DECISION OF THE MANAGEMENT BOARD ON SECURITY RULES ON THE PROTECTION OF COMMUNICATION AND INFORMATION SYSTEMS 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- Not for publication.
DECISION OF THE MANAGEMENT BOARD OF eu-LISA ON THE SECURITY RULES ON THE PROTECTION OF COMMUNICATION AND INFORMATION SYSTEMS IN eu-LISA

The Management Board,

1. Having regard to Article 15 of the Decision of Management Board on Security Rules in eu-LISA 2016-133 REV 3 on the need of all Corporate Communication and Information Systems ('CIS') to comply to security measures and standards identified in a Decision on The Management Board on the security of Communication and Information Systems,

2. Having used as reference the Commission Decision (EU, Euratom) No 2017/46 of 10 January 2017 and also ISO27000 series on information security,

3. Having regard to the subjects’ matters:
   i. The Agency’s communication and information systems are an integral part of the functioning of the Agency and information security incidents can have a serious impact on the Agency’s operations as well as on third parties, including individuals, businesses and Member States;
   ii. There are many threats that can harm the confidentiality, integrity or availability of the Agency’s communication and information systems and of the information processed therein. These threats include accidents, errors, deliberate attacks and natural events, and need to be recognised as operational risks;
   iii. Communication and information systems need to be provided with a level of protection commensurate with the likelihood, impact and nature of the risks to which they are exposed;
   iv. Information security in the Agency should ensure that the Agency’s Communication and Information Systems (CISs) protect the information they process and they function as they need to, when they need to, under the control of legitimate users;
   v. The information security policy of the Agency should be implemented in a manner, which is consistent with the policies on security in the Agency;
   vi. The Security Unit has the general responsibility for security in the Agency and it is under the authority and responsibility of the eu-LISA Security Officer;
   vii. The Agency’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;
   viii. Appropriate measures should be developed and implemented by eu-LISA departments and units responsible for communication and information systems and information security measures for protecting communication and information systems should be coordinated across the Agency to ensure efficiency and effectiveness;
   ix. The personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and
against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).  

Adopts this Decision:

---

1 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (23.10.2018, Article 4, p.20)
Table of Contents

CHAPTER 1 - GENERAL PROVISIONS ................................................................. 5
  Article 1 - Definitions .................................................................................. 5
  Article 2 - Subject matter and scope .......................................................... 7

CHAPTER 2 - ORGANISATION AND RESPONSIBILITIES ............................ 8
  Article 3 - Management Board .................................................................. 8
  Article 4 - Executive Director ................................................................... 8
  Article 5 - eu-LISA Security Officer ........................................................... 8
  Article 6 - Information Security Steering Board (ISSB) .............................. 9
  Article 7 - Security Unit ............................................................................ 9
  Article 8 – eu-LISA Departments ............................................................... 10
  Article 9 - System owners ......................................................................... 11
  Article 10 - Controller ............................................................................ 12
  Article 11 - Processor ............................................................................... 12
  Article 12 - Product Managers ................................................................. 12
  Article 13 - System Security Officers (SSOs) ........................................... 12
  Article 14 - Information Security Officers (ISOs) ..................................... 12
  Article 15 - Users .................................................................................... 12

CHAPTER 3 - INFORMATION SECURITY OBJECTIVES & REQUIREMENTS ... 13
  Article 16 - Basic Principles ..................................................................... 13
  Article 17 - Information Security Governance .......................................... 14
  Article 18 - Information Security Risk Management ............................... 14
  Article 19 - Outsourcing of CISs and Supplier Security ............................ 15
  Article 20 - Secure IT System Development and Acquisition .................. 16
  Article 21 - Secure IT operations .............................................................. 16
  Article 22 - Encrypting technologies ......................................................... 17
  Article 23 - Access from external networks .............................................. 18
  Article 24 - Information Security Incident Management ........................ 18
  Article 25 - Information Security Assessments and Inspections .............. 19
  Article 26 - Information Security Training, Awareness and Communications ........................................ 20
  Article 27 - Obligation to comply ............................................................. 20

CHAPTER 4 - FINAL PROVISIONS ................................................................. 20
  Article 28 - Transparency ........................................................................ 20
  Article 29 - Implementation of this Decision ............................................. 21
  Article 30 - Repeal and transitional measures ........................................ 21
  Article 31 - Entry into force ..................................................................... 21
CHAPTER 1 - GENERAL PROVISIONS

