Assurance in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.
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 that an action or event has taken place, so that this event or action cannot subsequently be denied.
3. Information Assurance shall be based on a risk management process.

Article 53
CIS handling EUCI

1. CIS shall handle EUCI in accordance with the concept of Information Assurance.
2. For CIS handling EUCI, compliance with Frontex Information Systems Security Policy, as referred to in the applicable rules concerning the security of CIS in Frontex, 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 the 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 Security Accreditation Authority, as detailed in Frontex Classified Communication and Information Systems Security Accreditation Policy, 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 is provided by cryptographic products, such products shall be approved as follows:
 - a) preference shall be given to products which have been approved by the Council or by the Secretary-General of the Council in its function as crypto approval authority of the Council upon recommendation by the European Commission's Security Expert Group;
 - b) where warranted on specific operational grounds, the Frontex Security Authority may waive the requirements referred to under point a) and grant an interim approval for a specific period.

5. During transmission, processing and storage of EUCI by electronic means, approved cryptographic products shall be used. Notwithstanding this requirement, specific procedures may be applied under emergency circumstances or in specific technical configurations after approval by the Frontex Security Authority.
6. The Frontex Security Authority may delegate the functions of Information Assurance Authority and Crypto Distribution Authority to a staff member.
7. The Security Authority shall appoint for each system an Information Assurance Operational Authority whose responsibilities shall be defined in implementing rules.
8. The specific responsibilities of the functions described in paragraphs 5 and 6 shall be defined in the implementing rules and specific arrangements as regards cybersecurity are defined in Frontex Policy on Cyber Security.

Article 54

Accreditation of CIS handling EUCI

1. All CIS handling EUCI shall undergo an accreditation process, based upon the principles of Information Assurance, whose level of detail must be commensurate with the level of protection required.
2. The accreditation process shall include the formal validation of the Security Plan for the CIS concerned by the Security Accreditation Authority in order to obtain assurance that:
 - a) the risk management process, as referred to in Article 53(1)(e), has been properly carried out;
 - b) the Security Authority 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 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.
4. The accreditation shall be the responsibility of the Security Accreditation Authority, 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 operations are no longer satisfied
 - i) require the definition and effective implementation of a security improvement plan within a well-defined timescale;
 - ii) potentially withdraw permission to operate the CIS until conditions for operations are again satisfied.
5. The accreditation process shall be established and detailed in the Frontex classified Communication and Information Systems Security Accreditation Policy adopted in accordance with Article 70 of this Decision.

Article 55

Emergency circumstances

1. Notwithstanding the provisions of this Chapter, the specific procedures described below may be applied in an emergency, such as during an impending or actual crisis, conflict, war situation or in exceptional operational circumstances.
2. EUCI may be transmitted without encryption with the consent of the Frontex Security 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 Frontex Security Authority.

CHAPTER 10

EXCHANGE OF CLASSIFIED INFORMATION WITH UNION INSTITUTIONS, AGENCIES, BODIES AND OFFICES, WITH MEMBER STATES AND WITH THIRD COUNTRIES AND INTERNATIONAL ORGANISATIONS

Article 56

Basic principles

1. Where there is a need to exchange classified information with specific authorities of third countries or departments thereof, or with international organisations, Frontex shall do so within the framework of an arrangement and in accordance with the Regulation. Such arrangements²³ may be concluded only with the authorisation of the Management Board after having received the prior approval of the Commission. These arrangements concern the parties signing and shall not be binding on the Union or on the Member States. Frontex shall inform the relevant institutional partners of such arrangements, in accordance with the Regulation.
2. The arrangements referred to in paragraph 1 may only be concluded with those specific authorities of third countries or departments thereof, or with those international organisations with which the European Commission already has an Administrative Arrangement or Security of Information Agreement in place within the meaning of Chapter 7 of Commission Decision 2015/444.
3. Where Frontex or one of its entities determines that there is an exceptional need in the context of a Union political or legal framework to release EUCI to a third country or international organisation but no relevant arrangements regarding exchange of classified information are in place, the Frontex Security Authority decision shall first be approved by the European Commission.
4. EUCI may be shared only with a Union institution, agency, body or office which has equivalent basic principles and minimum standards for protecting such information in place and if there is an appropriate legal or administrative framework.
5. Any arrangements that cover the exchange or sharing of classified information will be subject to the Commission's prior approval.
6. The transmission and handling of information and documents transmitted to the European Parliament in accordance with the Regulation shall comply with the rules concerning the forwarding
7. and handling of classified information which are applicable between the European Parliament and the European Commission.
8. The decision to release EUCI originating in Frontex shall be taken by the originator 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 European Union or one or more Member States. If the

