2019 - 148

DECISION OF THE MANAGEMENT BOARD ON THE SECURITY RULES ON THE PROTECTION OF COMMUNICATION AND INFORMATION SYSTEMS IN eu-LISA

Final

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- Not for publication.

DECISION OF THE MANAGEMENT BOARD ON THE SECURITY RULES ON THE PROTECTION OF COMMUNICATION AND INFORMATION SYSTEMS IN eu-LISA

The Management Board,

Having regard to Art 15 of the Decision of Management Board on Security Rules in eu-LISA 2016-133 REV 3[1],

Having regard to Commission Decision (EU, Euratom) No 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission[2], Commission Decision of 13 December 2017 laying down implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14, 15 of Decision 2017/46 on the security of communication and information systems in the European Commission[3] and Commission Decision (EU, Euratom) 2018/559 of 6 April 2018 laying down implementing rules for Article 6 of Decision (EU, Euratom) 2017/46 on the security of communication and information systems in the European Commission [4],

Having regard to the Decision No 112/2017 of the Executive Director repealing and replacing the Business Continuity Policy[5],

Having regard to international standards and IT Security good practices including ISO/IEC 27001, 27002, 27005 and 27035,

Whereas:

(1) The Agency's corporate communication and information systems (CISs) are an integral part of the functioning of the Agency and IT security incidents can have a serious impact on the Agency's operations as well as on third parties, including individuals, businesses and Member States.

(2) There are many threats that can harm the confidentiality, integrity or availability of eu-LISA's CISs, and of the information processed therein. These threats include accidents, errors, deliberate attacks and natural events, and need to be recognised as operational risks.

(3) CISs should be provided with a level of protection commensurate with the risks to which they are exposed.

---

[1] Decision of the Management Board No 133 REV 3 of 27 July 2017 on security rules in eu-LISA.
[2] OJ L 6, 11.1.2017, p. 40.
[3] COM (2017) 8841 final.
[4] OJ L 93, 11.4.2018, p. 4.
[5] Decision No 112/2017 of 31.10.2017 of the Executive Director of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice repealing and replacing the Business Continuity Policy approved and adopted by the Management Committee on 07.10.2014.

(4) IT security in eu-LISA should ensure that eu-LISA's CISs protect the information they process and function as they need to, when they need to, under the control of legitimate users.

(5) The IT security policy of eu-LISA should be implemented in a manner which is consistent with the policies on security in eu-LISA.

(6) eu-LISA's approach should take into account EU policy initiatives and legislation on network and information security, industry standards and good practices, to comply with all relevant legislation and to allow interoperability and compatibility.

(7) Appropriate measures should be developed and implemented by eu-LISA departments and units, approved by the Security Unit responsible for communication and information systems, and information technology security measures for protecting communication and information systems should be coordinated across eu-LISA to ensure efficiency and effectiveness.

(8) Rules and procedures for access to information in the context of IT security, including IT security incident handling, should be proportionate to the threat to eu-LISA or its staff and compliant with the principles laid down in 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[6].

(9) The policies and rules for communication and information systems processing EU classified information (EUCI), sensitive non-classified information and unclassified information are to be fully in line with the Decision of the Management Board on the Security Rules for protecting EU Classified Information in eu-LISA No 2019-273 of 20 November 2019[7] and with the Decision of the Management Board on Security Rules on Protecting Sensitive Non-Classified Information in eu-LISA No 2019-208 of 30 August 2019[8],

HAS ADOPTED THIS DECISION:

[6] OJL 295, 21.11.2018, p.39.
[7] Decision of the Management Board 2019-273 of 20 November 2019 on the Security Rules for Protecting EU Classified Information in eu-LISA.
[8] Decision of the Management Board 2019-208 of 30 August 2018 on the Security Rules for Protecting Sensitive Non-classified Information at eu-LISA.

Table of Contents

CHAPTER 1 - GENERAL PROVISIONS

Article 1 - Subject matter and scope

1. This Decision applies to all corporate CISs[9] which are owned, procured, managed or operated by or on behalf of eu-LISA and all usage of those CISs by eu-LISA.

2. This Decision sets out the basic principles, objectives, organisation and responsibilities regarding the security of those CISs and in particular for eu-LISA departments owning, procuring, managing or operating CISs and including CISs provided by an internal IT service provider. When a CIS is provided, owned, managed or operated by an external party on the basis of a bilateral agreement or contract with eu-LISA, the terms of the agreement or contract shall comply with this decision.

3. This Decision applies to all eu-LISA departments and units.

4. Notwithstanding any specific indications concerning particular groups of staff, this decision shall apply to all Agency staff falling under the scope of the Staff Regulations of Officials of the European Union (the 'Staff Regulations') and the Conditions of Employment of Other Servants of the Union (the 'CEOS')[10], to national experts seconded to the Agency ('SNEs')[11], to external service providers and their staff, to interns and to any individual with access to CISs in the scope of this decision.

Article 2 - Definitions

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

Accountable	'Accountable' means to be answerable for actions, decisions and performance.
Agency Security Authority	'Agency Security Authority' refers to the role laid down in Management Board Decision No 2019-273. According to Management Board Decision No 2019-273, the Management Board shall appoint the eu-LISA Executive Director as the eu-LISA Security Authority ('Security Authority').
Business Impact Assessment	'Business Impact Assessment' or 'BIA' means the activity to identify immediate or future impact of losing security (confidentiality, integrity, availability) on the business of the organisation.
CERT-EU	'CERT-EU' is the Computer Emergency Response Team for the EU institutions and agencies. Its mission is to support the European Institutions to protect themselves against intentional and malicious attacks that would hamper the integrity of their IT assets and harm the interests of the EU. The scope of CERT-EU's activities covers prevention, detection, response and recovery.

[9] Art 15 of the Decision of Management Board on Security Rules in eu-LISA 2016-133 REV 3.
[10] Laid down by Council Regulation (EEC, Euratom, ECSC) No 259/68 of 29 February 1968 laying down the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1).
[11] Decision No 2012-025 of the Management Board of the European Agency for the Operational Management of Large Scale IT Systems in the Area of Freedom, Security and Justice of 28 June 2012 on laying down rules on the Secondment of National Experts (SNE) to the Agency.

Communication and information system	'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 infrastructure, organisation, personnel and information resources. This definition includes business applications, shared IT services, outsourced systems, and end-user devices.
Crypto Approval Authority	'Crypto Approval Authority' (CAA) is a function assumed by the eu-LISA Security Authority that falls under the authority of the Executive Director.
Data owner	'Data owner' means the individual responsible for ensuring the protection and use of a specific data set handled by a CIS.
Data set	'Data set' means a set of information which serves a specific business process or activity of the eu-LISA.
Emergency procedure	'Emergency procedure' means a predefined set of methods and responsibilities for responding to urgent situations in order to prevent a major impact on eu-LISA.
Exception	'Exception' means an instance where a decision was taken at appropriate level not to implement a security measure that is based on a rule or on legislation.
External network connection	'External network connection' means any electronic communications connection between the eu-LISA's internal network and any other network, including the Internet. This definition excludes third party networks that are provided under contract to be part of the eu-LISA's internal network.
eu-LISA Security Officer	The eu-LISA Security Officer's responsibilities on security are defined in decision of the Management Board 2016-133 REV 3 and in the Article 6 of the current decision.
Information security policy	'Information security policy' means a set of information security objectives, which are or have to be established, implemented and checked. It comprises, but is not limited to, the decision of the Management Board No 2019-273 and the decision of the Management Board No 2019-208, in line with the parallel provision of Article 2(10) of COM Decision 2017/46.
Information Security Officers	The Information Security Officers (ISO) responsibilities on security are defined in decision of the Management Board 2016-133 REV 3.
IT asset	'IT asset' means a technical asset as part of an IT system.
'IT asset management inventory	'IT asset management inventory' means a repository for information technology installations which holds data relating to the collection of IT assets, as well as descriptive relationships between such assets;
IT security or security of CIS	'IT security' or 'security of CIS' means the preservation of confidentiality, integrity and availability of CISs and the data sets that they process.
IT security guidelines	'IT security guidelines' consist of recommended but voluntary measures that help support IT security standards or serve as a reference when no applicable standard is in place.
IT security incident	'IT security incident' means an event that could adversely affect the confidentiality, integrity or availability of a CIS.

