Document History

Status	Date	Update
Initial draft	22.10.2014	
Included comments	17.12.2014	Document reviewed and the comments were accommodated.
Endorsed **Version 1.0**		Security Policy endorsed by the ED

Document Sign-Off[1]

Initiation	Validation	Approval	Legal Check	Quality Check	Endorsement
Initiator	**IT & Corporate Services Coordinator**	**Governance & Organization Coordinator**	**Legal Coordinator**	**Governance& Organization Expert**	**Executive Director**
Signature	Signature	Signature	Signature	Signature	Signature
Date	Date	Date	Date	Date	Date

[1] *Delegations may apply*

1. Definitions

For the purposes of this Policy the following definitions apply:

Information	Data in a form that allows it to be communicated recorded or processed.
Document	Any letter, note, minute, report, memorandum, signal/message, sketch, photograph, slide, film, map, chart, plan, notebook, stencil, carbon, typewriter or printer ribbon, tape, cassette, computer disk, CD-ROM, or other physical medium on which information has been recorded.
Communication and Information System (CIS) or Information System	Set of equipment (mainly IT equipment), methods and procedures, and where relevant also persons, personnel, organised to perform information processing functions.
Need-to-know principle	The need of an individual employee to have access to a particular piece of information in order to be able to perform its duties.
Originator	The duly authorised author[1] of information or document.
Holder	The duly authorised person having the custody of information or document and having the responsibility to protect it according to the security provisions.
Third parties	European Union Institutions, Bodies and Agencies, Member States, Third States, International Organisations or other entities.

2. Policy Statement and Purpose

2.1 This policy demonstrates EIOPA's commitment for the appropriate application of the protective security and confidentiality principles, ensuring a secure working environment necessary for achieving the EIOPA objectives.

[1] *A department, unit, team, function or similar service*

2.2 This policy establishes the minimum standards of security to be applied in order to ensure that a sufficient degree of protection is guaranteed for the EIOPA's staff and valuable assets, such as information, documents, premises and equipment.

2.3 EIOPA ensures the compliance with the Protocol No 7 on the Privileges and Immunities of the European Union annexed to the Treaty of the European Union and the Treaty on the Functioning of the European Union[2].

2.4 EIOPA guarantees a high level of protection of personal data and the processing thereof in accordance with the Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[3].

2.5 EIOPA ensures that all stakeholders are informed about this policy and the subsequent implementing documents by necessary training and awareness programmes.

2.6 This policy is applicable to:

(a) all EIOPA statutory staff, hereafter referred to as "EIOPA Staff" or "EIOPA Staff member"[4];

(b) contractors, subcontractors and their employees[5]; and

(c) all other persons, working with EIOPA Staff or receiving access to EIOPA information, premises and equipment.

2.7 Any action or inaction, either accidental or deliberate, which is contrary to the rules established by this policy, might have disciplinary consequences in accordance inter alia with the provisions of the Staff Regulations[6].

---

[2] *O.J C 115, 9.5.2008*

[3] *O.J. L8, 12.1.2001*

[4] *The "EIOPA Staff member" includes: individuals covered by the Staff Regulations and CEOS, as well as Seconded National Experts*

[5] *For the purpose of this decision, interim employees and consultants*

[6] *Failing to comply with the provisions of this policy or with Article 17 of the Staff Regulations, disciplinary action may be taken under Article 86 of the Staff regulations*

3. Security Governance Areas

Personnel

3.1 EIOPA is committed to provide a safe and secure working environment for all Staff members, delegates, visitors, consultants, suppliers and any persons authorised to be on the Authority's premises by addressing the following key elements:

(a) Harassment and violence in the workplace;

(b) Prevention of loss and theft in the office; and

(c) Accidents on EIOPA's premises.

3.2 EIOPA is also committed to provide its Staff members with travel advice when on mission.

3.3 Training and awareness sessions provide relevant guidance for understanding and following the responsibilities defined under this policy.

Information and Documents

3.4 EIOPA is actively committed to ensuring the required levels of confidentiality, integrity and availability of information and documents by following the principles of the Commission Decision 2001/844/EC, ECSC, Euratom of 29 November 2001 amending its internal Rules of Procedure.

3.5 EIOPA information and documents require protection throughout their entire life-cycle, for preserving:

- Confidentiality: by ensuring protection against unauthorised disclosure;
- Integrity: by guaranteeing prevention of corruption, unauthorised alteration or unauthorised deletion; and
- Availability: by ensuring access to information is not being denied to those needing and authorised to have access.

3.6 The originator has the responsibility of assigning EIOPA information with the required levels of confidentiality, integrity and availability as defined by the Decision of the Management Board of EIOPA concerning the Protection of Information Systems and Information[7].

[7] *EIOPA Confidentiality levels:* ***Public, EIOPA Regular Use, EIOPA Restricted Use, EIOPA Confidential Use*** *as defined by EIOPA-MB-14/034 from 10 June 2014*

3.7 EIOPA's sensitive information is disseminated solely on the basis of the principle of need-to-know to individuals who have been briefed on the relevant security responsibilities.

3.8 The information originating from third parties should be protected in the same way as the EIOPA originated information and in accordance with the instructions received from those parties. Where applicable, security agreements or similar arrangements setting up the equivalence of the classification levels are used.

