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

Leitlinie Informationssicherheit

1. Zielsetzung / Motivation

Die Informationstechnik hat sich zu einem der wichtigsten Arbeitsmittel für ein modernes Institut entwickelt. So beeinflussen der Grad der digitalen Vernetzung und die Verarbeitungsmöglichkeit von Daten entscheidend die Arbeit am Institut mit. Für ein Forschungsinstitut ist es insbesondere von Bedeutung, dass Informationen eine hohe Integrität garantieren um zu gewährleisten, dass Forschungsdaten reproduzierbar und überprüfbar sind. Um die Qualität und Sicherheit der Informationen am Leibniz-Institut für Alternsforschung – Fritz-Lipmann-Institut (FLI) sicherzustellen, legt die Informationssicherheitsleitlinie (IS-LL) des FLI verbindliche Prinzipien der Informationssicherheit fest. Explizit wird mit dieser Leitlinie die Grundlage für das Informationssicherheitsmanagementsystem (ISMS) und dessen zentrale Schutzziele für informationsverarbeitende und -archivierende Systeme geschaffen. Die zentralen Ziele des ISMS sind:

- **Verfügbarkeit** (Gewährleistung, dass Informationen, Anwendungen und IT-Systeme für Berechtigte im vorgesehenen Umfang und in angemessener Zeit nutzbar sind),
- **Vertraulichkeit** (Gewährleistung, dass Informationen ausschließlich Berechtigten zugänglich sind), und
- **Integrität** (Gewährleistung, dass die Unverfälschtheit und Vollständigkeit von Informationen, Anwendungen und IT-Systemen gegeben und überprüfbar sind)

aller vorhandenen Informationen des Instituts

Zur Wahrung von Verfügbarkeit, Vertraulichkeit und Integrität von Daten und Informationssystemen sind - auf der Basis von Risikoeinschätzungen - geeignete Maßnahmen in einem Sicherheitskonzept darzustellen und umzusetzen. Insbesondere beinhalten diese Maßnahmen technische, organisatorische und infrastrukturelle Vorkehrungen.

2. Geltungsbereich

Diese Leitlinie gilt für alle Organisationseinheiten (OE) des FLI. Einbezogen sind digitale Informationen, die Geräte, mit denen die Informationen verarbeitet werden sowie analoge Medien (z.B. Ausdrucke), die ebenfalls schützenswerte Informationen enthalten können.

3. Zuständigkeiten

Ein angemessenes Sicherheitsniveau kann nur durch ein geplantes und organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Deshalb haben alle Beschäftigten die Informationssicherheit durch ihr verantwortliches Handeln zu gewährleisten und die für die

Informationssicherheit relevanten Regelwerke (Gesetze, Verordnungen, Richtlinien, betriebsverfassungsrechtliche Vereinbarungen, organisatorische Regelungen, vertragliche Verpflichtungen u.ä.) einzuhalten.
Die Mitarbeiter*innen des FLI werden mittels Schulungen und Unterweisungen durch die/den Informationssicherheits- bzw. den Datenschutzbeauftragten auf geltende Sicherheitsregeln im Rahmen der Informationssicherheit hingewiesen. Dabei ist die Meldepflicht an die Beauftragten bei Sicherheitsvorkommnissen hervorzuheben. Die zugehörige OE übernimmt die Übermittlung von spezifischen Regeln innerhalb der Gruppe. Alle Mitarbeiter*innen müssen regelmäßig an den angebotenen Sicherheitsschulungen teilnehmen.
Die Erstellung von Sicherheitskonzepten erfolgt in Zusammenarbeit zwischen dem Informationssicherheitsbeauftragten (ISB) und dem Datenschutzbeauftragen (DSB), im Benehmen mit dem Vorstand bzw. dem Leiter der jeweiligen OE. Jede OE des FLI ist für die Sicherheit der eigenen Daten verantwortlich, sofern diese außerhalb von beschlossenen Sicherheitskonzepten gespeichert und verarbeitet werden.
Der Vorstand trägt die Gesamtverantwortung für die Informationssicherheit und benennt zur Umsetzung der Sicherheitsziele eine/n Informationssicherheitsbeauftragte/n.