IT security measure	'IT security measure' means a technical or organisational measure aimed at mitigating IT security risks.
IT security need	'IT security need' means a precise and unambiguous definition of the levels of confidentiality, integrity and availability associated with a piece of information or an IT system with a view to determining the level of protection required.
IT security objective	'IT security objective' means a statement of intent to counter specified threats and/or satisfy specified organisational security requirements or assumptions.
Security plan	'security plan' means the documentation of the IT security measures required to meet the IT security needs of a CIS.
IT security policy	'IT security policy' means a set of IT security objectives, which are or have to be established, implemented and checked. It comprises this decision and its implementing rules.
IT security requirement	'IT security requirement' means a formalised IT security need through a predefined process.
IT security risk	'IT security risk' means an effect that an IT security threat might induce on a CIS by exploiting a vulnerability. As such, an IT security risk is characterised by two factors: (1) uncertainty, i.e. the likelihood of an IT security threat to cause an unwanted event; and (2) impact, i.e. the consequences that such an unwanted event may have on a CIS.
IT security standards	'IT security standards' means specific mandatory IT security measures that help enforce and support the IT security policy.
Security and Continuity Strategy	'Security and Continuity Strategy' means a set of projects and activities which are designed to achieve the objectives of the eu-LISA and which have to be established, implemented and checked.
IT security threat	'IT security threat' means a factor that can potentially lead to an unwanted event which may result in harm to a CIS. Such threats may be accidental or deliberate and are characterised by threatening elements, potential targets and attack methods.
IT Security Working Group	The 'IT Security Working Group' means a group representing different business areas that provides guidance and support to the eu-LISA Security Officer.
IT service	'IT service' means the services provided by an IT system or IT Service Provider to support the functionality or operations of a CIS.
IT system	'IT system' means the technical assets of a CIS, that is to say supporting information, hardware, software and/or a network, other digital information handling components or a combination of those, which may be dedicated for one CIS or shared between multiple CISs.
Key escrow	'Key escrow' means a procedure for storing copies of cryptographic keys with one or more separate parties, ensuring the segregation of duties, to enable their recovery in case the operational copy is lost. Keys may be split into two or more parts, each of which is lodged with a different party to ensure that no single party possesses the entire key.

Personal data, processing of personal data, controller and personal data filing system	'Personal data', 'processing of personal data', 'controller' and 'personal data filing system' shall have the same meaning as in Regulation (EU) 2018/1725.
Processing of information	'Processing of information' means all functions of a CIS with respect to data sets, including creation, modification, display, storage, transmission, deletion and archiving of information. Processing of information can be provided by a CIS as a set of functionalities to users and as IT services to other CIS.
Professional secrecy	'Professional secrecy' means the protection of business data information of the kind covered by the obligation of professional secrecy, in particular information about undertakings, their business relations or their cost components as laid down in Article 339 of the TFEU.
RASCI	'RASCI' is an abbreviation for a responsibility assignment based on the following attribution indicators: (a) 'responsible' (R) means having the obligation to act and take decisions to achieve required outcomes; (b) 'accountable' (A) means being answerable for actions, decisions and performance; (c) 'supports' (S) means having the obligation to work with the person responsible to complete the task; (d) 'consulted' (C) means being sought for advice or opinion; (e) 'informed' (I) means being kept up to date with relevant information.
Responsible	'Responsible' means having the obligation to act and take decisions to achieve required outcomes.
Residual risk	'Residual risk' means the risk remaining after risk treatment.
Risk treatment	'Risk treatment' means the process of mitigating risk, which may include risk avoidance, risk reduction, removing the source of the risk, changing the likelihood of risk, changing the consequences of risk, sharing the risk, and retaining the risk;
Security in the eu-LISA	'Security in eu-LISA' means 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.
Segregation of duties	'Segregation of duties' means sharing responsibilities within a key process and dispersing the critical functions of that process to more than one person or department.
Shared IT service	'Shared IT service' means the service a CIS provides to other CISs in the processing of information.
System owner	'System owner' is the individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of a CIS.
System Security Officer	'System Security Officer' (SSO) responsibilities on security are defined in the decision of the Management Board No 2016-133 REV3.

Technical specification	'Technical specification' means the detailed description of a requirement, typically used in the software design process.
User	'User' means any individual who uses functionality provided by a CIS, whether inside or outside eu-LISA.

Article 3 - Principles for IT security in eu-LISA

1. IT security in eu-LISA shall be based on the principles of legality, transparency, proportionality and accountability.

2. IT security issues shall be taken into account from the start of the development and implementation of eu-LISA's CISs. In order to do so, the Security Unit shall be involved for its respective areas of responsibility.

3. Effective IT security shall ensure appropriate levels of:

(a) authenticity: the guarantee that information is genuine and from bona fide sources;

(b) availability: the property of being accessible and usable upon request by an authorised entity;

(c) confidentiality: the property that information is not disclosed to unauthorised individuals, entities or processes;

(d) integrity: the property of safeguarding the accuracy and completeness of assets and information;

(e) non-repudiation: the ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied;

(f) protection of personal data: the provision of appropriate safeguards in regard to personal data in full compliance with Regulation (EU) 2018/1725;

(g) professional secrecy: the protection of information of the kind covered by the obligation of professional secrecy, in particular information about undertakings, their business relations or their cost components as laid down in Article 339 of the TFEU.

4. IT security shall be based on a risk management process. This process shall aim at determining the levels of IT security risks and defining security measures to reduce such risks to an appropriate level and at a proportionate cost. The risks and security measures shall be documented in a security plan for each CIS.

5. All CISs shall be identified, assigned to a system owner and recorded in an inventory.

6. The security requirements of all CISs shall be determined on the basis of their security needs and of the security needs of the information they process. CIS that provide services to other CIS may be designed to support specified levels of security needs.

7. The security plans and IT security measures shall be proportionate to the security needs of the CIS.

CHAPTER 2 - ORGANISATION AND RESPONSIBILITIES

Article 4- Management Board

The Management Board responsibilities on security are defined in Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011[12].

Article 5- Executive Director

The Executive Director responsibilities on security, in accordance with Regulation (EU) 2018/1726, shall be the following:

1. Be appointed as the eu-LISA Security Authority by the Management Board in accordance with Article 7 of decision of the Management Board No 2019-273; his/her specific tasks as Security Authority are defined in that decision.