3.9 In line with the transparency principles and the rights of public access to information and documents, the initially assigned confidentiality levels should be reviewed periodically and maintained only as long as the information requires protection.

Physical Infrastructure

3.10 Physical security measures are designed to protect the EIOPA's staff, valuable assets and the authorised persons within the EIOPA premises.

3.11 Unauthorised access to EIOPA premises, buildings, offices and meeting rooms should be prevented. Special rules for visitors should be implemented and followed.

3.12 An efficient and cost-effective combination of physical security measures should be in place, that are proportionate to:

(a) The level of threat to EIOPA assets;

(b) The value of the assets at stake; and

(c) The volume and the sensitivity level of the information and information systems at risk.

3.13 The physical security requirements are also applicable to third party premises where EIOPA information systems are housed or operated.

3.14 Contracts with third parties should include appropriate requirements for physical and environmental security in accordance with this policy, and provisions for auditing the relevant security measures.

Communication and Information Systems

3.15 EIOPA complies with the relevant parts of the Commission Decision C(2006) 3602, concerning the security of information systems used by the European Commission.

3.16 The integrity and the availability are assured for all EIOPA communication and information systems. When handling, storing or transmitting sensitive information, the confidentiality is also preserved.

3.17 EIOPA communication and information systems should have Security Plans describing their overall security needs. They fall into the following categories, based on their security needs:

(a) **'STANDARD'** if the required confidentiality level is EIOPA Restricted Use or below and both the required availability and integrity levels are MODERATE[8]; and

(b) **'SPECIFIC'** for all other combinations of required confidentiality, integrity and availability levels and also information systems handling personal data falling under Articles 10 or 27 of Regulation (EC) No 45/2001.

4. Security Roles and Responsibilities

The Executive Director of EIOPA

4.1 The Executive Director of EIOPA is responsible for the overall supervision of security related activities.

4.2 The Governance & Organisation Team on behalf of the Executive Director coordinates activities throughout EIOPA, ensuring that suitable policies are in place to support the security principles.

Local Security Officer (LSO)

4.3 The LSO is responsible for the development, implementation, monitoring and review of the general security principles and requirements. The LSO promotes security awareness within EIOPA and acts as the main point of contact on general security issues.

Local Informatics Security Officer (LISO)

4.4 The LISO, by having particular expertise in the IT domain, is responsible for the security related aspects of the communication and information systems.

[8] *The levels of integrity and availability (MODERATE, CRITICAL, STRATEGIC) are defined by the EIOPA-MB-14/034 from 10 June 2014*

Heads of Departments and Units / Team Coordinators

4.5 Heads of Departments and Units / Team Coordinators are responsible for the day-to-day implementation of the security requirements within their area of responsibility. They should ensure that security requirements and mechanisms are properly applied and used by authorised persons under their coordination.

EIOPA Staff

4.6 All EIOPA Staff and other parties referred under 2.6 are responsible for complying with the principles set by the security policy, procedures and working instructions where relevant to their activities. They are responsible for maintaining the security of sensitive information they originated or entrusted to them.

5. Breaches of security and compromises of sensitive information

5.1 A prompt identification of attempted or successful breaches of security or compromises of sensitive information should be maintained.

5.2 All suspected breaches of security require immediate reporting to the hierarchy, the Local Security Officer and, when necessary, the Data Protection Officer, for establishing the facts and taking corrective measures for preventing a recurrence.

6. Final provisions

6.1 The EIOPA Security Policy is reviewed periodically, at least annually. The policy revision process aims at ensuring that the policy is in line with international standards and technology advancements, as well as the organisational structure.

6.2 EIOPA regularly verifies compliance with this policy through audit, review, testing, technical monitoring and enforcement or any other means deemed appropriate.

6.3 The EIOPA Security Policy is complemented with specific procedures, working instructions and guidelines that ensure the proper implementation of this policy.

6.4 The above policy is without prejudice of the application of Regulation (EC) No 1049/2001, Regulation 45/2001 and Regulation (EEC) No 354/83.

7. References

Legal and Regulatory Framework (EC Decisions and Implementing Rules)

- Commission Decision 2001/844/EC, ECSC, Euratom on Information Security (dealing mainly with EU Classified Information)
- Commission Decision C(2006)3602 on Security of Information Systems, the Implementing Rules and the supporting Standards and Guidelines
- Commission Decision 2007/65/EC on Alert States and Crisis Management
- Security Notices (SN), European Commission HR.DS
- Council Decision 2011/292/EU on the security rules for protecting EU classified information
- Regulation (EC) No 45/2001 on data protection; Regulation 45/2001 and Regulation (EEC) No 354/83
- Regulation (EC) No 1049/2001 of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents

Related EIOPA Decisions, Policies and Internal Procedures

- Decision of the Management Board of EIOPA concerning the Protection of Information Systems and Information (EIOPA-MB-14/034 from 10 June 2014)
- Decision of the Management Board of EIOPA concerning public access to documents (EIOPA MB 11/051 from 31 May 2011)
- Decision of the Management Board on implementing rules relating to Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (as amended)
- EIOPA Business Continuity Strategy (EIOPA-GO-14/007)
- EIOPA Business Continuity Business Impact Analysis (EIOPA-GO-14/006)
- EIOPA Decisions - Adoption of implementing rules to Staff Regulations by analogy (EIOPA-MB-14/004, EIOPA-MB-14/018)