Article 1 - Definitions

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

<table>
<thead>
<tr>
<th>Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Impact Analysis (BIA)</td>
<td>It is the process of analysing activities and the effect that a business disruption might have upon them.</td>
</tr>
<tr>
<td>Communication and information system (CIS)</td>
<td>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.</td>
</tr>
<tr>
<td>Data set</td>
<td>Means a set of information, which serves a specific business process, or activity of the Agency.</td>
</tr>
<tr>
<td>Emergency procedure</td>
<td>Means a predefined set of methods and responsibilities for responding to urgent situations in order to prevent a major impact on the Agency.</td>
</tr>
<tr>
<td>Exception</td>
<td>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;</td>
</tr>
<tr>
<td>Information security policy</td>
<td>Means a set of information security objectives, which are or have to be established, implemented and checked.</td>
</tr>
<tr>
<td>Information security or security of CIS</td>
<td>Means the preservation of confidentiality, integrity and availability of CISs and the data sets that they process.</td>
</tr>
<tr>
<td>Information security guidelines</td>
<td>Consist of recommended but voluntary measures that support information security standards or serve as a reference when no applicable standard is in place.</td>
</tr>
<tr>
<td>Information security incident</td>
<td>Means an event that could adversely affect the confidentiality, integrity or availability of a CIS.</td>
</tr>
<tr>
<td>Information security measure</td>
<td>Means a technical or organisational measure aimed at mitigating information security risks.</td>
</tr>
<tr>
<td>Information security need</td>
<td>Means a precise and unambiguous definition of the levels of confidentiality, integrity and availability associated with a piece of information or a CIS with a view to determining the level of protection required.</td>
</tr>
<tr>
<td>Information security objective</td>
<td>Means a statement of intent to counter specified threats and/or satisfy specified organisational security requirements or assumptions.</td>
</tr>
<tr>
<td>Information security plan</td>
<td>Means the documentation of the information security measures required meeting the information security needs of a CIS.</td>
</tr>
</tbody>
</table>
### Information security requirement

Means a formalised information security need through a predefined process.

### Information security risk

Means an effect that an information security threat might induce on a CIS by exploiting a vulnerability. As such, an information security risk is characterised by two factors: (1) uncertainty, i.e. the likelihood of an information security threat to cause an unwanted event; and (2) impact, i.e. the consequences that such an unwanted event may have on a CIS.

### Information security standards

Means specific mandatory information security measures that help enforce and support the information security policy.

### Information 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 asset

Means a technical asset as part of an IT system that has value for the organisation.

### 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 service

Means the services provided by an IT system or IT Service Provider to support the functionality or operations of a CIS.

### IT system

Means the technical assets of a CIS that is to 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 CIs.

### Personal data

Means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.²

### 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.

---

² 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 (23.10.2018, p. 17)
**Risk treatment**

Means the process to modify risk, which may involve:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk with another party or parties (including contracts and risk financing); and
- retaining the risk by informed choice.

**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.

**Security in the Agency**

Means the security of persons, assets and information in the Agency, and in particular the physical integrity of persons and assets, the integrity, confidentiality and availability of information and communication and information systems, as well as the unobstructed functioning of Agency operations.

**Shared IT service**

Means the service a CIS provides to other CISs in the processing of information.

**Technical specification**

Means the detailed description of a requirement, typically used in the software design process.

**User**

Means any individual who uses functionality provided by a CIS, whether inside or outside the Agency.

---

**Article 2 - Subject matter and scope**

1. This Decision applies to all communication and information systems (CISs) which are owned, procured, managed or operated by or on behalf of the Agency and all usage of those CISs by the Agency.

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. When a CIS is provided, owned, managed or operated by an external party on the basis of a bilateral agreement or contract with the Agency, the terms of the agreement or contract shall comply with this Decision.

3. This Decision applies to all eu-LISA departments and units. When an CIS is used by other bodies and institutions on the basis of a bilateral agreement with the Agency, the terms of the agreement shall comply with this Decision.

4. Notwithstanding any specific indications concerning particular groups of staff, this Decision shall apply to the Members of the Agency, to Agency staff falling under the scope of the Staff Regulations of Officials of the European Union (the ‘Staff Regulations’) and the Conditions of

---

3 ISO/IEC 27005, Information technology – Security techniques – Information security risks management (01.06.2011, p. 11)
Employment of Other Servants of the Union (the ‘CEOS’), to national experts seconded to the Agency (‘SNEs’), to external service providers and their staff, to interns and to any individual with access to CIS in the scope of this Decision.