2. Hold ultimate accountability for IT security, including the overall responsibility for the governance of IT security as a whole in eu-LISA, and in particular the responsibility of the system owner and data owner, with the right to delegate certain of these responsibilities in accordance with paragraph 3.

3. Has the right to:

a) formally delegate certain responsibilities of the system owner for each CIS to a staff member who shall be responsible for ensuring the IT security of that CIS and

b) formally delegate certain responsibilities of the data owner for each data set handled in a CIS to a staff member, who shall be responsible for ensuring the confidentiality, integrity and availability of the data set.

4. Resolve any disagreements between those entities/staff of eu-LISA to whom he has delegated certain responsibilities of data owner and system owner.

Article 6 - eu-LISA Security Officer

Without prejudice to the responsibilities of the eu-LISA Security Officer as defined in Article 6 of the decision of the Management Board 2016-133 REV 3, he/she shall have the following responsibilities:

1. Support the Executive Director in its IT-security-related tasks.

2. Take the responsibility for the operational governance of IT security as a whole within the eu-LISA.

3. Develop eu-LISA's IT security policy for adoption by the Management Board.

4. Review and report annually to Executive Director and to the Management Board on governance matters, including the continual improvement process of the security

[12] OJ L 295, 21.11.2018, p.99.

management system of the Agency, as well as on IT-security-related issues, including serious information security incidents.

5. Monitor and review the overall implementation of and compliance with this decision and report on it to the Executive Director and to the Management Board.

6. Propose to the Executive Director for review, approval and monitoring the implementation of the rolling Security and Continuity Strategy. The eu-LISA Security Officer shall report on it to the Executive Director and to the Management Board.

7. Monitor, evaluate and control the eu-LISA's information risk treatment landscape and shall have the power to issue formal requirements for improvements wherever necessary.

8. Inform the Executive Director and the Management Board on specific IT security threats, incidents and exceptions to the eu-LISA IT security policy notified by the system owners, which could have a significant impact on the security in eu-LISA.

Article 7 – IT Security Working Group

1. The IT Security Working Group shall be chaired by the eu-LISA Security Officer. Its members shall include representatives of the Security Unit, the Operations Department, the Corporate Services Department, and representatives of other eu-LISA Units, Sectors or entities involved, where information security is a major concern for their operations.

2. The IT Security Working Group shall provide support and guidance to the eu-LISA Security Officer on business related matters, organisation's mission, strategy, goals and risk appetite.

3. The eu-LISA Security Officer will inform the IT Security Working Group on security related matters.

4. The IT Security Working Group shall facilitate the exchange of early warning and threat information.

Article 8 - Security Unit

In relation to IT security, the Security Unit shall have the following responsibilities:

1. Assure alignment between the IT Security Policy and the eu-LISA Information Security Policy;

2. Establish a framework for the authorisation of the use of encrypting technologies for the storage and communication by CISs;

3. Request authorisation from the eu-LISA Security Officer for any CIS that uses encrypting technology.

4. Ensure that back-ups of any decryption keys are stored in an escrow account. The recovery of encrypted data shall be carried out only when authorised in accordance with the framework defined by the Security Unit.

5. Inform the Executive Director and eu-LISA Security Officer about specific threats which could have a significant impact on the security of CISs and the data sets that they process.

6. Perform IT security inspections, information security inspections, technical vulnerability assessments and penetration tests to assess the compliance of eu-LISA's CISs with the security policy and report the results to the Executive Director, the eu-LISA Security Officer,

the Heads of departments/units and the system owners.

7. Establish a framework for the authorisation of access and the associated appropriate security rules to eu-LISA CISs from external networks and develop the related security standards and guidelines as delegated by the eu-LISA Security Officer.

8. Propose principles and rules for the outsourcing of CISs in order to maintain appropriate control of security of the information.

9. Develop the information security risk management methods and processes for all eu-LISA departments and assess and report on information security risks management outcomes regularly to the eu-LISA Security Officer and to the Executive Director.

10. Propose a rolling Security and Continuity Strategy, as delegated by the eu-LISA Security Officer, for revision and approval by the Executive Director and adoption by the Management Board and propose a programme, including the planning of projects and activities implementing the Strategy.

11. Monitor the execution of the eu-LISA Security and Continuity Strategy and report on this regularly to the eu-LISA Security Officer and to the Executive Director.

12. Monitor the IT security risks and IT security measures implemented in CISs and report on them regularly to the eu-LISA Security Officer and to the Executive Director.

13. Request system owners to take specific IT security measures in order to mitigate IT security risks to eu-LISA CISs.

14. Ensure that there is an adequate catalogue of eu-LISA's IT security services available for the system owners and data owners to fulfil their responsibilities for IT security and to comply with the IT security policy and standards.

15. Provide adequate documentation to system and data owners and consult with them, as appropriate, on the IT security measures implemented for their IT services in order to facilitate compliance with the IT security policy and perform IT risk management with the support of the systems owners.

16. Define the training needs and coordinate training programmes on IT security in cooperation with the eu-LISA departments and units, and develop, implement and coordinate awareness-raising campaigns on IT security as delegated by the eu-LISA Security Officer.

17. Ensure that system owners, data owners, users and other roles with IT security responsibilities in eu-LISA departments and units are made aware of the IT security policy.

18. Inform the eu-LISA Security Officer and the Executive Director on specific IT security threats, incidents and exceptions to the eu-LISA's IT security policy notified by the system owners which could have a significant impact on security in the eu-LISA.

19. Support the eu-LISA Security Officer in developing information security policies, rules, standards and guidelines and any implementing rules in accordance with Article 31 for the adoption by the Executive Director.

20. Report regularly on the overall implementation and compliance with this decision to the eu-LISA Security Officer and Executive Director.

21. Assess information security risks and determine the information security requirements for each CIS, in collaboration with the data controllers and the system owners.

22. Support the development of security plans for the corporate CIS, including, where appropriate, details of the assessed risks and any additional security measures required in collaboration with the data controller and the system owner to be submitted to the Executive Director.

23. Inform the relevant eu-LISA departments and units on specific information security threats, incidents and exceptions to the information security policy notified by the system owners that could have a significant impact on security in eu-LISA.

24. Establish a framework for the management of business continuity in relation to CISs and develop the related information security standards and guidelines as delegated by the eu-LISA Security Officer in close cooperation with the eu-LISA Departments and Units.

25. Establish, implement, maintain and continually improve an information security management system (ISMS) to ensure the confidentiality, integrity and availability of information.

Article 9 – eu-LISA Departments and Units

In relation to IT security in their Department / Unit, each Head of Department or Unit shall:

1. Ensure that appropriate IT security risk assessment and security plans have been made and implemented;

2. Ensure that the implementation of the required IT security measures is reported on a regular basis to the Security Unit, eu-LISA Security Officer and the Executive Director;

3. Ensure that appropriate processes, procedures and solutions are in place to ensure efficient detection, reporting and resolution of IT security incidents relating to their CISs;

4. Own the risks relating to their CIS and data sets;

5. Ensure that the security plans and IT security measures are implemented and the risks are adequately covered.

6. Ensure that the staff members under their responsibility comply with the IT security policy and the related standards and guidelines.

Article 10 - System owners

1. The system owner is responsible for ensuring the compliance with the provisions of the current decision and ensuring the IT security of the CIS under his or her responsibility and reports to the eu-LISA Security Officer and the Executive Director.

