Protection level **LIMITED BASIC**

2016-133 REV 3

DECISION OF THE MANAGEMENT BOARD ON SECURITY RULES IN eu-LISA

Handling instructions for the marking LIMITED BASIC

- Distribution on a need-to-know basis.
- Not to be released outside of the information stakeholders.
- Not for publication.

Table of Contents

DECISION OF THE MANAGEMENT BOARD ON SECURITY RULES IN eu-LISA

The Management Board,

Having regard to the *Regulation No. 1077/2011 of the European Parliament and the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice* (referred to hereinafter as "*eu-LISA Regulation*"),

Whereas:

(1) In accordance with Article 30 of the eu-LISA Regulation, eu-LISA shall be responsible for the security and the maintenance of order within the buildings, premises and land used by it and eu-LISA shall apply the security principles and relevant provisions of the legislative instruments governing the development, establishment, operation and use of large-scale IT systems.

(2) In accordance with Article 29 (3) of the eu-LISA Regulation, the Management Board shall decide on the Agency's internal structure necessary to fulfil the appropriate security principles.

(3) Pursuant to Article 29 (1) and (2) of eu-LISA Regulation, eu-LISA shall apply the security principles laid down in Commission Decision (EU, Euratom) 2015/444 of 13 March 2015[1] on the security rules for protecting EU classified information, including the provisions for the exchange, processing and storage of classified information as well as the security principles relating to the processing of non-classified sensitive information as adopted and implemented by the Commission.

(4) Commission Decision 2015/443 of 13 March 2015 sets out the objectives, basic principles, organisation and responsibilities regarding security at the Commission and equivalent rules should apply to the Agency.

(5) Pursuant to Article 12(1)(p) of eu-LISA Regulation, the Management Board shall adopt the necessary security measures, including a security plan and business continuity and disaster recovery plan, taking into account the possible recommendations of the security experts present in the Advisory Groups.

(6) Pursuant to Article 12(1)(q) the Management Board should appoint a Security Officer.

(7) Commission Decision C(2014) 3486 final of 11.6.2014 on the adoption of a Memorandum of Understanding between the European Commission and the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice that establishes specific rules on arrangements concerning crisis and security incidents management and business

1 Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 has repealed and replaced Commission Decision 2001/844/EC of 29 November 2001, referred to in Article 29(1) of the eu-LISA Regulation

continuity, on arrangements in case of major incidents or of any incident related to the operation of the network which could have an impact on the availability, confidentiality and integrity of data or on the quality or the availability of service to the systems' users and on the obligation to consult the Commission on draft security measures and any amendment thereto.

(8) The seat agreement and the agreements on the technical sites of Strasbourg and Sankt Johann im Pongau contain rules with regard to security of the Agency and assistance and cooperation on security matters.

(9) The objective of security within eu-LISA is to operate in a safe and secure environment, providing appropriate levels of protection for persons, assets and information commensurate with identified risks, and ensuring timely delivery of security.

10) Therefore there is a need to establish the regulatory basis for security at eu-LISA,

Has adopted the following Decision:

CHAPTER 1 - GENERAL PROVISIONS

Article 1 - Definitions

For the purposes of this Decision the following definitions apply:

Assets	all movable and immovable property and possessions of eu-LISA
Security Unit	the Unit in eu-LISA responsible for security, directly coordinated by eu-LISA Security Officer
eu-LISA information system	any Communication and Information system of eu-LISA 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 includes, e.g., the large-scale IT Systems operated by the Agency and the Corporate IT Systems
CIS	Communication and Information System
Crisis situation	a circumstance, event, incident or emergency (or a succession or combination thereof) posing a major or an immediate threat to security in eu-LISA, regardless of its origin
Data	information in any form that allows it to be communicated, recorded and processed
Personal data	as defined in Article 2(a) of Regulation (EC) No. 45/2001 of the European Parliament and of the Council[2]
Premises	any immovable or assimilated property and possessions of eu-LISA
Prevention of risk	security measures that can reasonably be expected to impede, delay or stop a risk to security
Risk to security	the combination of the threat level, the level of vulnerability and the possible impact of an event
Security in eu-LISA	the security of persons, assets and information in eu-LISA, 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 eu-LISA operations

2 *"any information relating to an identified or identifiable natural person hereinafter referred to as "data subject"; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity"*

