Ref.: EUSPA-SEC-AB-DEC-A22113

Version: 1.0

AB decision no.: EUSPA-AB-08-23-01-08

EU Agency for the Space Programme

Administrative Board 8

Prague, 26 January 2023

Decision of the Administrative Board on Security in the Agency

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

adopting the European Union Agency for the Space Programme Decision on Security in the Agency

THE ADMINISTRATIVE BOARD OF THE EUROPEAN AGENCY FOR THE SPACE PROGRAMME (hereinafter "the Agency"),

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

Having regard to Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission;

Having regard to the European Union Agency for the Space Programme Decision on the security rules for protecting EU Classified Information (EUSPA-AB-07-22-10-05);

Whereas:

1) The Agency is required, subject to prior consultation of the Commission, to adopt its own security rules equivalent to the Commission's security rules for protecting EUCI and sensitive non-classified information, including rules concerning the exchange, processing and storage of such information, in accordance with Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission and Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information;
2) The objective of security within the Agency is to enable it to operate in a safe and secure environment by establishing a coherent, integrated approach as regards its security, providing appropriate levels of protection for persons, assets and information commensurate with identified risks, and ensuring efficient and timely delivery of security. Security in the Agency must be based on the principles of legality, transparency, proportionality and accountability;
3) The Agency has consulted the Commission on such rules;
4) The Administrative Board of the Agency has adopted the European Union Agency for the Space Programme Decision on the security rules for protecting EU Classified Information (EUSPA-AB-07-22-10-05).

HAS DECIDED AS FOLLOWS:

Article 1 – Adoption

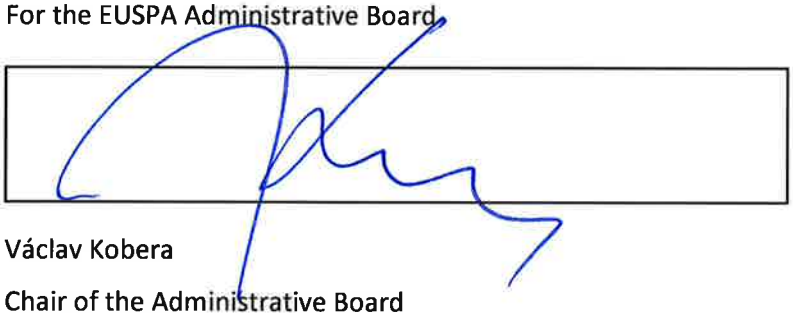
The European Union Agency for the Space Programme Decision on Security in the Agency, as set out in the Annex to this Decision, is hereby adopted.

Article 2- Entry into force

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

Done in Prague, on 26 January 2023

For the EUSPA Administrative Board,



Václav Kobera

Chair of the Administrative Board

Annexes:
Annex- European Union Agency for the Space Programme Decision on Security in the Agency.

ANNEX

European Union Agency for the Space Programme Decision on Security in the Agency

CHAPTER 1 – GENERAL PROVISIONS

Article 1 - Definitions

For the purposes of this Decision the following definitions apply:

1. 'assets' means all movable and immovable property and possessions of the Agency; including immovable property which the Agency is entitled to use on the basis of a hosting agreement, a lease or similar agreement;
2. 'Agency department' means a department, including administrative and operational department, within the organisational structure of the Agency approved by the Administrative Board;
3. '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. 'Agency CIS' means CIS owned by the Agency (this definition excludes the systems of the Space Programme Components);
4. 'control of risks' means any security measure that can reasonably be expected to effectively control a risk to security by its prevention, mitigation, avoidance or transfer;
5. '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 the Agency, regardless of its origin;
6. 'data' means information in a form that allows it to be communicated, recorded or processed;
7. 'personal data' means personal data as defined in Article 2(a) of Regulation (EC) No 2018/1725 of the European Parliament and of the Council[1];
8. 'premises' means any immovable or assimilated property and possessions which the Agency is entitled to use on the basis of a hosting agreement, a lease or similar agreement;
9. 'prevention of risk' means security measures that can reasonably be expected to impede, delay or stop a risk to security;
10. 'risk to security' means the combination of the threat level, the level of vulnerability and the possible impact of an event;
11. 'security in the Agency' means the security of persons, assets and information in the Agency, and in particular the physical integrity of persons and assets, the integrity,