2. The system owner is the individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of a CIS.

3. In relation to IT security, the system owner, with the support of Security Unit, shall:

(a) ensure the compliance of the CIS with the IT security policy;

(b) ensure that the CIS is accurately recorded in the relevant inventory;

(c) support the IT risk management process and determine the IT security needs for each CIS, in collaboration with the data owners and the Security Unit;

(d) implement appropriate IT security measures, proportionate to the information security risks identified and follow recommendations endorsed by the Security Unit;

(e) identify any dependencies on other CISs or shared IT services and implement security measures as appropriate based on the security levels proposed by those CISs or shared IT services;

(f) manage and monitor IT security risks;

(g) report regularly to the Executive Director on the IT security risk profile of their CIS and report to the Security Unit on the related risks, risk management activities and security risks taken;

(h) consult eu-LISA Security Officer and Security Unit on aspects of IT security;

(i) issue instructions for users on the use of the CIS and associated data as well as the responsibilities of users related to CIS;

(j) request authorisation from the eu-LISA Crypto Authority for any CIS that uses encrypting technology;

(k) consult the eu-LISA Security Authority in advance concerning any system processing classified information;

(l) respect any instructions from the relevant Data Controller(s) concerning the protection of personal data and the application of data protection rules on security of the processing;

(m) notify the Security Unit of any exceptions requests to the information security policy including relevant justifications;

(n) report any unresolvable disagreements between the data owner and the system owner to the Executive Director;

(o) communicate IT security incidents to the relevant stakeholders in a timely manner as appropriate according to their severity, in accordance with Article 22;

(p) for outsourced systems, ensure that appropriate IT security provisions are included in the outsourcing contracts and that information security incidents occurring in the outsourced CIS are reported in accordance with Article 22.

Article 11 - Data owners

1. The data owner is responsible for the IT security of a specific data set and is accountable for the confidentiality, integrity and availability of the data set.

2. In relation to this data set, the data owner shall:

(a) ensure that all data sets under his or her responsibility are appropriately classified in accordance with the decision of the Management Board No 2019-273 and the decision of the Management Board No 2019-208;

(b) define the information security needs and inform the relevant system owner and the Security Unit of those needs;

(c) participate in the CIS risk assessment;

(d) report any unresolvable disagreements between the data owner and the system owner to the Executive Director;

(e) communicate IT security incidents as provided for in Article 22.

3. Data owners may formally delegate some or all of their IT security tasks but they maintain their responsibilities as defined in this Article.

Article 12 - System Managers

The System Manager manages and/or operates the IT system on behalf of the System Owner and ensures proper access management, backup, logging, monitoring, patch management, identity and access management and change management.

Article 13 - System Security Officers (SSOs)

The System Security Officers responsibilities on security are defined in the decision of the Management Board 2016-133 REV 3[13].

Article 14 - Information Security Officers (ISOs)

The Information Security Officers responsibilities on security are defined in the decision of the Management Board 2016-133 REV 3[14].

Article 15 - Users

1. In relation to IT security, users shall:
   a) comply with the IT security policy and the instructions issued by the system owner on the use of each CIS;
   b) communicate IT security incidents as provided for in Article 22.

2. Use of the eu-LISA CIS in breach of the IT security policy or instructions issued by the system owner may give rise to disciplinary proceedings.

CHAPTER 3 – SECURITY REQUIREMENTS AND OBLIGATIONS

Article 16 - Implementation of this Decision

1. The adoption of all implementing rules, standards, guidelines, security notices and best practices shall be done by the Executive Director according to the Article 31.

2. The eu-LISA Security Officer shall develop all implementing rules, standards, guidelines, security notices and best practices mentioned under paragraph 1 , with the support of the Security Unit and, when necessary, after the consultation of the IT Security Working Group.

[13] Decision of the Management Board on security rules in eu-LISA (2016-133 REV 3, Article 8, p. 9)
[14] Decision of the Management Board on security rules in eu-LISA (2016-133 REV 3, Article 9, p. 9)

Article 17 - Obligation to comply

1. Compliance with the provisions outlined in the IT security policy and standards is mandatory.

2. Non-compliance with the IT security policy and standards may trigger liability to disciplinary action in accordance with the Treaties, the Staff Regulations and the CEOS, to contractual sanctions and/or to legal action under national laws and regulations.

3. The Security Unit shall be notified of any exceptions to the IT security policy.

4. In the event the eu-LISA Security Officer decides there is a persistent unacceptable risk to a CIS of the eu-LISA, the Security Unit in cooperation with the system owner shall propose mitigating measures to the eu-LISA Security Officer for approval. These measures may, amongst others, include reinforced monitoring and reporting, service limitations and disconnection. The Executive Director shall be informed of the adoption of such measures.

5. The eu-LISA Security Officer shall impose the implementation of approved mitigating measures wherever necessary. The eu-LISA Security Officer may also recommend to the Security Unit to open an administrative enquiry. The Security Unit shall report to the eu-LISA Security Officer on every situation when mitigating measures are imposed. The Executive Director shall be informed of the adoption of any measure.

Article 18 - IT security incident handling

1. The Security Unit is responsible for providing the principal operational IT security incident response capability within eu-LISA.

2. The Security Unit as contributing stakeholders to the IT security incident response shall:

(a) have the right to access summary information for all incident records and full records upon request;

(b) participate in IT security incidents crisis management groups and IT security emergency procedures;

(c) be in charge of relations with law enforcement and intelligence services;

(d) perform forensic analysis regarding cyber-security in accordance with Article 16 of the decision of the Management Board on security rules in eu-LISA 2016-133 REV3;

(e) decide on the need to launch an inquiry according to the Article 18 of the decision of the Management Board on security rules in eu-LISA 2016-133 REV3;

(f) inform the eu-LISA Security Officer and the relevant Head of eu-LISA Departments or Units as well as relevant System Owners of any IT security incidents that may present a risk to other CISs;

(g) inform the eu-LISA Data Protection Officer for any IT security incident that lead to a data breach.

3. Regular communications shall take place between the Security Unit, Head of eu-LISA Departments or Units and the eu-LISA Security Officer to exchange information and coordinate the handling of security incidents.

4. The incident coordination services of Computer Emergency Response Team for the European institutions, bodies and agencies ('CERT-EU') may be used to support the incident

handling process when appropriate and for knowledge sharing with other EU institutions and agencies that may be affected.

5. System owners involved in an IT security incident shall:

(a) immediately notify their Head of Departments or Units, the eu-LISA Security Officer, and the Security Unit and, where appropriate, the data owner of any major IT security incidents, in particular those involving a breach of data confidentiality;

(b) cooperate and follow the instructions of the relevant eu-LISA authorities on incident communication, response and remediation.

6. Users shall report all actual or suspected IT security incidents to the Security Unit in a timely manner.

7. Data owners shall report all actual or suspected IT security incidents to the relevant IT security incident response team in a timely manner.

8. The Security Unit, with support from the other contributing stakeholders, is responsible for handling any IT security incident detected in relation to eu-LISA CISs that are not outsourced systems.

9. The Security Unit shall inform affected eu-LISA Departments or Units about IT security incidents and, where appropriate, the CERT-EU on a need-to-know basis.

10. The eu-LISA Security Officer shall regularly report on major IT security incidents affecting the eu-LISA's CIS to the Executive Director.