Security measure	any measure taken in accordance with this Decision, the eu-LISA establishing Regulation, the Regulations governing the systems operated by eu-LISA, the seat and site agreements for purposes of controlling risks to security
Staff Regulations	the Staff Regulations of officials of the European Union, as laid down by Regulation (EEC, Euratom, ECSC) No. 259/68 of the Council[3] and its amending acts
Threat to security	an event or agent that can reasonably be expected to adversely affect security if not responded to and controlled
Immediate threat to security	a threat to security which occurs with no or with extremely short advance warning
Major threat to security	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 eu-LISA
Vulnerability	a weakness of any nature that can reasonably be expected to adversely affect security in eu-LISA, if exploited by one or more threats

Article 2 – Subject matter

1. This Decision sets out the objectives, basic principles, organisation and responsibilities regarding security at eu-LISA.
2. It applies to all eu-LISA departments, units and sectors and in all premises of eu-LISA.
3. Notwithstanding any specific indications concerning particular groups of staff, this Decision shall apply to the eu-LISA 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 eu-LISA (SNEs), to service providers and their staff, to trainees (interns) and to any individual with access to eu-LISA buildings or other assets, or to information handled by eu-LISA.

CHAPTER 2 - PRINCIPLES

Article 3 - Principles for security in eu-LISA

1. In implementing this Decision, eu-LISA shall comply with the Treaties and in particular the Charter of Fundamental Rights and Protocol No. 7 on the Privileges and Immunities of the European Union with any applicable rules of national law as well as with the terms of the present Decision. Furthermore, the present rules shall observe the security principles introduced in the regulations on the establishment

3 Regulation (EEC, Euratom, ECSC) No 259 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).

and the operational management of each of the IT systems under the responsibility of eu-LISA. If necessary, specific security standards, policies, procedures and/or notifications providing guidance in this respect shall be issued.

2. Security in eu-LISA 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. The implementation of any security measure shall be performed transparently 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. eu-LISA departments, units and sectors shall ensure that security risks and requirements are taken into account from the start of the development and during the entire phase of the implementation of eu-LISA policies, decisions, programmes, projects and activities for which they are responsible. In order to do so, they shall involve the Security Unit and eu-LISA Security Officer as regards all aspects related to the IT systems, from the earliest stages of preparation.
6. eu-LISA shall, where appropriate, and in line with the specific provisions of the relevant seat and site agreements, seek cooperation with the competent authorities of the host states, of other Member States and of EU institutions, agencies or bodies, where feasible and appropriate, taking account of the measures taken or planned by those authorities to address the risk to security.

Article 4 – Obligation to comply

1. Compliance with the present Decision, with its corresponding security implementing rules, standards, policies, procedures and notices and with the security measures and the instructions given by mandated staff, is mandatory.
2. Non-compliance with this Decision may trigger, depending on the case, disciplinary actions in accordance with the Treaties and the Staff Regulations, contractual sanctions and/or legal actions under national laws and regulations.
3. 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.

CHAPTER 3 - ORGANISATION

Article 5 - General responsibilities of security in eu-LISA

1. The MB responsibilities on security are derived from Article 12(1)p) of the Agency Establishing regulation 1077/2011.
2. The Executive Director's responsibilities are derived from Article 17(6)h) of the Agency Establishing regulation. The specific arrangements as regards cyber security are defined in eu-LISA Implementing Rules of the Commission Decision 2017/46 on the security of Communication and Information systems in the European Commission and its corresponding security standards, policies, procedures and/or

notifications.