CHAPTER 2 - ORGANISATION AND RESPONSIBILITIES

Article 3- Management Board

The Management Board responsibilities on security are defined in the Agency Establishing regulation.

Article 4- Executive Director

The Executive Director responsibilities on security are defined in the Agency Establishing regulation. Furthermore, the Executive Director shall be accountable for the information security governance in the Agency.

Article 5- eu-LISA Security Officer

1. The eu-LISA Security Officer’s responsibilities on security are defined in Decision of the Management Board on security rules in eu-LISA.
2. The eu-LISA Security Officer shall take the operational responsibility for the governance of information security as a whole within the Agency.
3. The eu-LISA Security Officer shall propose to the Executive Director the Agency’s information security policy for further adoption by the Management Board.
4. The eu-LISA Security Officer shall report to Executive Director and to the Management Board on governance matters including the implementation status of the security and continuity strategy as well as on IT-security-related issues, including serious information security incidents.
5. The eu-LISA Security Officer shall monitor and review the overall implementation of this Decision and report it to the Executive Director and to the Management Board.
6. The eu-LISA Security Officer shall monitor, evaluate and control the Agency’s information risk treatment landscape and shall have the power to issue formal requirements for improvements.

---

5 Commission Decision of 12 November 2008 laying down rules on the secondment to the Commission of national experts and national experts in professional training (C(2008) 6866 final)
8 Decision of the Management Board on security rules in eu-LISA (2016-133 REV 3, Article 6, p. 7-8)
Article 6 - Information Security Steering Board (ISSB)

1. The ISSB shall be chaired by the eu-LISA Security Officer or his delegate. Its members shall include representatives of the Security Unit, the Operations Department, the Resources and Administration Department, and representatives of other eu-LISA departments involved, where information security is a major concern for their operations.
2. The ISSB shall provide advice and guidance on security related matters to the Management Committee.
3. The ISSB shall facilitate the exchange of early warning and threat information in line with the Agency mandate.
4. The ISSB shall facilitate an easier exchange of information among the eu-LISA Departments in case of security incidents and of tasks related to the security of the CISs and the large-scale IT systems.

Article 7 - Security Unit

In relation to information security, the Security Unit shall:
1. Support the eu-LISA Security Officer in developing information security policies, rules, standards and guidelines.
2. Develop the information security risk management methods and processes for all eu-LISA departments and report on information security risks management outcomes regularly to the eu-LISA Security Officer.
3. Propose the security strategy for revision and approval by the Management Committee and further adoption by the Management Board, and propose a programme, including the planning of projects and activities implementing the security and continuity strategy.
4. Monitor the execution of the Agency's security and continuity strategy and report on this regularly to the eu-LISA Security Officer.
5. Monitor the information security risks and information security measures implemented in CISs and report on this regularly to the eu-LISA Security Officer and the System Owner.
6. Report regularly on the overall implementation and compliance with this Decision to the eu-LISA Security Officer.
7. Ensure that there is an adequate catalogue of information security services available for the system owners and data controllers to fulfil their responsibilities for information security and to comply with the information security policy and standards.
8. Provide adequate documentation to system owners and data controllers, support and consult with them, as appropriate, on the information security measures implemented for their IT services in order to mitigate information security risks to CISs and facilitate compliance with the overall eu-LISA information security policy.
9. Assess information security risks and determine the information security requirements for each CIS, in collaboration with the data controllers and the system owner.
10. Prepare a security plan, including, where appropriate, details of the assessed risks and any additional security measures required in collaboration with the data controller and the system owner.
11. Inform the relevant eu-LISA departments 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 the Agency.

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

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

14. Define the training needs and coordinate training programmes on information security in cooperation with the eu-LISA departments and develop, implement and coordinate awareness-raising campaigns on information security in close cooperation with the Human Resources and Training Unit.

15. Ensure that system owners, data controller and other roles with information security responsibilities in eu-LISA departments are made aware of the information security policy.

16. Perform information security inspections, technical vulnerability assessments and penetration tests to assess the compliance of the CISs with the security policy, and report the results to the eu-LISA Security Officer.

17. Establish a framework for the authorisation of access with the associated appropriate security rules to CISs from external networks and develop the related information security standards and guidelines in close cooperation with the eu-LISA Departments.