11. The Security Unit shall have access to IT security incident records concerning the CIS of the eu-LISA Department or Units.

12. In case of a major IT security incident, the eu-LISA Security Officer shall be the contact point for the management of the crisis situations by coordinating the crisis management groups.

13. In case of an emergency eu-LISA can decide to launch an IT security emergency procedure. The eu-LISA Security Officer shall develop emergency procedures to be approved by the Executive Director.

14. The Security Unit shall report on the execution of emergency procedures to the eu-LISA Security Officer and the Heads of eu-LISA Departments or Units affected.

CHAPTER 4 – IT SECURITY PROCESSES

Article 19 - IT security governance

1. The governance of IT security is the process of establishing and maintaining a framework to support management structure and processes to provide assurance that IT security strategies are aligned with and support eu-LISA's objectives. The effective governance of IT security ensures that the Executive Director receives relevant reporting - framed in a business context - about IT security-related activities. This enables pertinent and timely decisions about IT security issues in support of the strategic objectives of eu-LISA.

2. The processes related to governance of IT security shall be carried out through the following:

(a) 'evaluate': the governance process that considers the current and planned achievement of security objectives based on current processes and planned changes, and determines where any adjustments are required to optimise the achievement of strategic objectives in the future;

(b) 'direct': the governance process by which the Executive Director gives direction about the IT security objectives and strategy that needs to be implemented; direction may include changes in prioritisation of activities, and endorsement of policies, material risk acceptance and the security plans;

(c) 'monitor': the governance process that enables the Executive Director and the Management Board to assess the achievements of strategic objectives;

(d) 'communicate': the bidirectional governance process by which the Executive Director and stakeholders exchange information about IT security, appropriate to their specific needs;

(e) 'assure': the governance process by which the Executive Director commissions independent and objective audits, reviews or certifications which shall identify and validate the objectives and actions related to carrying out governance activities and conducting operations in order to attain the desired level of information security.

3. The roles relating to IT security governance shall be defined in accordance with the RASCI model as follows:

(a) the Executive Director is responsible for IT security governance and ensures that the necessary IT security governance processes are performed;

(b) the eu-LISA Security Officer and Security Unit are responsible for the implementation of the IT security governance processes;

(c) the Security Unit shall support the eu-LISA Security Officer in the implementation of its responsibilities, additionally the Security Unit has responsibilities related to the governance process in relation to Article 8;

(d) the eu-LISA Departments and Units shall support the eu-LISA Security Officer and the Security Unit in performing their IT security governance responsibilities and shall be consulted where appropriate;

(e) The eu-LISA Departments and Units shall be kept informed.

4. The main activities related to the process of IT security governance shall be the following:

(a) the Security Unit shall develop and maintain the overall eu-LISA's Security and Continuity Strategy with long term objectives, including activities to be performed in the years ahead. These activities shall support eu-LISA's priorities, be prioritised on the basis of past performance reviews, audits and incidents and receive sufficient investment and resources;

(b) the Security Unit shall, in close cooperation with the IT Security Working Group, support the IT Security Policy, and develop and maintain standards and guidelines aligned with Annex A of the ISO 27001 standard and other corporate frameworks of eu-LISA, as delegated by the eu-LISA Security Officer. The IT security policy shall be adopted by eu-LISA based on a recommendation from the eu-LISA Security Officer;

(c) the Security Unit shall provide advice and support on the implementation of the IT security policy, as well as on standards and guidelines and offer methodologies, templates and tools;

(d) the eu-LISA Security Officer shall respond to the effectiveness and efficiency issues of IT security controls and initiate required actions when the residual risk level is deemed too high;

(e) the eu-LISA Security Officer shall monitor the Security and Continuity Strategy effectiveness, key performance indicators on preventive and reactive measures, the risk landscape, compliance with security policies and significant incidents on a quarterly basis and shall report annually on these topics to the Executive Directory and the Management Board for their review;

(f) the Security Unit shall report to the eu-LISA Security Officer on a quarterly basis on the progress of the implementation and the effectiveness of preventive, detective and corrective IT security measures, as well as on significant IT security threats, exceptions to the security policies, incidents, risks and strategy implementation. On an annual basis, the IT security report shall summarise the threats, IT security incidents, preventive, detective and corrective measures relevant for the previous year, draw conclusions and highlight the future outlook on IT security;

(g) the Security Unit shall review the IT security policy, standards and guidelines whenever there are significant changes in the organisational or technical environment, in the legal conditions or when new or changing threats are identified. It may recommend changes to the eu-LISA Security Officer;

(h) the Security Unit shall monitor the implementation of the IT security policies, standards and guidelines to ensure ongoing compliance. It shall issue annual security evaluation forms or questionnaires on chosen topics of interest that shall be used to update the Security and Continuity strategy and IT security policy on those topics;

(i) the eu-LISA Departments and Units shall respond to annual security questionnaires and evaluation forms issued by the Security Unit;

(j) the Security Unit shall monitor relevant internal or external trends or developments including threats, vulnerabilities, security techniques or products, insofar as they have an impact on eu-LISA's IT security policy or Security and Continuity Strategy;

(k) the eu-LISA Security Officer shall evaluate the residual risk levels related to eu-LISA's CIS as reported by the Security Unit. The eu-LISA Security Officer may issue formal recommendations to Heads of eu-LISA Departments and Units in case of persistent failure to properly treat risks and enforce appropriate measures. Those requests shall include targets for residual risk levels and a timeline for remediation.

Article 20 - IT security risk management

1. The IT security risk management process shall identify, assess and implement a set of cost-effective security measures for an IT system to reduce risks to an acceptable level. The process shall be applied to all IT systems.

2. The IT security risk management process shall consist of the following phases:

(a) 'context establishment': the external and internal context for IT security risk management is established; it involves setting the basic criteria necessary for information security risk

management, defining the scope and boundaries, and establishing an appropriate organisation operating the IT security risk management;

(b) 'risk assessment': risks are identified, quantitatively or qualitatively described, and prioritised against risk evaluation criteria and objectives relevant to the organisation;

(c) 'risk treatment': controls to reduce, retain, avoid, or share the risks are selected and a risk treatment is defined in the security plan;

(d) 'risk acceptance': the decision to accept the risk and the responsibility for the decision are made and are formally recorded;

(e) 'risk monitoring and review': risks and their factors, including values of assets, impact, threats and the likelihood of their occurrence are monitored and reviewed to identify any changes in the context of the organisation at an early stage, and to maintain an overview of the complete risk picture;

(f) 'risk communication': information about risks is exchanged between decision-makers and other stakeholders.

3. The roles relating to IT security risk management shall be the following, in accordance with the RASCI model:

(a) the Executive Director shall be accountable for IT security risk management;

(b) the Security Unit shall be responsible for IT security risk management, but may delegate certain responsibilities;

(c) the System Security Officer shall take delegated responsibility for the activities in the IT risk management process;

(d) the Data Owner shall provide support and be consulted;

(e) the eu-LISA Departments and Units shall be kept informed;

(f) the System Suppliers support the Security Unit to perform the IT security risk management process.