4. Informationssicherheitsbeauftragte/r (ISB)

Die/der ISB besitzt eine unabhängige, organisatorisch herausgehobene Stellung, ist direkt dem Vorstand unterstellt und berichten diesem. Sie/Er koordiniert den übergreifenden Informationssicherheitsprozess und unterstützt den Vorstand in dessen Arbeit. Weitere Aufgaben der/des ISB sind:

- Abstimmung von Informationssicherheitszielen des FLI mit dem Vorstand
- Beratung des Vorstandes und anderer OE in Fragen der Informationssicherheit
- Koordinierung und Planung der Informationssicherheit in Kooperation mit dem IT-Bereichen des FLI und dem Betrieblichen Datenschutzbeauftragten (BDSB) des FLI
- Überprüfung der Einhaltung aller IT-Sicherheitsregelungen des FLI
- Untersuchung von Vorfällen, die die Informationssicherheit beeinträchtigen und Festlegung geeigneter Maßnahmen zur Vermeidung solcher Vorfälle.
- Erstellung sowie Pflege von Richtlinien und Regelungen zur Informationssicherheit am FLI
- Beteiligung/ Beratung im Rahmen des Compliance Management System (CMS) des FLI
- Durchführung bzw. Veranlassung von Sicherheitsüberprüfungen bei externen Dienstleistern des FLI
- Dokumentation der Informationssicherheitsmaßnahmen am FLI
- Organisation und Durchführung von Schulungen der Beschäftigten bzgl. Informationssicherheit und Ansprechpartner für diese
- Planung und Konzeption des Managements von „Vorfällen“ („Incidents“) sowie der Notfallvorsorge (inkl. Notfallplan/-handbuch)

Die/der ISB erstattet dem Vorstand jährlich sowie in dringenden Angelegenheiten Bericht und informiert über die aktuelle Gefahrenlage, getroffene und geplante Maßnahmen, sowie vergangene Vorkommnisse.

5. Sicherheitsstrategie

Das FLI betreibt ein ISMS nach dem BSI-Grundschutz (Bundesamt für Sicherheit in der Informationstechnik) und folgt darin dem PDCA-Zyklus (plan-do-check-act). Dieser Prozess beschreibt im Kern die Phasen *Planen – Umsetzen – Überprüfen – Handeln* und beinhaltet insbesondere die fortlaufende Verbesserung des Sicherheitskonzepts. Um alle relevanten Geschäftsprozesse mit Maßnahmen abzusichern, verfolgt das Institut im Rahmen des BSI-Grundschutzes die Basis-Absicherung.
Dafür ist die/der Informationssicherheitsbeauftragte bei allen organisatorisch-technischen Neuerungen oder Änderungen, die Auswirkungen auf die Informationssicherheit haben könnten, durch die OE frühzeitig einzubinden.
Für die Umsetzung des ISMS werden im erforderlichen Rahmen Personal- und Finanzmittel bereitgestellt, um ein angemessenes Informationssicherheitsniveau bei der Verarbeitung schützenswerter Informationen sicherzustellen. Die Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der anderenfalls durch Sicherheitsvorfälle verursacht werden kann.

6. Inkrafttreten

Diese Leitlinie zur Informationssicherheit tritt am 1.12.2021 in Kraft und ersetzt die bisherige Leitlinie vom 27.02.2013. Sie behält ihre Gültigkeit bis zum Abschluss einer neuen Leitlinie.

Der Vorstand

Anhang

A1. Abkürzungen

Abkürzung	Beschreibung
BSI	Bundesamt für Sicherheit in der Informationstechnik
DSB	Datenschutzbeauftragte/r
FLI	Leibniz-Institut für Alternsforschung – Fritz-Lipmann-Institut
IS-LL	Informationssicherheitsleitlinie
ISB	Informationssicherheitsbeauftragte/r
ISMS	Informationssicherheitsmanagementsystem
OE	Organisationseinheiten
PDCA-Zyklus	Plan-Do-Check-Act Zyklus