[1] Regulation (EU) 2018/1725 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

confidentiality and availability of information and Communication and Information Systems, as well as the unobstructed functioning of the Agency operations;

12. 'security measure' means any measure taken in accordance with this Decision for purposes of controlling risks to security;
13. 'security rules' means European Union Agency for the Space Programme Decision on Security in the Agency as approved by the Administrative Board;
14. 'sites' means the actual premises where the Agency is entrusted with responsibilities for its security, including where specified in the relevant hosting agreement, lease or similar agreement;
15. 'Staff Regulations' means the Staff Regulations of officials of the European Union, as laid down by Regulation (EEC, Euratom, ECSC) No 259/68 of the Council[2] and its amending acts;
16. 'threat to security' means an event or agent that can reasonably be expected to adversely affect security if not responded to and controlled;
17. 'immediate threat to security' means a threat to security which occurs with no or with extremely short advance warning; and
18. '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 the Agency;
19. 'vulnerability' means a weakness of any nature that can reasonably be expected to adversely affect security in the Agency, if exploited by one or more threats.

Article 2 – Subject matter and scope

1. This Decision sets out the objectives, basic principles, organisation and responsibilities regarding security at the Agency.
2. This Decision shall apply to all Agency departments and in all its premises and sites.
3. Notwithstanding any specific indications concerning particular groups of staff, this Decision shall apply to Agency staff under the scope of the Staff Regulations and of the Conditions of Employment of other servants of the European Union, to national experts seconded to the Agency (SNEs), to service providers and their staff, to trainees and to any individual with access to Agency premises, sites or other assets, or to information handled by the Agency.

CHAPTER 2 - PRINCIPLES

Article 3 – Principles for security in the Agency

1. In implementing this Decision, the Agency shall comply with the Treaties and in particular the Charter of Fundamental Rights and Protocol No. 7 on the Privileges and Immunities of

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

the European Union, with any applicable rules of national law as well as with the terms of the present Decision. If necessary, a security notice in the sense of Article 21(2) providing guidance in this respect shall be issued.

2. Security in the Agency shall be based on the principles of legality, transparency, proportionality and accountability.
3. The principle of legality indicates the need to stay strictly within the legal framework in implementing this Decision and the need to conform to the legal requirements.
4. Any security measure 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.
5. Agency departments shall ensure that security issues are taken into account from the start of the development and implementation of the Agency policies, decisions, programmes, projects and activities for which they are responsible. In order to do so, they shall involve the Security Authority in general and the Head of the department responsible for ICT in the Agency as regards ICT systems from the earliest stages of preparation.
6. The Agency shall, where appropriate, seek cooperation with the competent authorities of the host state, of other Member States and of EU institutions, other agencies or bodies, where feasible, taking account of the measures taken or planned by those authorities to address the risk to security concerned.

Article 4 – Obligation to comply

1. Compliance with this Decision and with the security rules of the Agency shall be mandatory.
2. Non-compliance with the security rules and this Decision may trigger liability to disciplinary action in accordance with the Treaties, the Staff Regulations, to contractual sanctions and/or to legal action under national laws and regulations.

CHAPTER 3 – DELIVERING SECURITY

Article 5 – Mandated staff

1. Only staff appointed on the basis of a nominative mandate by the Security Authority in consultation with the Executive Director, given their current duties, may be entrusted with the obligation to take one or several of the following measures:
   a. Carry side arms;
   b. Conduct security inquiries as referred to in Article 13;
   c. Take security measures as referred to in Article 12 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 person concerned holds the post or function in respect of which the mandate has been conferred. They 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 6 – General provision regarding security measures

1. When taking security measures, the Agency shall in particular ensure so far as reasonably possible, that:
   a. it only seeks support or assistance from the state concerned, provided that that state is either a Member State of the European Union or, if not, party to the European Convention on Human Rights, or guarantees rights which are at least equivalent to the rights guaranteed in this Convention;
   b. it shall only transfer information on an individual to recipients, other than Union institutions and bodies, which are not subject to national law adopted pursuant to Regulation (EU) 2016/679[3], in accordance with Article 9 of Regulation (EU) No 2018/1725;
   c. 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 incurring costs. 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. the Agency 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 individual and his/her rights.
2. The Security Authority shall establish an overview of security measures which may require an order by a judge in accordance with the laws and regulations of the Member States hosting Agency premises.
3. The Security Authority may turn to a contractor to carry out, under their direction and supervision, tasks relating to security.