²³ Pursuant to Article 92(1) of the Regulation.

originator of the classified information for which release is desired, or of the source material it may contain, is not Frontex, the Frontex entity which holds this classified information, shall first seek the originator's written consent to release. If the originator cannot be established, the Frontex entity, which holds this classified information, shall assume the former's responsibility after consulting the European Commission.

Article 57

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, Frontex 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 CIS, which guarantee an equivalent level of protection of EUCI as that afforded in Frontex;
 - c) marks classified information which it creates, as EUCI.
2. The Frontex Security Authority shall, in close cooperation with the European Commission, be the lead service within Frontex for the conclusion of arrangements for sharing EUCI with Union institutions, agencies, bodies or offices.
3. Arrangements shall as a general rule take the form of an Exchange of Letters, signed by the Executive Director on behalf of Frontex.
4. Before entering into an arrangement on sharing EUCI, the Frontex 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 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. The Frontex Security Authority shall be informed of the process of concluding arrangements pursuant to paragraph 2.

Article 58

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 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 Union²⁴.
2. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the European Union, Frontex 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 to the Agreement
3. between the Member States of the European Union, meeting within the Council, regarding the

²⁴ Agreement 2011/C 202/05, OJ C 202, 8.7.2011, p. 13.

protection of classified information exchanged in the interests of the European Union.

Article 59

Exchange of classified information with specific authorities of third countries or departments thereof and international organisations

1. Any administrative arrangement established by Frontex within the meaning of Article 56(1) shall ensure that EUCI is given protection appropriate to its classification level and according to minimum standards which are laid down in this Decision.
2. The European Commission shall give prior agreement to the conclusion of any arrangement established within the meaning of Article 56.

Article 60

Exceptional ad hoc release of EUCI

1. In the absence of an arrangement with the specific authority concerned of a third country, department thereof or international organisation, and in the absence of working arrangements with Union institutions, agencies, bodies and offices, EUCI may be released under the exceptional ad hoc release procedure. The decision to release shall be taken by the Frontex Security Authority after consultation with and prior approval of the European Commission on the basis of a proposal by the Frontex Security Authority.
2. Following the Frontex Security Authority's decision to release the EUCI and subject to the prior written consent of the originator, including the originators of source material it may contain, the Frontex EUCI Registry shall forward the information concerned. The information shall bear a releasability marking indicating the relevant specific authority of a third country, department thereof, international organisation, or Union institution, agency, body or office to which it is being released. Prior to or upon actual release, the third party in question shall undertake in writing to protect the EUCI it receives in accordance with the basic principles and minimum standards set out in this Decision.

CHAPTER 11

INDUSTRIAL SECURITY

Article 61

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) beneficiaries throughout the life-cycle of classified grant agreements.
2. Unless stated otherwise, provisions in this Chapter referring to classified contracts and grant agreements or to contractors and beneficiaries shall be applicable also to classified subcontracts and subcontractors.
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 Frontex Security Authority, 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

Frontex Security Authority and the relevant NSA or DSA.

4. The Frontex Security Officer, when necessary, may consult the relevant services of the European Commission and of the National Authorities.
5. Implementing rules on Industrial Security shall be issued in accordance with Article 70.

Article 62

Procedure for classified contracts or grant agreements

1. Frontex, 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 grant agreements.
2. The Frontex Security Officer 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, and respectively beneficiaries of grant agreements.
3. When the Authorising Officer intends to launch a procedure aimed at concluding a classified contract or grant agreement, he shall obligatorily seek the advice of the Frontex Security Officer on issues regarding the classified nature and elements of the procedure, during all its stages.
4. Classified contracts or grant agreements may be concluded to economic operators registered in a third country only if that third country has concluded a security of information agreement with the EU.

