MINDLER

Information Security Policy

Mindler AB

2025-04-11

PART 1: INTRODUCTION

1.1. Mindler AB, with organisation number 559150-0722 (hereafter defined as “we,” “us,” or “Mindler”), is a mental healthcare provider which develops, manages, and operates digital solutions for web-based assessments, investigations, and treatments of patients.

1.2. This information security policy encompasses our commitment and strategy of working with information security with goal to protect Mindler information systems and data integrity, availability and confidentiality.

PART 2: TERMS AND DEFINITIONS

2.1. Within this document, the following definitions apply:

- **Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.
- **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed
- **Availability** means that authorised users are able to access personal data when they need it for authorised purposes.
- **Traceability** is a characteristic of information or information systems on how important it is to trace who has interacted with the information and what has been done with it.
- **Information Security** - the act of preserving the confidentiality, integrity, and availability of information and information systems.

- **Information Security Management System (ISMS)** - the overall management process that includes the planning, implementation, maintenance, review, and improvement of information security.

PART 3: SCOPE

3.1. This policy is applicable to all of Mindler's employees, contractors, and others who work on behalf of Mindler when managing information at Mindler, regardless of communication form. This policy shall constitute the foundation of Mindler's information security work and implementation.

3.2. All subordinate policies and controls adhere to this policy and are contained within Mindler's information security management environment and can be made available as specific documents where required.

3.3. The policies within the ISMS environment and overarching system linked to the environment demonstrate a commitment to satisfy the applicable requirements and continual improvement of the management system.

PART 4: PURPOSE AND AMBITION

4.1. As a digital healthcare provider, we are committed to holding ourselves to a high standard to protect and secure all information managed or owned by us. We strive to continuously and on a long-term basis work with information security to ensure that information supervised by us maintains its integrity and trust.

4.2. Information at Mindler should be managed so that it is confidential, accessible, traceable, and maintains integrity at any given moment and insofar as it is deemed necessary and appropriate in regard to the information's value and risks. Our routines regarding information security should continuously be maintained and updated so that it is protected in line with our vision and goals as well as legal regulations and requirements.

PART 5: ROLES AND RESPONSIBILITIES

5.1. Mindler's board of directors shall stipulate the information security policy that is applicable to the company. In addition, Mindler's Board of Directors shall be responsible for establishing and updating this policy as well as all relevant documentation on Mindler's information security work.

5.2. Mindler's Compliance Manager (CM) shall be responsible for implementing the information security work within the company, following this policy, guidelines, and other relevant documentation. The CM shall also ensure that Mindler's employees and personnel who work on behalf of Mindler are updated on the latest information security routines at Mindler.

5.3. All personnel at Mindler have a responsibility to uphold the integrity of information security. Defects or faults that threaten our information security should always be handled and communicated according to the appropriate policies, guidelines, or other relevant documentation.

PART 6: AVAILABILITY

6.1. This policy is available at https://mindler.se/informationsecuritypolicy. A physical copy of this policy shall always be available at Mindler's headquarters:

Mindler AB,
559150-0722
Hovslagargatan 3,
111 48 Stockholm

PART 7: POLICY REVISION

7.1. Revision of this policy shall occur at least once a year from the date of signing or at the earlier date for which it is required. Policies, guidelines and other relevant information security documentation derived from this policy shall be revised at least once (1) every year or at the earlier date for which it is required.

Revision history

Document Information			
Document Name	Information Security Policy		
Information Classification	Public		
Approved by	CEO		
Document Owner	CM/DCEO		
Revision Interval	Annually		
Revision History			
Author	**Change**	**Date**	**Version**
Kenny Chung	V. 3 draft	2021-05-17	3.0
Mindler Board	Approval	2021-11-24	3.0
Krista Ehrnrooth	Review	2022-08-18	4.0
Anders Myhre	Review	2022-09-14	4.0
Krim Talia	Approval	2022-11-08	4.0
Krista Ehrnrooth	Review	2023-04-17	4.1
Matilda Wernérus	Review	2023-04-27	4.1
Krim Talia	Approval	2023-04-28	4.1
Krista Ehrnrooth	Review	2024-04-08	4.2
Erica Larson	Approval	2024-04-08	4.2
Krista Ehrnrooth	Review	2025-04-10	4.3
Erica Larson	Approval	2025-04-11	4.3