18. Establish a framework for the management of business continuity in relation to CISs and develop the related information security standards and guidelines in close cooperation with the eu-LISA Departments.

19. Establish principles and rules for information security aspects in relationships with suppliers of the CISs in order to maintain appropriate control of security of the information.

**Article 8 – eu-LISA Departments**

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

1. Formally appoint a system owner for each CIS who will be responsible for information security of that CIS and formally appoint a data controller for each data set handled in a CIS according to the Regulation (EC) No 1725/2018;

2. Hold ultimate accountability for information security for the CISs and the data sets under their Department’s responsibilities;

3. Own the risks relating to their CISs and data sets;

4. Ensure, with the support of the Security Unit, that appropriate information security risk assessments and information security plans have been made;

5. Ensure, with the support of the Security Unit, that information security plans and information security measures are implemented and the risks are adequately treated;

6. Be aware about the information security risks and measures applicable to the CISs under their responsibility;

7. Ensure, with the support of the Security Unit, that appropriate processes, procedures and solutions are in place to ensure efficient detection, reporting and resolution of information security incidents relating to their CISs;
8. Launch, with the support of the Security Unit, an emergency procedure in case of information security emergencies;

9. Resolve any disagreements between data controllers and system owners and in case of continued disagreement bring the issue to the Executive Director for resolution.

**Article 9 - System owners**

1. Without prejudice to the regulations established the large scale IT systems operated by the Agency, the system owner is responsible for the information security of the CIS with the support of the Security Unit and reports to the Head of the eu-LISA Departments or Units.

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

3. In relation to information security, the system owner, with the support of Security Unit, shall:
   a) ensure the compliance of the CIS with the information security framework;
   b) ensure that the CIS is accurately recorded in the relevant inventory;
   c) decide and implement appropriate information security measures, proportionate to the information security risks identified;
   d) 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;
   e) be informed regularly by the Security Unit of the information security risk profile of their CIS, on the related risks, risk management activities and security measures taken to be able to manage and monitor these risks;
   f) ensure that the appropriate instructions are issued to users on the use of the CIS and associated data as well as the responsibilities of users related to CIS;
   g) for outsourced systems, ensure that appropriate information security provisions are included in the outsourcing contracts and that information security incidents occurring in the outsourced CIS are reported in accordance with Article 24;
   h) for the relationship with the system suppliers, ensure that appropriate information security provisions are included in the contracts and that information security incidents occurring in the CIS are reported in accordance with Article 24;
   i) for CIS providing shared IT services, ensure that a defined security level is provided, clearly documented and security measures are implemented for that CIS in order to reach the defined security level.

4. Consult the Security Unit in advance concerning any system processing EU classified information.

5. 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.

6. Notify the Security Unit of any exceptions to the information security policy including relevant justifications.

7. Report any unresolvable disagreements between the data controller and the system owner to the head of the Agency, Department or Unit.

8. Ensure that the information security incidents are communicated to the relevant stakeholders in a timely manner as appropriate according to their severity as laid down in Article 24.
Article 10 - Controller

1. Controller means the Union institution or body or the Directorate-General or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law.9

2. The responsibilities of the Data Controller are defined in the 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.10

Article 11 - Processor

The Processor responsibilities are defined in the Regulation (EU) 2018/1725.11

Article 12 - Product Managers

The Product Manager manages and/or operates the IT system on behalf of the System Owner and ensures proper access management, backup, logging, monitoring, patch 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 on security rules in eu-LISA12.

Article 14 - Information Security Officers (ISOs)

The Information Security Officers responsibilities on security are defined in the Decision of the Management Board on security rules in eu-LISA13.

Article 15 - Users

1. In relation to information security, users shall:
   a) comply with the information security policy and the instructions issued by the System Owner on the use of each CIS;

---

9 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 (23.10.2018, p. 18)

10 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 (23.10.2018, Article 26, p. 30)

11 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 (23.10.2018, Article 19, p. 31)

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

13 Decision of the Management Board on security rules in eu-LISA (2016-133 REV 3, Article 9, p. 9)
b) communicate information security incidents as provided for in Article 24.

2. Use of the CIS in breach of the information security policy or instructions issued by the System Owner may give rise to disciplinary proceedings.

CHAPTER 3 - INFORMATION SECURITY OBJECTIVES & REQUIREMENTS

Article 16 - Basic Principles

1. Information security in the Agency shall be based on the principles of legality, transparency, proportionality and accountability.