4. The main activities related to the process of IT security risk management shall be the following:

(a) as part of the IT risk assessment, the System Security Officer, shall perform, in collaboration with the relevant stakeholders, in particular the Data Owner and the System Owner, a business impact assessment to identify the IT security needs based on the required levels of confidentiality, integrity and availability of the IT system. Security measures shall be selected to mitigate identified risks, be aligned with the business needs of the IT system and comply with rules and legislation;

(b) the System Security Officer shall draw up security plans that shall contain the key output of the IT risk management process, in particular, the IT security needs, IT security measures and selection rationale, residual risks, risk acceptance criteria and exceptions with a timespan of their validity;

(c) the Executive Director shall formally adopt the security plans and residual risks within the scope of this decision, supported by the Security Unit and the Security Officer as appropriate;

(d) the Security Unit shall monitor at least once a year the IT security needs and risk assessments' results, the residual risks, exceptions and the identified acceptable levels of

risks, taking into account changes to the organisation, technology, business objectives and processes, identified threats, effectiveness of the implemented security measures and external events, such as changes to the legal, contractual or regulatory environment or changes in eu-LISA's IT security policy. The results will be subject to management review and the security plans shall be updated as necessary;

e) The System Owner shall report on the implementation of the IT risk management process to the Security Unit in order to enable the Security Unit to assess the IT risk management methods and identify potential improvements;

(f) The Security Unit shall provide guidance and coaching on the implementation of the security plans to facilitate compliance with the IT security policy and standards and support the System Owners in managing IT security risks;

(g) The Security Unit shall monitor eu-LISA-wide IT security risks and IT security measures implementation and report to the eu-LISA Security Officer on a quarterly basis and System Owners shall communicate the information required for the Security Unit to report to the eu-LISA Security Officer in a timely manner.

Article 21 - Secure IT operations

1. Secure IT operations management shall comprise planning and sustaining the day-to-day processes for maintaining the security of eu-LISA's IT environments.

2. The roles relating to secure IT operations shall be the following, in accordance with the RASCI model:

(a) the Executive Director shall be accountable for secure IT operations;

(b) the System Owner shall be responsible for secure IT operations, but may delegate responsibilities to the System Manager and the IT Service Provider;

(c) the System Manager and IT Service Provider, if the appropriate powers are delegated to them by the System Owner, shall take delegated responsibility for the activities in the secure IT operations management process;

(d) the Security Unit shall be consulted and the eu-LISA Departments or Units shall be kept informed about it.

3. The main activities related to the secure IT operations management process shall be the following:

(a) the System Owner shall identify responsibilities and priorities for managing the operation and continuous improvement of security measures, taking into account the business impact of their system, and eu-LISA Department's budget and priorities;

(b) the System Manager and the IT Service Provider, if the appropriate powers are delegated to them by the System Owner, shall implement the operational IT security measures identified for the IT system in the security plan, and in particular perform and test backups according to agreed schedules, system monitoring and logging as well as vulnerability and patch management;

(c) the System Manager, if the appropriate powers are delegated to him by the System Owner, may request an exception to the planned measures if approved by the System Owner

and the eu-LISA Security Officer and if the related residual risk is formally accepted by the Executive Director; this shall be documented in the security plan;

(d) the Executive Director shall formally approve the implementation of the security plan before the IT system is taken into production based on predefined acceptance criteria;

(e) the System Manager, if the appropriate powers are delegated to him by the System Owner, shall:

(i) manage the operation of the IT system on behalf of the System Owner. The System Manager, if the appropriate powers are delegated to him by the System Owner, may manage the specific IT security measures directly, or subcontract the management to an IT Service Provider; in the latter case, the System Manager shall conclude a formal agreement with the IT Service Provider to ensure that the security measures for which they are responsible are implemented;

(ii) ensure IT asset registration is done and kept up to date in the relevant IT asset management inventory;

(iii) maintain a register of user access rights including approvals, enforce and monitor access control mechanisms and review access periodically, in particular privileged access;

(iv) ensure that logging and monitoring solutions are in place and relevant security logs and alerts are shared with the Security Unit if requested.

Article 22 - IT security incident management

1. IT security incident management shall aim at minimising the direct negative impact of IT security incidents by detecting, stopping and containing, eradicating, analysing and reporting, and following them up; to that effect related artefacts and evidence are collected and handled.

2. The IT security incident management process shall be aligned with the regular incident management process and shall be detailed in implementing rules adopted in accordance with Article 31.

3. The roles relating to IT security incident management shall be the following, in accordance with the RASCI model:

(a) the Executive Director shall be accountable for IT security incident management;

(b) the Security Unit shall be responsible for IT security incident management;

(c) the System Owner shall support the Security Unit;

(d) the System Manager shall support the Security Unit;

(e) the eu-LISA Security Officer and the eu-LISA Departments and Units shall be kept informed;

(f) the Security Unit shall be informed and shall be responsible and accountable for forensic analysis regarding cyber security and relations with law enforcement and intelligence services as provided in Article 18 of the current decision. The System Manager and the IT Service Providers shall support the Security Unit in these activities.

4. The main activities related to the IT security incident management process shall be the following:

(a) the System Owner shall provide information and support to handle IT security incidents;

(b) in the context of security incidents, the Security Unit shall take the lead in the handling of all incidents for those IT systems that are not outsourced;

(c) all access to information in IT systems for the purposes of IT security incident management shall be proportionate to the severity of the IT security incident concerned and compliant with the principles laid down in Regulation (EU) 2018/1725 and with the principle of professional secrecy;

(d) all personnel involved in the IT security incident management process shall receive prior and adequate training in the relevant procedures;

(e) the Security Unit may access, acquire and process relevant information held in IT systems when necessary for the IT security incident management process in accordance with Regulation 1725/2018 and the following:

(i) for sensitive non-classified information, explicit prior approval shall be obtained from the Executive Director;

(ii) for access to user information or eu-LISA information stored on end user devices, such as e-mails or documents, prior approval shall be obtained from end users on a case-by-case basis;

(iii) for access to other information, including system log files, operating system files, system configuration information and potentially suspicious executable file, approval shall not be required.

(f) the Security Unit shall lay down detailed procedures for IT security incident management that shall provide for a transparent audit trail, appropriate management supervision and security measures to ensure the confidentiality of any information acquired during and after the handling of IT security incidents. The audit trail shall be available for consultation by the Executive Director;

(g) information that is accessed, acquired or processed during an IT security incident response shall not be used for any other purpose and shall not be shared with any other party without authorisation from the Data Owner, except the eu-LISA Security Officer, the Executive Director and OLAF;

(h) the Information Security Officer, Systems Security Officer, System Owner, System Manager, the Data Owner and the Data Protection Officer shall support the incident management process.

Article 23 - Secure IT system development and acquisition

1. IT security shall be sufficiently considered in the development or acquisition of all IT systems and shall be built into every phase of the IT System Development Lifecycle, including system conception, design and development, build and construction, testing, deployment, ongoing maintenance and distribution.2. The roles relating to secure IT system development and acquisition shall be the following, in accordance with the RASCI model:

(a) the Executive Director shall be accountable for secure IT system development;

(b) the System Owner shall be responsible for secure IT system development, but may delegate responsibilities to the System Manager and the System Supplier;

(c) the Security Unit shall support the System Owner;

(d) the eu-LISA Departments and Units shall be kept informed.