Article 6 - eu-LISA Security Officer

1. The eu-LISA Security Officer shall in particular be responsible for:
    a) developing eu-LISA's security policies and standards, business continuity and disaster management policies, implementing rules or any security procedures and notifications as delegated by the Executive Director;
    b) gathering information in view of assessing threats and risks to security and on all issues which may affect security in eu-LISA;
    c) providing electronic counter-surveillance and protection to all the sites of eu-LISA, taking due account of threat assessments and evidence of unauthorised activities against eu-LISA's interests;
    d) providing a 24-hour/7-day emergency service for eu-LISA services and staff for any work-related safety-/ security-related issues;
    e) implementing security measures aimed at mitigating risks to security and developing and maintaining appropriate CIS to cover its operational needs, particularly in the domains of physical access control, administration of security authorisations, handling of sensitive non-classified and of EU classified information and the protection of personal data;
    f) raising awareness, organising exercises and drills and providing training and advice on all issues related to security in eu-LISA, in view of promoting a security culture and creating a pool of personnel appropriately trained in security matters;
    g) securing the transmission of sensitive non-classified and of EU classified information, including the transmission of personal data.
2. The eu-LISA Security Officer shall, without prejudice to other eu-LISA services' competences and responsibilities, ensure liaison:
    a) with the Commission in accordance with Articles 6, 11, 12, 22 of the Memorandum of Understanding between the European Commission and eu-LISA, in cases of crisis and security incidents management and business continuity, major incidents or of any incident related to the operation of the network which could have an impact on the availability, confidentiality and integrity of data or on the quality or the availability of service to the systems' users and for the purpose of consulting the Commission on draft security measures and any amendment thereto;
    b) with other EU institutions, agencies or bodies in order to ensure that the security risks are identified, assessed, mitigated and monitored;
    c) with security, intelligence and threat assessment services, including national security authorities of the Member States, on issues affecting the security of persons, information systems and other assets in eu-LISA or concerning threats posed by terrorist and espionage activities affecting security in eu-LISA;
    d) with police and other emergency services on all routine and emergency issues affecting eu-LISA's security;
    e) with the relevant security-/business continuity- oriented professional bodies and organisations.

Article 7 - eu-LISA responsibilities regarding the Security Officers Network (SON)

1. eu-LISA, further to the establishment of the Security Officers Network[4], supports its mandate, including the meetings and activities of its members.
2. eu-LISA shall actively support the SON in fulfilling its mandate to provide security advice and expertise to the Management Board and the Advisory Groups, where appropriate, on matters relating to eu-LISA internal security and to the security of any IT System operated by eu-LISA.

Article 8 - System Security Officers (SSOs)

1. For each system managed by eu-LISA, the System Security Officers (SSOs) shall be appointed through an Executive Director Decision. The SSOs shall be temporary agents, contract agents or SNEs working in the Security Unit.
2. SSOs shall be responsible for the following:
   a) Ensuring that the security of the systems is consistent with their respective security plans;
   b) Coordinating the activities of the Information Security Officers (ISOs);
   c) Elaborating on the definition, implementation and verification of the security of the systems for which they are responsible;
   d) With regard to the Corporate IT systems, reporting to the eu-LISA Security Officer on all relevant security matters.

Article 9 - Information Security Officers (ISOs)

1. The Information Security Officers are responsible for the daily operational security matters related to the information systems of eu-LISA, including the following:
   a) Developing the systems' security plans and business continuity plans, and monitoring their performance;
   b) Contributing to the dissemination of the information systems security policy in eu-LISA and preparing and performing the security awareness campaigns;
   c) Ensuring that an inventory of all information systems is kept and updated with a description of the security needs and a grading of the requirements;
   d) Advising and reporting to the SSOs, eu-LISA Security Officer, IT project managers on all the information systems security matters;
   e) Ensuring that the IT service providers put in place the necessary security measures;
   f) Taking part in checks whenever security risks and incidents are identified.
2. ISOs shall be sufficiently available and have the appropriate experience, knowledge and skills in the information systems security in order to fulfil their specific tasks and responsibilities efficiently and effectively.

CHAPTER 4 - DELIVERING SECURITY

Article 10 - Mandated staff

4 Security Officers Network is a workgroup of security specialists representing eu-LISA, European Commission, other EU bodies and EU Member States providing support to eu-LISA Management Board and eu-LISA Advisors Groups regarding security, safety and business continuity related matters concerning the Agency and the large-scale IT systems under its responsibility.

1. Only staff authorised on the basis of a nominative mandate conferred to them by the eu-LISA Executive Director, given their current duties, may be entrusted with the power to take one or several of the following measures:
    a) Carry side arms;
    b) Conduct security inquiries as referred to in Article 18;
    c) Take security measures regarding persons and objects as referred to in Article 17 as specified in the mandate.
2. The mandates referred to in paragraph 1 shall be conferred for a duration that shall not exceed the period during which the person concerned holds the relevant 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 to mandated staff, this Decision constitutes a service instruction within the meaning of Article 21 of the Staff Regulations which applies by analogy to eu-LISA temporary agents and contract agents.[5]