2. Information security issues shall be taken into account from the start of the development and implementation of CISs. In order to do so, the Security Unit shall be involved.

3. Effective information 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 (EC) No 1725/2018;
   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. The Agency shall establish, implement, maintain and continually improve an information security management system (ISMS), which preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed and ensure business continuity by pro-actively limiting the impact of a security breach. The ISMS shall be integrated with the organization’s processes and overall management structure and that information security is considered in the design of processes, information systems, and controls.

5. The ISMS shall meet the European Union’s regulatory requirements and should be aligned with ISO 27001 information security management systems requirements and ISO 22301 business continuity management systems requirements. The ISMS shall take into account the synergy opportunities provided by both ISO standards with the goal to increase efficiency and added value of implementing both management systems and shall enable the implementation of a resiliency framework.

6. Information security shall be based on a risk management process. This process shall aim at determining the levels of information security risks and defining security measures to reduce such risks to an appropriate level and at a proportionate cost.

7. All CIS shall be identified, assigned to a system owner and recorded in an inventory.
8. The security requirements of all CIS 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.

9. Information security plans and information security measures shall be proportionate to the security needs of the CIS.

**Article 17 - Information Security Governance**

1. Information security governance is the process of establishing and maintaining a framework to support management structure and processes to provide assurance that information security strategies are aligned with and support the Agency’s objectives. The effective governance of information security ensures that the governing body receives relevant reporting about information security-related activities. This enables pertinent and timely decisions about information security issues in support of the strategic objectives of the Agency.

2. The processes related to governance of information 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 Governance Body gives direction about the information 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 information security plans;

   c) ‘monitor’: the governance process that enables the Governance Body to assess the achievements of strategic objectives;

   d) ‘communicate’: the bidirectional governance process by which the Governance Body and stakeholders exchange information about information security, appropriate to their specific needs;

   e) ‘assure’: the governance process by which the Governing Body commissions Agency’s 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.

**Article 18 - Information Security Risk Management**

1. The information security risk management process shall consist of the following phases:

   a) ‘context establishment’: the external and internal context for information 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 information 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 information 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.

2. The information security risk management process shall identify, assess and implement a set of cost-effective security measures for a CISs to reduce risks to an acceptable level.

3. All CISs of the Agency shall have a documented Security Plan that provides advice and guidance regarding their security, their preparation and use, complementing other Agency standards and guidelines of the established Information Security Management System (ISMS), such as those associated with risk management, asset classification and other aspects of security. A security plan shall be implemented and reviewed in regular intervals.

Article 19 - Outsourcing of CISs and Supplier Security

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-Agency premises. This includes the outsourcing of individual or multiple CISs or other IT services, data centres on non-Agency premises, and the handling of Agency data sets by external services. The outsourcing of a CIS shall take into account the sensitivity or classification of the information handled as follows. CIS handling EUCI shall be accredited in accordance with the Agency security rules derived from Decision (EU, Euratom) 2015/444, and the Agency Security Accreditation Authority (SAA) as defined in that Decision shall be consulted in advance.

2. Agency shall be concerned about the security risks related to the products and services delivered by external parties and Suppliers. A standard on Supplier Security shall aim to decrease supply chain security risks.

3. The information security requirements for mitigating the risks associated with supplier access to Agency’s information or information processing facilities shall be documented.

4. Suppliers shall follow the information security standards and guidelines of the Agency.

5. Supplier agreements shall be established and documented to ensure that there is no misunderstanding between the Agency and the supplier regarding both parties’ obligations to fulfil relevant security requirements.

6. Agreements with suppliers shall include requirements to address the information security risks associated with Information and Communications Technology services and product supply chain. In order to maintain an agreed level of information security and service delivery in line with supplier contracts/agreements, Agency shall regularly monitor, review and audit supplier service delivery.

7. Secure Software Development Lifecycle guidelines of the Agency shall be followed by the system Supplier.
Article 20 - Secure IT System Development and Acquisition

1. Software applications shall be secured in order to protect them from security incidents caused by human error or abuse. The necessary controls shall be built into information systems during the System Development Lifecycle.

2. 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.

3. All information systems shall have a System Owner, whose responsibilities include system security.

4. Appropriate information security requirements (by means of non-functional requirements) shall be identified, analysed and documented at the requirements phase of a project, in the functional/technical specifications of the Agency's information processing systems. It is noted that security requirements shall be justified, agreed and documented as part of the project documentation.