Article 7 – Security measures regarding persons

1. An appropriate level of protection shall be afforded to persons in the premises of the Agency, taking into account security and safety requirements.
2. In case of major risks to security, the Agency may order the evacuation of its premises.
3. Victims of accidents or attacks within Agency premises shall receive assistance.
4. In order to prevent and control risks to security, mandated staff, to the extent permitted and subject to any authorisation provided under any applicable law, may carry out background checks of persons falling under the scope of this Decision, so as to determine whether giving such persons access to Agency premises or information presents a threat to security. For that purpose, and in compliance with Regulation (EU) No 2018/1725 and provisions referred to under Article 3(1), the mandated staff concerned may:
   a. use any source of information available to the Agency, taking into account the reliability of the source of information;

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.

b. access the personnel file or data the Agency holds with regard to individuals it employs or intends to employ, or for contractors' staff when duly justified.

Article 8 – 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 the Agency as well as to protect assets.
3. Physical security shall have the following objectives:
   a. preventing acts of violence directed against staff members of the Agency or 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 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 22(2) hereunder and other information sources.
4. Physical security shall include at least:
   a. an access policy applicable to any person or vehicle requiring access to the 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,
   c. Intrusion Detection System (IDS),
   d. CCTV system.
5. In order to ensure physical security, the following actions may be taken:
   a. recording entry to and exit from Agency premises of persons, vehicles, goods and equipment,
   b. identity controls at Agency premises,
   c. inspection of vehicles, goods and equipment by visual or technical means,
   d. preventing unauthorised persons, vehicles and goods, from entering Agency premises.

Article 9 – Security measures regarding information

1. Security of information covers all information handled by the Agency.
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 classify 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' (hereafter 'EUCI'), that is to say 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;
b. 'Sensitive non-classified information', that is to say information or material the Agency must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof, and/or because of its sensitivity. Sensitive non-classified information 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 1049/2001 of the European Parliament and of the Council[4] 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.

6. Sensitive non-classified information shall be subject to policies regarding its handling and storage. It shall only be released to those individuals who have a 'need-to-know'. When deemed necessary for the effective protection of its confidentiality, it shall be identified by a security marking and corresponding handling instructions approved by the Security Authority of the Agency. When handled or stored on Communication and Information Systems, such information shall be protected also in compliance with the ICT Security Policy of the Agency, its implementing rules and corresponding standards.
7. 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 10 – Security measures regarding Communication and Information Systems

1. All Agency Communication and Information Systems ('CIS') shall comply with the ICT security policy of the Agency, the Agency COMSEC policies, when applicable, and their implementing rules and corresponding security standards.
2. Agency services owning CIS shall only allow Union institutions, other agencies, bodies, Member States or other organisations to have access to those systems provided that those Union institutions, agencies, bodies, Member States or other organisations can provide reasonable assurance that their ICT systems are protected at a level equivalent to the ICT security policy of the Agency, its implementing rules and corresponding security standards. The Agency shall monitor such compliance, and in case of serious non-compliance or continued failure to comply, be entitled to prohibit access.

Article 11 – Forensic analysis regarding cyber-security

The Security Authority shall in particular be responsible for conducting forensic technical analysis, as needed, in cooperation with the competent teams of the Agency in support of

[4] 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).

the security inquiries referred to in Article 13, related to counterintelligence, data leakage, cyberattacks and information systems security.

Article 12 – Security measures regarding persons and objects

1. In order to ensure security in the Agency and to prevent and control risks, staff mandated in accordance with Article 5 may, in compliance with the principles set out in Article 3 including without limitations provisions under Regulation 2018/1725 and relevant guidelines issued by EDPS, 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 the Agency's premises, escorting persons from the Agency's premises, banning persons from the Agency's premises for a period of time, the latter implemented in accordance with criteria to be defined in security policies;
   c. limited measures concerning objects posing a threat to security including removal, seizure and disposal of objects;
   d. searching of premises, where applicable, including of offices within them;
   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 the Agency's rights as a landlord or as an employer in accordance with the applicable national laws.
2. Under exceptional circumstances, staff members of the Security Authority Department, mandated in accordance with Article 5, 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 inform the Security Authority, who shall confirm the measures taken and authorise any 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, within reasonable delay after they are 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 their rights of defence and of protection of personal data in accordance with Regulation (EU) No 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 (b), the Agency shall in addition guarantee that the individual concerned is given the opportunity to contact a lawyer or a person of confidence and be made aware of their right to have recourse to the Agency Data Protection Officer or the European Data Protection Supervisor.