Article 11 - General provisions regarding security measures

1. When taking security measures in the interest of eu-LISA, necessary for the Agency's management and functioning[6], eu-LISA shall in particular ensure so far as reasonably possible, to:
    a) only seek support or assistance from the state concerned, provided that that state either is 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) only transfer information on an individual to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC of the European Parliament and of the Council[7], in accordance with Article 9 of Regulation (EC) No. 45/2001;
    c) where an individual poses a threat to security, any security measure shall be directed according to the law at that individual and that individual may be subjected to bearing the incurring costs. Those security measures may only be directed at other individuals if an immediate or major threat to security must be controlled and the following conditions are fulfilled:
        I. the measures envisaged to prevent the individual from posing the threat to security cannot be taken or are not likely to be effective;
        II. eu-LISA 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 rights.

5 "*An official in charge of any branch of the service shall be responsible to his superiors in respect of the authority conferred on him and for the carrying out of instructions given by him. The responsibility of his subordinates shall in no way release him from his own responsibility.*"

6 Article 5 and Recital 27, Regulation No. 45/2001

7 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

2. The Security Unit of eu-LISA is responsible to establish the processes for assuring proper response to formal requests from the Police, Judges or Prosecutors and 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 eu-LISA premises.
3. The Security Unit may turn to a contractor to carry out specific tasks relating to security under the direction and supervision of its staff.

Article 12 - Security measures regarding persons

1. An appropriate level of protection shall be afforded to persons in the premises of eu-LISA, taking into account security and safety requirements.
2. In case of major risks to security, the Security Unit shall provide close protection to MB and AG members, VIPs and to the staff present in eu-LISA buildings, premises and land used by it, where a threat assessment has indicated that such protection is needed to ensure their safety and security.
3. eu-LISA may decide to apply similar security measures as the ones laid down in paragraph 2 when the MB and AG members, VIPs and staff of the Agency are outside eu-LISA premises but carrying out eu-LISA activities. In such cases, the implementation of the security measures needs to comply with the national legislation of the state where the activities are performed. In all these cases, eu-LISA applies the national legislation of the states concerned.
4. The specific provisions of the seat and site agreements on security of the Agency and assistance and cooperation in security matters by the host Member States shall apply.
5. In case of major risks to security, eu-LISA may order the evacuation of its premises. The emergency action plan shall be adopted for each eu-LISA site through an Executive Director Decision.
6. Victims of accidents or other incidents within eu-LISA premises shall receive assistance.
7. In order to prevent and control risks to security, mandated staff may carry out background checks of persons falling under the scope of these rules on security, so as to determine whether giving the access for such persons to eu-LISA premises, assets or information presents a threat to eu-LISA security. For that purpose, and in compliance with Regulation (EC) No. 45/2001 and provisions referred to under Article 3(1), the mandated staff concerned may:
   a) Use any source of information available to eu-LISA, taking into account the reliability of the source of information;
   b) Access the personnel file or data eu-LISA holds regarding individuals it employs or intends to employ, or for contractors' staff, only when duly justified.

Article 13 - 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 eu-LISA as well as to protect its assets.
3. Physical security shall have the following objectives:
   a) preventing acts of violence directed against any 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 eu-LISA buildings and assets;
   d) ensuring appropriate protection to designated secured areas;

e) preventing, deterring or detecting unauthorised physical access in secured areas or to locations where information systems process sensitive or classified information;
f) enabling investigation and inquiry into security incidents, including through checks on access and exit control log files, CCTV coverage, telephone call/emails recordings and similar data as referred to in Article 23(2) hereunder and other information sources.

4. Physical security shall include:
   a) an access policy applicable to any person or vehicle requiring access to eu-LISA premises, including the parking lots, which shall be adopted through an Executive Director Decision;
   b) access-control and intrusion-detection systems comprising guards, technical equipment and measures, processes, 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 eu-LISA premises of persons, vehicles, goods and equipment;
   b) performing identity controls at its premises;
   c) inspecting vehicles, goods and equipment by visual or technical means;
   d) preventing unauthorised persons, vehicles and goods from entering eu-LISA premises.

Article 14 – Security measures regarding information

1. Security of information covers all information handled by eu-LISA.
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, policies 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 eu-LISA 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 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 (EC) No. 45/2001.
6. Sensitive non-classified information shall be subject to rules 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 an Executive Director Decision. When handled or stored on Communication and Information Systems, such information shall be protected also in compliance with the Decision of the Management Board on the security of Communication and Information systems in eu-LISA and its corresponding security standards.