5. Information security requirements shall be addressed for new systems, applications or products to be acquired or implemented by the Agency (or on behalf of the Agency by a Supplier) as well as for existing that will be updated/enhanced.

6. Agency shall establish a formal testing and acquisition process, which will be based on well-defined acceptance criteria according to the categorisation/classification level of the target system, application or product.

7. The applied security controls shall mitigate - in an acceptable way according to the Agency standards and requirements - the identified security risks in the operational environment of the system, during its entire lifecycle, and be proportional to system categorisation/classification.

8. Any functionality not supporting or not necessary for any business needs shall be disabled as it may enlarge the attack surface of the target system, application or product.

9. Introduction of new systems and major changes to existing CIS (including patches, service packs and other updates) shall be approved after:
   a. conducting a risk assessment in order to analyse the impacts of changes,
   b. implementation of the appropriate security controls,
   c. security testing (including security code review where possible) and acceptance in an environment segregated from both the production and development environments.

10. Vulnerability assessments and penetration tests shall be performed regularly in accordance with the criticality and the sensitivity of the CIS.

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 the Agency’s IT environments.
2. Documented operating procedures shall be prepared for all IT and communication systems. These procedures shall be kept up to date at all times and made available to all personnel on a need to know basis. The procedures shall not be made available to unauthorised people.

3. Sensitive system documentation shall be stored securely, whether it is in electronic or non-electronic form.

4. Current and future capacity requirements shall be reviewed to ensure that resources are acquired in time to prevent availability issues, taking into account the business criticality of the concerned system.

5. System tuning and monitoring shall be applied to ensure and, where necessary, to improve the availability and efficiency of systems while detective controls shall be put in place to indicate problems in due time.

6. All relevant resources that are used for the provision of IT systems shall be included in the capacity management.

7. Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of information systems.

8. Development, test and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.

9. Services delivered by third parties involving accessing, processing, communicating or managing the information or information processing facilities or adding products or services to information processing facilities shall have appropriate integrated security controls. These security controls, the service definition and the delivery levels shall be documented in service delivery agreements to ensure they are properly implemented, operated and maintained by the third party.

10. The services, reports and records provided by the third party shall be managed by designated Agency personnel, regularly monitored and reviewed, and audits shall be carried out regularly. Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, must be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

**Article 22 - Encrypting technologies**

1. The use of encrypting technologies for the protection of EU classified information (EUCI) shall comply with the Agency’s security rules based on Decision (EU, Euratom) 2015/444.

2. Cryptographic controls for the protection of information shall be approved in advance and their use will be allowed for the approved purposes and under the approved conditions. Cryptographic measures shall be used in compliance with all relevant agreements, laws and regulations.

3. Cryptographic requirements shall be initially determined by the data categorization.

4. Key management, including recovery and escrow arrangements, shall be in place to support the use of cryptographic techniques. A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.
Article 23 - Access from external networks

1. Rules shall be laid down in a standard on authorising access between Agency CISs and external networks. The standard 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.

2. Networks shall be managed and controlled to protect information in systems and applications, using the following controls:
   a) Responsibilities and procedures for the management of networking equipment shall be established;
   b) If possible, operational responsibility for networks shall be separated from computer operations;
   c) Controls shall be established to safeguard the confidentiality and integrity of data passing over Agency's networks;
   d) Logging and monitoring of network traffic shall be enabled;
   e) Management activities shall be closely coordinated both to optimize the service to the Agency and to ensure that controls are consistently applied across the information processing infrastructure;
   f) Systems on the network shall be authenticated;
   g) Connection of systems to the network shall be restricted.

Article 24 - Information Security Incident Management

1. A standard shall provide the essential elements that shall be in place for the reporting of and response to events that may impact information confidentiality, integrity or availability. Consequently, the standard shall also provide rules for determining the security relevance of such events so that they may be reported and escalated when appropriate, according to the risks involved.