Article 13 – Inquiries

1. Without prejudice to Article 86 and Annex IX of the Staff Regulations, security inquiries may be conducted:
   a. in case of incidents affecting security at the Agency, including suspected criminal offences;
   b. in case of potential leakage, mishandling or compromise of sensitive non-classified information, EUCI or other classified information;
   c. in the context of counter-intelligence and counter-terrorism;
   d. in case of serious cyber-incidents.
2. The decision to conduct a security inquiry shall be taken by the Security Authority who will also be the recipient of the inquiry report.
3. Security inquiries shall be conducted only by dedicated members of staff appointed by the Security Authority in consultation with the Executive Director, duly mandated in accordance with Article 5.
4. The mandated staff shall exercise their powers of security inquiry independently, as specified in the mandate and shall have the powers listed in Article 12.
5. 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 the Agency premises or involving persons referred to in Article 2(3) either as victim or perpetrator of such offences.
6. The Security Authority 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 a criminal act having been perpetrated. In this context, the Security Authority may, where appropriate or required, provide support to the authorities of the host Member State or any other Member State concerned.
7. In the case of cyber-incidents, the department responsible for ICT shall collaborate closely with the Security Authority to provide support on all technical matters. The Security Authority shall decide, in consultation with the department responsible for ICT, when it is appropriate to inform the competent authorities of the host country or any other Member State concerned. The incident coordination services of Computer Emergency Response Team for the European institutions, bodies and agencies ('CERT-EU') will be used as regards support to EU institutions and other agencies that may be affected.
8. Security inquiries shall be documented.

Article 14 – Delineation of competences with regard to security inquiries and other types of investigation

1. Where the Security Authority conducts security inquiries, as referred to in Article 13, and if these enquiries fall within the competences of the European Anti-Fraud Office (OLAF) or the Disciplinary Board of the Agency, it shall liaise with those bodies at once with a view, in particular, not to compromise later steps by either OLAF or the Disciplinary Board of the Agency. Where appropriate, the Security Authority shall invite OLAF or the Disciplinary Board of the Agency to be involved in the investigation.
2. The security inquiries, as referred to in Article 13, shall be without prejudice to the powers of OLAF or the Disciplinary Board of the Agency as laid down in the rules governing those

bodies. The Security Authority may be requested to provide technical assistance for inquiries initiated by OLAF or the Disciplinary Board of the Agency.

3. The Security Authority may be asked to assist OLAF's agents when they access Agency premises in accordance with Articles 3(5) and 4(4) of Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council[5], in order to facilitate their tasks. The Security Authority informs the Executive Director of such requests for assistance.
4. Without prejudice to Article 22(a) of the Staff Regulations, where a case may fall within the competence of both the Security Authority and the Disciplinary Board of the Agency, the Security Authority shall, in compliance with Article 13, at the earliest possible stage advise whether there are grounds that justify that the Disciplinary Board of the Agency be seized with the matter. This stage shall in particular be considered to have been reached when an immediate threat to security has come to an end. The Security Authority shall decide on the matter.
5. Where a case may fall within the competence of both the Security Authority and OLAF, the Security Authority shall inform the Executive Director who will inform the Director-General of OLAF at the earliest possible stage. This stage shall in particular be considered to have been reached when an immediate threat to security has come to an end.

Article 15 – Security inspections

1. The Security Authority shall undertake security inspections in order to verify compliance by Agency services, premises and individuals with this Decision and its implementing rules and to formulate recommendations when deemed necessary.
2. Where appropriate, the Security Authority shall undertake security inspections or security monitoring or assessment visits to verify whether the security of Agency staff, assets and information falling under the responsibility of Union institutions, other agencies or bodies, Member States, third states or international organisations, are appropriately protected in accordance with security rules, regulations and standards which are at least equivalent to those of the Agency. Where appropriate and in the spirit of good cooperation between administrations, those security inspections shall also include inspections conducted in the context of the exchange of classified information with Union institutions, other agencies and bodies, Member States or with third states or international organisations.