2. The main activities related to the secure IT system development and acquisition process shall be the following:

(a) the System Owner with the support of the Security Unit shall bear responsibility for the specification of IT security requirements;

(b) the Project Manager, if the appropriate powers are delegated to him by the System Owner, shall ensure the specification of the IT security requirements on the basis of the IT security needs as identified in the business impact assessment and shall apply the security measures based on eu-LISA's standards and other applicable regulations and legislation;

(c) The Executive Director shall approve the IT security requirements as part of the security plan approval;

(d) the Project Manager, if the appropriate powers are delegated to him by the System Owner, shall:

(i) ensure that the security measures are implemented in the IT system or in the infrastructures that support it, whether local or centralised;

(ii) ensure that the design, installation and implementation of the system are in accordance with the IT security requirements of the IT system and the IT security standards;

(iii) bear responsibility for the deployment and hand-over of the IT system to the System Owner;

(iv) with the support of the Security Unit, evaluate the cost of the required IT security measures and may request not to implement measures if approved by the System Owner and if the related residual risk is formally accepted by the Executive Director; these expectations shall be documented in the security plan.

(e) the System Supplier, if the appropriate powers are delegated to him by the System Owner, shall provide operating manuals and instructions for the System Manager;

(f) the Security Unit shall provide recommended tools and services to help development teams to identify and assess source code vulnerabilities in the earliest stages of the development life cycle;

(g) the Security Unit shall provide secure development guidelines, including fundamental practices to support developers in their day-to-day work with the aim of avoiding security weaknesses in the early stages of the system's development;

(h) when an IT system is acquired from a third party (Commercial Off-The-Shelf), the functionality and security of the system shall be assessed against the IT security requirements and the System Supplier, if the appropriate powers are delegated to him by the System Owner, shall provide assurance on the quality of the development process;

(i) when an IT system is developed for eu-LISA, the following activities shall be performed:

(i) the System Supplier, if the appropriate powers are delegated to him by the System Owner, shall define the technical architecture and draw up technical specifications for the implementation of the IT security requirements as defined by the Project Manager, if the appropriate powers are delegated to him by the System Owner;

(ii) the System Security Officer shall support the specification of IT security requirements, the definition of IT security architecture, and the implementation and verification of security measures during the IT project;

(iii) the System Supplier, if the appropriate powers are delegated to him by the System Owner, shall construct and ensure the development of the IT system in accordance with the IT security requirements;

(iv) the Project Manager, if the appropriate powers are delegated to him by the System Owner, shall ensure that a secure system development lifecycle is applied and that the necessary IT Security clauses are included in contracts with external parties;

(v) the System Supplier, if the appropriate powers are delegated to him by the System Owner, shall ensure good quality by performing code reviews and security tests of applications prior to their deployment in production.

Article 24 - IT security training, awareness and communication

1. IT security is as much a human issue, as it is a technology issue. IT security training, awareness and communication shall:

(a) determine the necessary competences of individuals working within their remit that affects the IT security performance of eu-LISA;

(b) ensure that these individuals are competent on the basis of appropriate education, training, or experience;

(c) take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken, where applicable;

(d) retain appropriate documented information as evidence of competence;

(e) ensure awareness of:

(i) the IT security policy;

(ii) these individuals contribution to the effectiveness of improvements in IT security performance;

(iii) the implications of not conforming to the IT security policy.

(f) communicate appropriately and in a timely manner, both internally and externally with relevant stakeholders and target groups, using suitable content and defined processes, communication channels and spokespersons.

2. The roles relating to IT security training, awareness and communication shall be the following, in accordance with the RASCI model:

(a) the eu-LISA Departments or Units shall be accountable for IT security training, awareness and communication;

(b) the Security Unit shall be responsible for performing the activities in this process as delegated by the eu-LISA Security Officer in accordance with Decision of Management Board 2016-133 REV 3;

(c) the eu-LISA Security Officer shall be kept informed of the process.

3. The main activities related to the IT security training, awareness and communication process shall be the following:

(a) the Security Unit shall define the training needs and coordinate training programmes on IT security in cooperation with the Human Resources Unit;

(b) the Security Unit shall organise IT security trainings both online and offline in cooperation with the Human Resources Unit;

(c) the Security Unit shall coordinate awareness-raising activities on IT security in close cooperation with the Human Resources Unit, targeting different audiences such as management, IT professionals and users within eu-LISA;

(d) the Security Unit shall coordinate communication to ensure that System Owners, Data Owners and other roles with IT security responsibilities in eu-LISA Departments or Units are made aware of the IT security policy, standards and guidelines and shall maintain a corporate website dedicated to IT security;

(e) the eu-LISA Departments shall organise specific awareness-raising or training activities for all personnel, in collaboration with Human Resources Unit and the Security Unit and they shall ensure alignment between local IT security information and corporate IT security information;

(f) the eu-LISA Departments shall ensure and monitor that the System Owner, Data Owner, System Manager and Project Manager have a sufficient level of IT security awareness and training to perform their assigned duties;

(g) the eu-LISA Departments or Units shall ensure that users take at least one training session or follow one awareness activity on IT security every year and that all new staff take IT security induction training when joining eu-LISA; all training, awareness and communication activities related to IT security shall be performed in close cooperation with Security Unit.

Article 25 - IT security compliance and continuous improvement

1. IT security compliance and continuous improvement shall involve the proper implementation and regular update of IT security policy, IT security standards and the security plans to meet the changing needs of eu-LISA. This process is there to ensure the recurring activities to enhance performance of the implementation of IT Security.

2. The roles relating to IT security compliance and continuous improvement shall be the following, in accordance with the RASCI model:

(a) the Executive Director shall be accountable for IT security compliance and continuous improvement;

(b) the Security Unit shall be responsible for performing the activities in this process;

(c) the eu-LISA Security Officer and the eu-LISA Departments and Units shall be kept informed.

3. The main activities associated with the IT security compliance and continuous improvement process shall be the following:

(a) the Security Unit shall ensure continuous improvement for activities within his responsibility;

(b) the Security Unit shall take into account the management review of security and risk management and results from audits, logs, security performance evaluations and triggers for changes to the IT security risk management process and suggest improvements to the Security Officer;

(c) the Security Unit shall take into account lessons learnt from the experience of past IT security incidents and where appropriate, shall organise 'lessons-learnt' sessions with the relevant stakeholders, in particular those involved in IT risk management; the goal of those sessions shall be to identify ways to improve the existing security controls or processes in order to prevent or reduce the impact of future incidents;

(d) the System Owner shall monitor compliance with the eu-LISA IT security policies and standards, in order to detect errors or potential breaches of compliance, to take appropriate corrective or preventive action and to assess the effectiveness and efficiency of the action taken; System Suppliers and IT Service Providers shall provide assurance to the System Owner of their compliance with the IT security policy;

(e) the Security Unit shall verify the implementation of the eu-LISA IT security policy on the basis of information in the security plans, the results of the annual IT security questionnaires and evaluation forms, exception reports, identified and reported IT security incidents and other relevant information; System Owners shall communicate to the Security Unit in a timely manner the information required to perform those activities;

(f) the eu-LISA Security Officer may request the Internal Audit Capability of eu-LISA to perform IT security audits on the eu-LISA's CIS if he or she deems it is necessary.

Article 26 - Encrypting technologies

1. The use of encrypting technologies for the protection of EU classified information (EUCI) shall comply with the decision of the Management Board No 2019-273.

2. The decisions on the use of encrypting technologies for the protection of non-classified data shall be taken by the eu-LISA Security Officer by consulting the Security Unit, taking into account both the risks that are intended to be mitigated through encryption and the risks that it introduces.

