Information Security Policy

1. Purpose

The purpose of the Information Security Policy is to prevent information security incidents or minimize the risk of damage in order to ensure Mobile Health AG's business continuity and reduce the impact of potential threats.

In this context, the Information Security Management System has been established and it is aimed to comply with the ISO 27001:2022 standard.

2. Scope

This policy covers information assets within Mobile Health AG. It is applied by employees at all locations, in and out of location suppliers/contractors.

3. Responsibility

The Information Security Management Board is responsible for ensuring the installation and operation of the Information Security Management System in accordance with the ISO 27001:2022 standard, which will ensure that the confidentiality, integrity and accessibility values of the company's information assets are protected within the scope of the scope and that the risks to the processes are kept at an acceptable level approved by the senior management. These responsibilities also include ensuring that the Information Security Management System meets the requirements of the General Data Protection Regulation (GDPR).

4. Information Security Requirements

A clear definition of the information security requirements within Mobile Health AG is agreed and maintained with the internal business so that all ISMS activities are focused on the fulfillment of these requirements. Legal, regulatory and contractual requirements are also documented and included in the planning process. Specific requirements for the security of new or modified systems or services are recorded as part of the design phase of each project.

It is a fundamental principle of the Mobile Health AG Information Security Management System that the controls implemented are driven by business needs and this is regularly communicated to all staff through team meetings and briefing documents.

5. Framework for Setting Objectives

A regular cycle is used to set information security objectives to coincide with the budget planning cycle. These objectives are based on a clear understanding of the business requirements, informed by the management review process where relevant parties are consulted. Information security objectives are documented for an agreed period of time, with details of how they will be achieved. These are assessed and monitored as part of management reviews to ensure they remain valid. If changes are required, these are managed through the change management process.

6. Continuous Improvement of ISMS

- Mobile Health AG's policy on continuous improvement
- To continuously improve the effectiveness of ISMS
- Improve existing processes to align them with good practices defined in ISO/IEC 27001 and related standards
- Maintain ISO/IEC 27001 certification on an ongoing basis
- Increasing the level of proactivity (and stakeholders' perception of proactivity) regarding information security
- Make information security processes and controls more measurable to provide a sound basis for informed decisions
- Review on an annual basis to assess whether it is appropriate to modify relevant metrics based on historical data collected
- Gather ideas for improvement through regular meetings and other forms of communication with interested parties
- Review improvement ideas at regular management meetings to prioritize and assess timelines and benefits

Ideas for improvement can come from any source, including employees, customers, suppliers, IT staff, risk assessments, and service reports. Once identified, they are recorded and considered as part of management reviews.

7. Information security policy areas

Mobile Health AG defines policies in a wide variety of areas related to information security, which are detailed in a comprehensive set of policy documents that accompany this overarching information security policy.

Each of these policies is defined and agreed upon by one or more individuals with competence in the relevant field and, once formally approved, is communicated to an appropriate audience both internally and externally.

8. Implementation of information security policy

This Information Security Policy and supporting policies have been reviewed and approved by senior management of Mobile Health AG. The Information Security Policy has been communicated to relevant parties and employees. Failure by an employee to comply with these policies may result in disciplinary action by the organization's Employee Disciplinary Process.