Article 16 – Alert states and management of crisis situations

1. The 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 the Agency, and for measures required for managing crisis situations.
2. The alert state measures referred to in paragraph 1 shall be commensurate with the level of threat to security. The alert states levels shall be defined in close cooperation with the competent services of Union institutions, other agencies and bodies, and of the Member States hosting Agency premises.

[5] 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).

3. The Security Authority shall be the contact point for alert states and management of crisis situations.

CHAPTER 4 - ORGANISATION

Article 17 – General responsibilities

1. The responsibilities of the Agency referred to in this Decision shall be exercised by the Security Authority of the Agency.
2. The specific arrangements as regards cyber-security are defined in the ICT Security Policy of the Agency.
3. The responsibilities for implementing this Decision and its implementing rules and for day-to-day compliance may be delegated to Agency Departments, whenever decentralised delivery of security offers significant efficiency, resource or time savings, for instance because of the geographical location of the services concerned.
4. Where paragraph 3 applies, the Security Authority, and where appropriate the department responsible for ICT, shall conclude arrangements with individual Agency departments establishing clear roles and responsibilities for the implementation and monitoring of security policies.

Article 18 – The Security Authority

1. The Security Authority (SA), shall perform its functions in the following areas as laid down in European Union Agency for the Space Programme Decision on the security rules for protecting EU Classified Information:
   a. personnel security;
   b. physical security;
   c. management of EUCI;
   d. accreditation of Agency communication and information systems (CIS) handling EUCI;
   e. industrial security; and
   f. exchange of classified information.
2. The Security Authority shall ensure mandatory training for the Local Security Officers (LSOs), deputy LSOs, Registry Control Officers (RCOs), deputy RCOs, as well as for the Local Informatics Security Officers (LISOs), deputy LISOs, Crypto Custodians (CC), deputy CC, Communication Security Officers (COMSOs) and deputy COMSOs, on their responsibilities and duties.
3. The Security Authority of the Agency, is entrusted with the following functions:
   a. Information Assurance Authority (IAA)
   b. Security Accreditation Authority (SAA)
   c. TEMPEST Authority (TA)
   d. Crypto Approval Authority (CAA)
   e. Crypto Distribution Authority (CDA)

   The Security Authority can delegate these functions to Agency staff.
4. The Security Accreditation Authority shall be consulted in coordination with the LSO and the LISO as appropriate whenever a department intends to:
   a. construct a Secured Area;

b. implement an Agency CIS to handle EUCI;
c. install any other equipment for the handling of classified information, including connections to a third-party CIS.

5. The Security Accreditation Authority shall provide advice in respect of these activities during both the planning and the construction or development processes.
6. EUCI shall not be handled in a Secured Area or CIS before the Security Accreditation Authority has issued an accreditation at the appropriate level of EUCI.
7. The requirements for accrediting a Secured Area shall include:
   a. approval of the plans for the Secured Area;
   b. approval of any contracts for works performed by external contractors, taking into consideration the provisions on industrial security such as any requirements for security clearances of the contractors and their staff;
   c. availability of all requisite declarations and certificates of conformity;
   d. a physical inspection of the Secured Area to verify that the building materials and methods, access controls, security equipment and any other items comply with the requirements issued by the Security Authority;
   e. validation of the countermeasures against electromagnetic radiation for any technically Secured Area;
   f. approval of the security operating procedures (SecOPs) for the Secured Area.
8. The requirements for accrediting an Agency CIS handling EUCI shall include:
   a. creation of a System Accreditation Strategy;
   b. validation of the CIS's security plan, based on a risk management approach;
   c. validation of the SecOPs for the CIS;
   d. validation of all other required security documentation, as determined by the Security Accreditation Authority;
   e. approval of any use of encrypting technologies;
   f. validation of the countermeasures against electromagnetic radiation for a CIS handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above;
   g. an inspection of the CIS to verify that the documented security measures are correctly implemented.
9. Following successful fulfilment of the requirements for accreditation, the Security Accreditation Authority shall issue a formal authorisation for the handling of EUCI in the Secured Area or an Agency CIS, for a stated maximum level of EUCI and for up to 5 years, depending on the levels of EUCI handled and the risks involved.
10. Upon notification of a security breach or a significant change in the design or security measures of a Secured Area or Agency CIS, the Security Accreditation Authority shall review and, if necessary, may revoke the authorisation to handle EUCI until any identified issues are resolved.
11. The Information Assurance Authority (IAA) shall be responsible of the following activities in relation to the protection of EUCI:
    a. developing information assurance security policies and security guidelines and monitoring their effectiveness and pertinence;
    b. safeguarding and administering technical information related to cryptographic products;
    c. ensuring that information assurance measures comply with the Agency's security and procurement policies as appropriate;