Article 63

Security elements in a classified contract or grant agreement

1. Classified contracts or grant agreements shall include the following security elements:
 - a) 'Security Aspects Letter' ('SAL') means a set of special contractual conditions, issued by the contracting or granting authority. The SAL forms an integral part of any classified contract or grant agreement or sub-contract, and identifies the security requirements and those elements requiring security protection in accordance with the minimum standards laid down in this Decision;
 - b) '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. SCG shall be part of the SAL or PSI.
2. Classified contracts or grant agreements may also include 'Programme or Project Security Instruction' ('PSI'), which is a list of security procedures applied to a specific programme or project in order to standardize security procedures.

Article 64

Access to EUCI for contractors' and beneficiaries' staff

Classified contract or classified grant agreement shall include provisions indicating that staff of a contractor, subcontractor or 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) it has been established that they have a need-to-know;
- 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 65
Facility security clearance

1. A Facility Security Clearance ('FSC') granted by the NSA, DSA or any other competent security authority shall be forwarded by the Frontex Security Officer to the Frontex entity 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 at its facilities.
2. Where relevant, the Frontex Security Authority shall notify the appropriate NSA, DSA or any other competent security authority that an FSC is required during the course of a classified procurement or grant award procedure and/or for performing the classified contract or grant agreement.
3. Frontex shall not award a classified contract or grant agreement to a preferred tenderer or participant before having received confirmation from the NSA, DSA or any other competent security authority of the country in which the contractor, subcontractor or grant beneficiary concerned is registered that, where required, an appropriate FSC has been issued.
4. When the Frontex Security Authority 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 Frontex entity in charge of the procurement or grant procedure. In the case of a sub-contract, the NSA, DSA or any other competent security authority shall be informed accordingly.
5. Withdrawal of an FSC by the relevant NSA, DSA or any other competent security authority shall constitute sufficient grounds for Frontex to terminate a classified contract or grant agreement, 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 66
Provisions for classified contracts and grant agreements

1. Where EUCI is provided to a candidate, tenderer or applicant during the procurement or granting 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 Frontex Security Authority shall notify 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 beneficiaries, the duration of the contract and the maximum level of classification.
3. When such contracts or grant agreements are terminated, the Frontex Security Authority shall promptly notify the NSA, DSA or any other competent security authority in which the contractor or grant beneficiary is registered.
4. As a general rule, the contractor or beneficiary shall be required to return to Frontex, upon termination of the classified contract or grant agreement, 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 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.
7. With regard to EUCI created or handled by the contractor, grant beneficiary or subcontractor, Frontex shall be considered to be the originator, and the rights incumbent on the originator shall be exercised by Frontex.

Article 67

Subcontracting for classified contracts or grant agreements

1. The conditions relevant for the protection of EUCI under which the contractor or beneficiary may subcontract shall be defined in the call for tender or for proposal and in the classified contract or grant agreement.
2. A contractor or beneficiary shall obtain permission from Frontex, 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 that third country has a Security of Information Agreement with the European Union.
3. The contractor or 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 Frontex.

Article 68

Visits in connection with classified contracts or grants agreements

1. Where Frontex staff members 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, DSAs or any other competent security authority concerned. The Frontex Security Authority shall be informed of such visits to Frontex facilities. However, in the context of specific programmes or projects, the NSAs, DSAs 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.

CHAPTER 12

FINAL PROVISIONS

Article 69

Classified information created before the entry into force of this Decision

All classified information held by Frontex before the entry into force of this Decision shall:

- a) If created by Frontex, retain its original classification and be treated as EUCI of the equivalent level;
- b) If created by authors outside Frontex, retain its original classification and be protected as EUCI of the equivalent level.

Article 70

Implementing rules and security notices

1. As necessary, the Frontex Security Authority shall adopt implementing rules for this Decision.
2. The Frontex Security Authority may adopt security notices setting out security guidelines and best practices within the scope of this Decision and its implementing rules.

Article 71

Processing of personal data

1. Frontex shall process personal data needed for implementing this Decision in accordance with

Regulation (EU) No 2018/1725.

2. Notwithstanding the measures already in place at the time of adoption of this Decision and notified to the European Data Protection Supervisor, any measure under this Decision involving the processing of personal data, such as relating to access and exit logs, CCTV recordings, recordings of telephone calls to duty offices or dispatch centres and similar data, which are required for reasons of security or crisis response, shall be subject to implementing rules in accordance with Article 70 which lays down appropriate safeguards for data subjects.
3. The Frontex Security Authority shall be responsible for the security of any processing of personal data undertaken in the context of this Decision.

Article 72

Transparency

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