7. Any individual who is responsible for compromising European Union classified information 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.

Article 15 - Security measures regarding Communication and Information Systems

1. All Corporate Communication and Information Systems ('CIS') used by eu-LISA shall comply with the Decision of the Management Board on the security of Communication and Information systems in eu-LISA and its corresponding security standards.
2. eu-LISA shall only allow European Union institutions, agencies, bodies to have access to its Corporate systems provided that those entities can provide reasonable assurance that their IT systems are protected at a level equivalent to Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of Communication and Information systems in the European Commission and its implementing rules and its corresponding security standards. eu-LISA shall be entitled to refuse access to a European Union institution that does not provide equivalent protection. For the large-scale IT systems under eu-LISA's operational management, the specific security rules foreseen in the legislative instruments governing the large scale IT systems will apply.

Article 16 - Forensic analysis regarding cybersecurity

The Security Unit shall be responsible for conducting forensic technical analysis in cooperation with the competent eu-LISA departments, units and sectors, in consultation with the relevant Commission Departments in support of the evidence-gathering processes and security inquiries referred to in Article 18, especially those related to counter-intelligence, data leakage, cyber-attacks and information systems security. If needed, eu-LISA Security Officer may request technical support from the specialised entities or authorities of the EU Member States and other EU bodies or institutions.

Article 17 – Specific security measures regarding persons and objects

1. In order to ensure the security of the persons, information and assets in eu-LISA, and to prevent and control risks, staff mandated in accordance with Article 10 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 the scenes and the evidence (including access and exit control log files, CCTV images, etc.) 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 eu-LISA's premises, escorting persons from eu-LISA's premises, banning persons from entering eu-LISA's premises for a period of time, the latter defined in accordance with criteria established by an Executive Director Decision;
   c) limited measures concerning objects posing a threat to security, including removal, seizure and disposal of objects;
   d) searching of eu-LISA 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 eu-LISA's rights as a landlord or as an employer in accordance with the applicable national laws.

2. Under exceptional circumstances (including threat to the interest of eu-LISA vital for the Agency's management and functioning), staff members of the Security Unit, mandated in accordance with Article 10, may take any urgent measures needed, in strict compliance with the principles laid down in Article 3. They shall inform as soon as possible the Security Officer of eu-LISA, who shall seek the appropriate mandate from the Executive Director, confirming the measures taken and authorising 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 was based. The documentation can be concise, but should be constituted in such a way to allow the persons subjected to the measure to exercise their rights of defence and of protection of personal data in accordance with Regulation (EC) No. 45/2001, and to allow a 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 1(b), above, eu-LISA shall in addition guarantee that the individual concerned is given the opportunity to contact a lawyer or a person of his confidence and be made aware of their right to have recourse to the European Data Protection Supervisor.

Article 18 - Inquiries

1. Without prejudice to Article 86 and Annex IX of the Staff Regulations, and to the Management Board Decision on administrative inquiries no. 13/2015, security inquiries may be conducted:
   a) In case of incidents affecting security in eu-LISA, including suspected criminal offences;
   b) In case of potential leakage, mishandling or compromise of sensitive non-classified information, or classified information processed by eu-LISA;
   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 eu-LISA Executive Director, who will define the purpose and the scope of the inquiry and the process to be followed.
3. Security inquiries shall be conducted only by dedicated members of staff of the Security Unit duly mandated in accordance with Article 10.
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 17.
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 eu-LISA premises or involving persons referred to in Article 2(3) either as victim or perpetrator of such offences.
6. eu-LISA 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 Executive Director may, where appropriate or required, provide support or ask the Security Unit to provide such support to the authorities of the host Member States or any other Member State concerned.
7. In the case of serious cyber-incidents the Corporate Service Sector and the Operations Department shall collaborate closely with Security Unit in order to provide support on all technical matters. The Security Unit shall decide, in consultation with the Corporate Service Sector and the Operations Department, when it is appropriate to inform the competent authorities of the host countries 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 to support EU institutions and other agencies that may be affected.