d. ensuring that cryptographic products are selected in compliance with policies governing their eligibility and selection;
e. consulting with system owners, system providers, security actors and representatives of users with respect to information assurance security policies and security guidelines.

12. TEMPEST security measures shall be implemented to protect CIS handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, and may be implemented for information classified RESTREINT UE/EU RESTRICTED.
13. The TEMPEST Authority shall be responsible for approving the measures taken to protect against compromise of EUCI through unintentional electronic emanations.
14. Upon request from a system owner of a CIS handling EUCI, the TEMPEST Authority shall issue specifications for TEMPEST security measures as appropriate for the classification level of the information.
15. The TEMPEST Authority shall ensure the performance of technical testing during the accreditation of Secured Areas and CIS for handling EUCI at the level of CONFIDENTIAL UE/EU CONFIDENTIAL or above and, upon successful testing, issue a TEMPEST certificate.
16. A TEMPEST certificate shall specify at least:
    a. the date of the test;
    b. a description of the TEMPEST security measures, with plans of the area;
    c. the expiry date of the certificate;
    d. any changes that will invalidate the certification;
    e. the signature of the TEMPEST Authority.
17. An LSO or a meeting organiser with the responsibility for organising a classified meeting, in coordination with the LSO, may request the TEMPEST Authority to test meeting rooms in order to ensure that they are technically secured.
18. The CAA shall be responsible for approving the use of encrypting technologies.
19. The CAA shall issue guidance on the requirements for the use and approval of encrypting technologies.
20. The CAA shall approve the use of encryption solutions on the basis of a request from the system owner. Without prejudice to Article 34.4 of the European Union Agency for the Space Programme Decision on the security rules for protecting EU Classified Information, the approval shall be based upon a satisfactory evaluation of at least:
    a. the security needs of the information to be protected;
    b. an overview of the CIS involved in the solution;
    c. an assessment of the inherent and residual risks;
    d. a description of the proposed solution;
    e. the SecOPs for the encryption solution.
21. The CAA shall keep a register of approved encryption solutions.
22. The CDA shall be responsible for distributing cryptographic materials used for protecting EUCI (mainly encryption equipment, cryptographic keys, certificates and related authenticators) to the following:
    a. users or departments inside the Agency;
    b. users or organisations outside the Agency for CIS that are administered by the Agency.
23. The CDA may delegate the distribution of cryptographic materials for third parties to other departments in line with Article 17(3) of this Decision.
24. The CDA shall ensure that all cryptographic materials are sent via secure channels that protect against and show evidence of any tampering, in line with the security rules

applicable for the level of classification of the EUCI that will be protected by those materials.

25. The CDA shall provide guidance to the Local Security Officer (LSO), the Crypto Custodian and the Communication Security Officer (COMSO) and, where relevant, the LISO of each Agency premise that is involved in the production, distribution or use of the cryptographic materials.
26. The CDA shall ensure that suitable SecOPs are established for the distribution process.

Article 19 – Information Assurance Operational Authority

1. The Information Assurance Operational Authority (IAOA) for each CIS of the Agency shall:
   a. establish security documentation in line with security policies and guidelines, in particular the security plan, the SecOPs related to the system and the cryptographic documentation within the CIS accreditation process;
   b. participate in selecting and testing the system-specific technical security measures, devices and software, to supervise their implementation and to ensure that they are securely installed, configured and maintained in accordance with the relevant security documentation;
   c. participate in selecting TEMPEST security measures and devices, if required in the security plan, and, in cooperation with the TEMPEST Authority, ensure that they are securely installed and maintained;
   d. monitor implementation and application of the SecOPs related to the operation of the system;
   e. manage and handle cryptographic products, in collaboration with the CDA, to ensure the proper custody of cryptographic materials and controlled items and, if required, ensure the generation of cryptographic variables;
   f. conduct security analysis, reviews and tests, in particular to produce the relevant risk reports, as required by the Security Accreditation Authority;
   g. provide CIS-specific Information Assurance training;
   h. implement and operate CIS-specific security measures.