2. The IT security incident management process shall be based on the Cyber Security Readiness Team (CSRT) Framework consists of the following main phases:
   a) Preparation: This phase defines the main actions that should be in place in order to ensure the CSRT and eu-LISA readiness and that the appropriate technical and organizational countermeasures are in place in order to prevent from unwanted events.
   b) Detection: The goal of this phase is to ensure that all possible security incidents are promptly detected and reported for further analysis in order to minimize the potential impact at the core business systems or corporate eu-LISA systems.
   c) Triage: During this phase, the authorized eu-LISA personnel will collect and analyse all the evidences regarding the detected incident and assess its criticality in order to properly contain and eradicate the unwanted event.
   d) Containment – Eradication: The main goal of this phase is the limitation of the damage and the prevention of any further damage to the same or other constituent systems.
   e) Recovery: This phase defines the proper actions required in order to return to the normal operation the affected systems.
   f) Post Incident Activity: This phase helps evaluate the reason for the incident outbreak, the missed precursors and new indicators that should be added to the procedure for earlier
detection and/or prevention.

3. Appropriate methodologies and tools shall be adopted in order to identify, collect, analyse and present all the digital evidences related to a computer crime ensuring the proper presentation into court.

Article 25 - Information Security Assessments and Inspections

1. The information security assessments and inspections shall apply to all CIS that are operated by or on behalf of the Agency, to all facilities housing these systems and to all processes relevant to their operation.

2. The information security assessments and inspections shall be conducted in order to verify whether the security measures comply with the Agency’s information security policies and standards and to check the integrity of these control measures.

3. The information security assessments and inspections shall be conducted in order to verify whether all relevant personnel, including all Agency officials, service providers and third parties who are responsible for operating Agency IT systems comply with the established security policy and procedures.

4. The security assessment plan shall provide the objectives for the security inspection, detail how to conduct the actual assessment, and what procedures to follow. These procedures might be slightly differentiating depending on whether the Agency is conducting:
   a) internal developmental testing and evaluation;
   b) independent verification and validation;
   c) assessments supporting security authorizations or reauthorizations;
   d) audits;
   e) continuous monitoring;
   f) assessments subsequent to remediation actions;
   g) other.

5. The Agency shall provide to the assessors all of the essential supporting assessment-related materials needed in order to conduct an effective security control assessment.

6. The findings of the assessment shall be used to proceed to the mitigation of the associated risks, according to the Agency's priorities.

7. Following the mitigation of security risks via the security controls, the remediated controls shall be reassessed for effectiveness. This can help determine whether the remediated controls are implemented correctly and are operating as intended.

8. The findings of the assessment shall be reflected on the security plan as well, which shall be updated to reflect the actual state of the security controls after the initial assessment. Any modifications made by the system owner addressing recommendations for corrective actions have to be included in the security plan. The list of residual vulnerabilities shall also be documented.
Article 26 - Information Security Training, Awareness and Communications

1. The Agency shall design, develop, implement, and maintain a security awareness and training program, as a part of its security program. Therefore, it will be enabling members of staff working with the Agency (including Suppliers staff) to have the appropriate skills and awareness to perform their duties in a secure manner and to protect the Agency’s business and assets.

2. All Agency staff and, where relevant, Agency contractors and third party personnel shall receive appropriate training in security awareness, policies and procedures, to the extent required by their duties.

3. Information security training, awareness and communication shall:
   a) determine the necessary competences of individuals working within their remit that affects the information security performance of the Agency;
   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:
      a. the information security policy;
      b. the implications of not conforming to the information 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.

Article 27 - Obligation to comply

1. Compliance with the provisions outlined in the current Decision, the information security policy and standards is mandatory.

2. Non-compliance with the current Decision, information 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 information security policy.

4. In the event the eu-LISA Security Officer decides that there is a persistent unacceptable risk to a CIS of the Agency, the Security Unit in cooperation with the system owner shall propose mitigating measures to the eu-LISA Security Officer for approval.

CHAPTER 4 - FINAL PROVISIONS

Article 28 - Transparency

This decision shall be brought to the attention of Agency staff and to all individuals to whom they apply.
Article 29 - Implementation of this Decision

1. The Executive Director shall approve the information security baseline, standards, guidelines and security notices derived from this Decision. The Management Board shall in particular adopt the security baseline.

2. The detailed roles and responsibilities for the provisions in chapters 2 and 3 shall be further detailed in the relevant standards.

Article 30 - Repeal and transitional measures


The implementing rules and information security standards adopted pursuant to Article 10 of decision C(2006) 3602 shall remain in effect insofar as they do not conflict with this decision, until they are replaced by the standards that shall be adopted under Article 29 of this Decision.

Article 31 - Entry into force

This decision shall enter into force on the date of its adoption.

Done at Strasbourg,

For the Management Board,

Zsolt Szolnoki
Chairman