8. Security inquiries shall be documented.

Article 19 - Delineation of competences with regard to security inquiries and other types of investigations

1. Where the Security Unit conducts security inquiries, as referred to in Article 18, and if these enquiries fall within the competences of the European Anti-Fraud Office (OLAF) or the Investigation Panel (IP)[8], it shall liaise with those bodies at once with a view, in particular, not to compromise later steps by either OLAF or IP. Where appropriate, the Security Unit shall invite OLAF or IP to be involved in the investigation or shall inform the Executive Director in order to initiate the disciplinary procedures.
2. The security inquiries, as referred to in Article 18, shall be without prejudice to the powers of OLAF and IP as laid down in their governing rules. The Security Unit shall provide upon request technical assistance for inquiries initiated by OLAF or IP.
3. The Security Unit may be asked to assist OLAF's agents when they access eu-LISA 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[9] in order to facilitate their tasks.
4. Without prejudice to Article 22(a) of the Staff Regulations, where a case may fall within the competence of the Security Unit and in the same time might be a failure to comply with the staff obligations, Security Unit shall, when it reports to the Executive Director in compliance with Article 18 at the earliest possible stage advise whether there are grounds that justify notifying IP about 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 Executive Director shall decide on the matter.
5. Where a case may fall within the competence of both the Security Unit and OLAF, Security Unit shall without delay report to the Executive Director who shall 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 20 - Security inspections

1. The Security Unit shall undertake security inspections in order to verify compliance by eu-LISA services and individuals with this Decision and its implementing rules and to formulate recommendations when deemed necessary.
2. Security inspections shall be documented and the results shall be reported to the Executive Director of eu-LISA and the Commission without delay.

8 The Investigation Panel is a collective body in charge of performing specific inquiries to ascertain certain facts or actions, appointed permanently or temporarily for specific inquiries, composed of two or three members chosen from eu-LISA staff or external experts with relevant experience on the subject of the inquiry.

9 Regulation (EU, EURATOM) No 883 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Antifraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (O.J. L 248, 18.9.2013 p. 1).

Article 21 - Alert states and management of crisis situations

1. The Security Unit shall be responsible for putting in place appropriate alert state measures in anticipation of or in response to threats and incidents affecting security in eu-LISA, and for measures required for managing crisis situations including the ones established through the relevant business continuity plans.
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 the Commission, and of the Member State or Member States hosting eu-LISA premises.
3. The Security Unit shall be the contact point for alert states and management of crisis situations and shall inform accordingly the eu-LISA Executive Director when needed.

CHAPTER 5 - IMPLEMENTATION

Article 22 - Implementing rules and security standards, policies, procedures and/or notifications

1. As necessary, the Security Unit shall draft all the Implementing Rules for this Decision and then shall subsequently consult them with the Commission before their submission to the Executive Director, the Advisory Groups and the Management Board.
2. After the adoption of the present Decision and of the implementing rules mentioned in paragraph 1, the Security Unit shall be responsible for drafting the corresponding security standards. These security standards and policies shall be adopted through Executive Director Decisions.
3. The corresponding security procedures and notifications shall be approved by the Executive Director. The Executive Director may delegate the competence of approving these security procedures and notifications to the eu-LISA Security Officer.

CHAPTER 6 - MISCELLANEOUS AND FINAL PROVISIONS

Article 23 - Processing of personal data

1. eu-LISA shall process personal data needed for implementing this Decision in accordance with Regulation (EC) No 45/2001.
2. Notwithstanding the measures already in place at the time of adoption of the present rules and notified to the European Data Protection Supervisor, any measure under these rules 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 22, which shall lay down appropriate safeguards for data subjects.
3. The eu-LISA Security Officer shall be responsible for the security of any processing of personal data undertaken in the context of this Decision.
4. The Implementing Rules mentioned at Article 22 shall be adopted after consultation of the Data Protection Officer and, if required, with the European Data Protection Supervisor in accordance with Regulation (EC) No 45/2001.

Article 24 - Transparency

The present Decision and its implementing rules, security standards, policies, procedures and/or, notifications, shall be brought to the attention of eu-LISA staff under the scope of the *Staff Regulations and of the Conditions of Employment of other servants of the European Union*, of the national experts seconded to eu-LISA (SNEs), of the external service providers and their staff, of interns (trainees) and to any individual with access to eu-LISA buildings or other assets, including the information handled by eu-LISA, who shall apply them immediately after their approval.

Article 25 - Entry into force

The present Decision shall enter into force 30 days following their approval by the Management Board. At the same date, the Agency Security Policy from 30.11.2012 shall be repealed.