3. Prior approval from the CAA is required for all uses of encrypting technologies, unless the encryption is used only to protect the confidentiality of non-EUCI data in transit and uses standard network communications protocols.

4. With the exception noted in paragraph 3 of this Article, the Security Unit shall ensure that back-ups of any decryption keys are stored in key escrow for the purpose of recovering stored data in the event that the decryption key is not available. The recovery of encrypted data using back-ups of decryption keys shall be carried out only when authorised in line with the standard defined by the CAA.

5. Requests for approval for the use of encrypting technologies shall be formally documented and shall include details of the CIS and data to be protected, the technologies to be used and

the related security operating procedures. These requests shall be approved by the eu-LISA Security Officer.

6. Requests for approval for the use of encrypting technologies shall be evaluated by the CAA in line with the published standards and requirements.

Article 27 - IT security inspections

1. The Security Unit shall undertake IT security inspections in order to verify whether IT security processes, operations and measures comply with eu-LISA's IT security policies and to check the integrity of these control measures.

2. The Security Unit may perform an IT security inspection:

(a) on its own initiative;

(b) on request from the eu-LISA Security Officer

(c) on request from the Executive Director;

(d) on a request received from a system owner;

(e) further to a security incident; or

(f) further to the identification of a high risk to a particular system.

3. Data owners may request an IT security inspection before storing their information in a CIS.

4. The results of an inspection shall be documented in a formal report to the Executive Director, the eu-LISA Security Officer and to the system owner that includes findings and recommendations for improving the CIS's compliance with the IT security policy.

5. The Security Unit shall monitor the implementation of the recommendations.

6. Where appropriate, IT security inspections shall include the inspection of services, premises and equipment provided to the system owner, including both internal and external service providers.

Article 28 - Access from external networks

1. Without prejudice to Regulation (EU) 2018/1726, the Security Unit shall lay down the rules in a standard on authorising access between eu-LISA CISs and external networks.

2. The rules shall distinguish different types of external network connections and lay down appropriate security rules for each type of connection, including whether a prior authorisation for the connection is required from the relevant authority as noted in paragraph 4 of this Article.

3. If required, authorisation shall be granted on the basis of a formal request and approval process. The approval shall be valid for a specified duration and shall be obtained before the connection is activated.

4. The Security Unit shall have the overall responsibility for authorising requests.

5. The authorising entity may impose additional security requirements as a prerequisite for approval, in order to protect eu-LISA's CIS and networks from the risks of unauthorised access or other security breaches.

6. The System Owner of a CIS with the support of the Security Unit shall determine the security requirements for external access to that CIS and shall ensure the implementation of appropriate measures to protect its security.

7. The security measures implemented for external network connections shall be based on the principles of need to know, least privilege and secure baselining which ensure that individuals only receive the information and access rights that they need to perform their official duties for eu-LISA and they do it under conditions and with the means that ensure access security.

8. All external network connections shall be filtered and monitored to detect potential security breaches.

9. Where connections are established to allow the outsourcing of a CIS, the authorisation shall be conditional on the successful completion of the procedure described in Article 29.

Article 29 - Outsourcing of CISs

1. For the purposes of this decision, a CIS is considered to be outsourced when it is provided on the basis of a contract with a third party contractor, under which the CIS is housed on non-eu-LISA premises. This includes the outsourcing of individual or multiple CISs or other IT services, data centres on non-eu-LISA premises, and the handling of eu-LISA data sets by external services.

2. The outsourcing of a CIS shall take into account the sensitivity or classification of the information handled as follows:

(a) CISs handling EUCI shall be accredited in accordance with the decision of the Management Board No 2019-273. Systems handling EUCI shall not be outsourced;

(b) the system owner of a CIS handling non-EUCI information, with the support of the Security Unit, shall implement proportionate measures to address the security needs in line with the relevant legal obligations or the sensitivity of the information, taking into account the risks of outsourcing. The Security Unit may impose additional requirements.

(c) outsourced development projects shall take into account the sensitivity of the developed code and any test data used during development.

3. The following principles shall apply to outsourced CIS in addition to those laid down in Article 3 of the current decision:

(a) outsourcing arrangements shall be designed to avoid dependency on specific suppliers;

(b) outsourcing security arrangements shall minimise the possibilities for third party staff to access or modify eu-LISA information;

(c) third party staff that have access to an outsourced CIS shall provide confidentiality agreements;

(d) the outsourcing of a CIS shall be indicated in the inventory of CISs.

4. The Security Unit with the participation of the system owner and data owner shall:

(a) assess and document the risks relating to outsourcing;

(b) lay down relevant security requirements;

(c) consult with the system owners of all other connected CISs to ensure that their security requirements are included;

(d) ensure that appropriate security requirements and rights are included in the outsourcing contract;

(e) fulfil any other requirements laid down in the detailed procedure as noted in paragraph 8 of this Article.

These actions shall be completed before the contract or other agreement is signed for the outsourcing of one or more CISs.

5. System owners shall manage the risks relating to outsourcing during the lifetime of the CIS in order to meet the defined security requirements.

6. System owners shall ensure that third party contractors are obliged to immediately notify eu-LISA of all IT security incidents affecting an outsourced eu-LISA CIS.

7. The system owner is responsible for ensuring the compliance of the CIS, the outsourcing contract and the security arrangements with eu-LISA's rules on information security and IT security.

8. The detailed standards related to the responsibilities and activities set out in points (1) to (7) shall be laid down in accordance with Article 31 below.

CHAPTER 5 – MISCELLANEOUS AND FINAL PROVISIONS

Article 30 - Transparency

This decision shall be brought to the attention of Agency staff and to all individuals to whom it applies.

Article 31 - Implementing rules, standards, guidelines, security notices and best practices

1. The provisions of this decision shall, where necessary, be further detailed in implementing rules, standards, guidelines, security notices and best practices. IT security standards and guidelines shall provide further details for specific security domains according in particular to ISO 27001 Annex A. These standards and guidelines shall be based on industry best practices and selected to suit eu-LISA's IT environment.

2. Standards shall, where necessary, be developed according in particular to ISO 27001 Annex A in the following domains:

(1) organisation of information security;

(2) human resources security;

(3) asset management;

(4) access control;

(5) cryptography;

(6) physical and environmental security;

(7) operational security;

(8) communications security;

(9) system acquisition, development and maintenance;

(10) supplier relationships;

(11) information security incident management;

(12) information security aspects of business continuity management;

(13) compliance.

3. According to Article 24(3)(c) of Regulation (EU) 2018/1726, the Management Board empowers the Executive Director to adopt implementing rules, standards, guidelines, security notices and best practices falling under the scope of this decision.

4. The Management Board may revoke, by way of a decision, this empowerment at any time and exercise this right itself.

5. The Executive Director shall keep the Management Board informed about the adopted implementing rules, standards, guidelines, security notices and best practices falling under the scope of this decision, in particular through the interim report and consolidated annual report of the Agency's activities.

6. The Executive Director may instruct the eu-LISA Security Officer to prepare the measures under this article.

Article 32 – Relation to other acts

The provisions of this decision are without prejudice to the Decision No 2019-273 and with the Decision No 2019-208.

Article 33 - Entry into force

This decision shall enter into on the day of its adoption by the Management Board.

Zsolt Szolnoki

Chairperson of the Management Board