Article 20 – Agency Security Roles

1. Local Security Officer (LSO)
   a. For each Agency site (or premise, if needed), an LSO shall be appointed by the Agency Security Authority. The LSO shall act as the principal point of contact between the site or premise and the Security Authority on all matters related to security in the Agency. Where appropriate one or more deputy LSOs may be appointed. The LSO shall be an official or a temporary agent.
   b. As the main point of contact on security for each site or premise, the LSO shall, at regular intervals, report to the Security Authority and to their hierarchy on security issues involving their Agency site or premise and, immediately, on any security incidents, including those where EUCI or sensitive non-classified information may have been compromised.
   c. For matters related to security of CIS, the LSO shall liaise with the LISO.

d. The LSO shall contribute to security training and awareness activities addressing the specific needs of staff, contractors and other individuals working at the respective Agency site or premise.
e. The LSO may be assigned specific tasks in cases of major or immediate risks to security or of emergencies at the request of the Security Authority.
f. The responsibilities of the LSO shall be without prejudice to the role and responsibilities assigned to LISOs, Health and Safety Managers, RCOs or any other function implying security or safety-related responsibilities. The LSO shall liaise with them in order to ensure a coherent and consistent approach to security and an efficient flow of information on matters related to security in the Agency.
g. The LSO shall have direct access to the Security Authority, while informing their direct hierarchy.
h. The LSO shall hold a security authorisation to access EUCI, at least up to the level of SECRET UE/EU SECRET.
i. In order to promote the exchange of information and best practices, the Security Authority will grant permission at least twice a year for the LSO to attend a dedicated LSO conference. Attendance of LSOs at the conferences organised by the European Commission shall be mandatory.

2. Registry Control Officer (RCO)
   a. The Agency EUCI registries shall be managed by RCOs. The RCO shall be appropriately security cleared.
   b. The RCO shall be subject to the supervision of the LSO, 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.
   c. Within their responsibility for managing the EUCI Registry to which they have been assigned, the RCO shall assume the following overall tasks:
      i. Manage operations relating to the registration, preservation, reproduction, translation, transmission, dispatch and destruction of EUCI;
      ii. Verify periodically the need to maintain the classification of information;
      iii. Assume any other tasks related to the protection of EUCI defined in implementing rules.
3. Local Informatics Security Officer (LISO)
   The role and responsibilities of the LISO shall be defined in the Agency ICT Security Policy.
4. Crypto Custodian (CC)
   a. The Agency COMSEC accounts shall be managed by CCs. The CC shall be appropriately security cleared.
   b. The role and responsibilities of the Crypto Custodian shall be defined in the Agency COMSEC Policy.
5. Communication Security Officer (COMSO)
   The role and responsibilities of the COMSO shall be defined in the Agency COMSEC Policy.

CHAPTER 5 - IMPLEMENTATION

Article 21 – Implementing rules and security notices

1. The Administrative Board may delegate the adoption of implementing rules for this Decision to the Security Authority of the Agency by a separate delegation decision, in full compliance with the internal rules of procedure.
2. The Security Authority of the Agency is empowered to develop and adopt security policies, processes, procedures as well as security notices setting out guidelines and best practices with the scope of this Decision and its implementing rules.

CHAPTER 6 – MISCELLANEOUS AND FINAL PROVISIONS

Article 22 – Processing of personal data

1. The Agency 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, 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 21, which shall lay down appropriate safeguards for data subjects.
3. The Security Authority shall be responsible for the security of any processing of personal data undertaken in the context of this Decision.
4. Those implementing rules and procedures shall be adopted after consultation of the Agency Data Protection Officer in accordance with Regulation (EU) 2018/1725.

Article 23 – Transparency

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

Article 24 – Entry into force

This Decision shall enter into force on the day of adoption by the Administrative Board of the Agency.