deepcloud

INFORMATION SECURITY POLICY

ISMS MANAGER
DEEPCLOUD AG
Wittenbach

ID: DC021
Version: 1.1
Date: 30.10.2023

Classification level: C1 - Public

DOCUMENT CONTROL SECTION

Change Log

Date	Version	Status (draft/to be review)	Author	Description
27.8.2021	1.0	Final	CEO/ISMS Manager	First version
8.9.2021	1.1	Approved	ISMS Manager	Updated introduction and minor semantic changes (not relevant to the content)

Revision and Approval

Date	Version	Revision/Approval	Revisional/Approver	Note
8.9.2021	1.1	Approval	CEO	
10.10.2022	1.1	Revision	ISMS Manager	Review of document, no changes made
30.10.2023	1.1	Revision	ISMS Manager	Minor corrections, not relevant to the content

REFERENCE EXTERNAL DOCUMENTS

Date	Version	Doc ID	Name and Description	Filename/Link

REFERENCE INTERNAL DOCUMENTS

Date	Version	Doc ID	Name and Description	Filename/Link

DISTRIBUTION LIST

Date	Name	Role
20.9.2021	Public	-

1. Table of Contents

2. INTRODUCTION

DeepCloud AG (hereinafter "the Company") deems the protection of the data and the organizational structure (technological and physical) as a primary objective for the security of information and has therefore implemented an Information Security Management System (hereinafter "ISMS") that is designed to be always up to date, adhering to the defined scope and compliant to the following properties:

1. **Confidentiality**, ensure that information is only accessible to duly authorized subjects and/or processes
2. **Integrity**, protect the consistency of information from unauthorized changes
3. **Availability**, ensure that authorized users have access to information when they require it
4. **Control**, ensure that data management takes place through secure and tested processes and tools
5. **Authenticity**, ensure a reliable source of information
6. **Privacy**, guarantee the protection and control of personal data

The services offered by the Company, through its technological infrastructure, are guaranteed by the security levels implemented in the ISMS, which encompass:

- A reliable system for information management
- The utmost care for the corporate image
- The full compliance with the Service Level Agreements established with customers
- The customers satisfaction
- The compliance with current regulations and international security standards

The ISMS implemented within the Company complies with the requirements specified by the ISO/IEC 27001:2013 standard and information security relevant laws in the context of its business.

3. SCOPE

This Information Security Policy applies to all internal staff and third parties which play a role in the management of information and to all processes and resources involved in the design, implementation, start-up and continuous provision of company services.

4. INSPIRING PRINCIPLES

The meaning of security for the Company is broad and includes the loss of tangible or intangible assets such as information, as well as risks related to its business continuity. The implemented ISMS has been designed to both identify and prevent such risks at an early stage.

The added value of the information security policy adopted by the Company derives from its ability to act before a harmful event occurs. This is possible because every member of the organization acts with common sense and applies its seniority to strive towards the achievement of a high level of efficiency and effectiveness in information security management. Knowledge of the rules of information security, combined with a proactive personal attitude (systematically applied to day-to-day work) make the results of this company commitment recognizable and tangible.

The information security policy of the Company is inspired by the following principles:

- To guarantee the full knowledge of the managed information and the assessment of its criticality by the organization, in order to facilitate the implementation of adequate levels of protection
- To ensure rightful and secure access to information, in order to prevent unauthorized processing

- To ensure that the organization and third parties collaborate in the processing of information by adopting procedures aimed at respecting adequate levels of security
- To ensure that the organization and third parties involved in the processing of information are fully aware of security issues
- To ensure that anomalies and incidents affecting the information system and corporate security are promptly recognized and correctly managed through efficient prevention, communication and reaction systems in order to minimize the impact on the business
- To ensure that access to offices and individual company premises is made exclusively by authorized personnel, to guarantee the security of the areas and relevant assets
- To ensure the compliance with legal requirements and compliance with the security commitments established in the agreements with third parties
- To ensure the detection of anomalous events, incidents and vulnerabilities of information systems in order to increase the security and availability of services and information
- To guarantee the Business Continuity and the Disaster Recovery, through the application of established safety procedures

The information security policy is formalized in the ISMS, is constantly updated to ensure its continuous improvement and is shared with the organization, third parties and customers through the proper communication channels.

5. OBJECTIVES

In accordance with the above principles, the Company defines the following objectives that must be pursued in all business processes:

- To manage information security defining adequate targets, providing suitable resources, preparing specific security policies and procedures to be implemented in the individual departments, always ensuring full compliance with legal and regulatory requirements
- To communicate information security policies, objectives and targets so that there is real sharing and unity of purpose on the behaviors to be adopted
- To minimize the risk conditions and prevent vulnerabilities that expose people, assets and business to threats also guaranteeing corporate standards and objectives, the competitiveness, the brand and the company image
- To involve all employees and suppliers through information, education and training actions aimed at increasing knowledge, competence and awareness of information security aspects both in the management of daily activities and in case of incidents that may compromise business continuity
- To guarantee a prompt return to normal operations in the event of emergencies and crises, limiting damages and losses, protecting people and company assets
- To monitor internal processes to constantly review the adequacy of the system and identify possible improvement actions
- To improve the ISMS to align it with changing global, business and regulatory requirements

The stated principles and defined objectives are an integral part of the daily activities of the Company.

6. RESPONSIBILITY OF INFORMATION SECURITY POLICY

The Management is responsible for ensuring that the ISMS is always up to date, in line with the evolution of the business and market context, evaluating any action to be taken in relation to:

- Significant business developments
- New threats compared to those considered in the risk analysis activity
- Relevant security incidents
- Changes in the regulatory or legislative context regarding the secure processing of information

The responsibility to protect the people and the company resources belongs to the organization. All those who manage, operate and exercise control over corporate processes must guarantee an adequate level of protection using the tools and resources made available by the Company.

The managers of each function and department must therefore ensure that this Information Security Policy is understood and implemented by all the employees and the involved suppliers.