fli
Leibniz-Institut
für Alternsforschung –
Fritz-Lipmann-Institut e.V.

Guideline on Information Security

1. Objective / Motivation

Information technology has become one of the most important tools for a modern institute. The degree of digital networking and the ability to process data have a crucial influence on the work at the institute. For a research institute, it is essential that information guarantees a high level of integrity to ensure that research data is both reproducible and verifiable. To ensure the quality and security of information at the Leibniz Institute on Aging - Fritz Lipmann Institute (FLI), the FLI's Information Security Guideline (ISG) stipulates binding principles regarding information security. This guideline explicitly serves as the basis for the information security management system (ISMS) and its central protection goals for information processing and archiving systems. The central objectives of the ISMS are:

- **Availability** (ensuring that information, applications and IT systems are available for authorized individuals to the extent intended and within a reasonable period of time),
- **Confidentiality** (ensuring that information is only accessible to authorized individuals) and
- **Integrity** (Ensuring that the authenticity and completeness of information, applications and IT systems are given and verifiable)

of all existing information of the institute

To ensure the availability, confidentiality and integrity of data and information systems, suitable measures must be presented and implemented on the basis of risk assessments in a security concept. In particular, these measures include technical, organizational and infrastructural precautions.

2. Scope

This guideline applies to all organizational units (OU) of the FLI. Included are digital information, the devices processing the information, as well as analog media (e.g. printouts), which may also contain information worthy of protection.

3. Responsibilities

An adequate level of safety can only be achieved and maintained with a planned and organized approach by all parties involved. Therefore, all employees must ensure information security through their responsible actions and comply with the regulations relevant to information security (laws, regulations, guidelines, company constitutional agreements, organizational regulations, contractual obligations, and the like).
FLI staff members are made aware of the applicable security rules in the context of information security in the form of trainings and briefings held by either the Information Security Officer (ISO) respectively the Data Protection Officer (DPO). In this context, the obligation to report the officers safety incidents should be emphasized. The respective OU is responsible for the

communication of specific rules within the group. All employees must attend the safety courses regularly.
Security concepts are drawn up in collaboration between the ISO and the DPO, in consultation with the board of directors or the head of the respective OU. Each OU is responsible for the security of its own data insofar as it is stored and processed outside of approved security concepts. The Board of Directors takes overall responsibility for information security and appoints a DSO to implement the security objectives.

4. Information Security Officer (ISO)

The ISO has an independent, organizationally prominent position and reports directly to the board of directors. She/he coordinates the general information security process and supports the Executive Board in its work. Additional tasks of the ISO are:

- Coordination of information security goals of the FLI with the board of directors.
- Advising the board of directors and other organizational units on information security issues.
- Coordination and planning of information security in cooperation with the IT. departments of the FLI and the DPO of the FLI
- Verification of compliance with all IT security regulations of the FLI.
- Investigating incidents affecting information security and determination of appropriate measures to prevent such incidents from occurring.
- Drafting and updating guidelines and regulations on information security at the FLI.
- Participation / advice within the scope of the Compliance Management System (CMS) of the FLI.
- Performance or initiation of security checks at external service providers of the FLI
- Documentation of information security measures at the FLI.
- Organization and implementation of training courses for employees with regard to information security and contact persons for them.
- Planning and conception of the management of "incidents" as well as emergency preparedness (including emergency plan / manual).

The ISO reports annually as well as in urgent matters to the Board of Directors, providing information on the current risk assessment, actions taken and planned, and past incidents.

5. Security strategy

The FLI operates an ISMS in accordance with BSI basic protection and within it follows the PDCA (plan-do-check-act) cycle. This process essentially describes the phases of planning – implementing – reviewing – acting and includes, in particular, the continuous improvement of the safety concept. In order to protect all relevant business processes with fundamental measures, the Institute pursues basic protection within the framework of the BSI (Federal Office for Security in Information Technology) basic protection.

Therefore, the ISO must be involved by the OU at an early stage in all organizational-technical changes or modifications that might affect information security.
For the implementation of the ISMS, personnel and financial resources are provided to the extent necessary in order to ensure an appropriate level of information security in the processing of information requiring protection. Security measures must be economically justifiable in relation to the damage that may otherwise result from security incidents.

6. Entry into force

This Guideline on Information Security shall enter into force on 1.12.2021 and replaces the previous guideline from 27.02.2013. It will remain valid until a new guideline is finalized.

Appendix

A1. Abbreviations

Abbreviation	Description
BSI	Federal Office for Security in Information Technology
DPO	Data Protection Officer
FLI	Leibniz Institute on Aging – Fritz-Lipmann-Institute
ISG	Information Security Guideline
ISO	Information Security Officer
ISMS	Information Security Management System
OU	Organizational Unit
PDCA-Zyklus	Plan-Do-Check-Act Zyklus