PS ISMS Policy

Document Status

Document Name	PS ISMS Policy
Description	The ISMS Policy outlines Cloudflight's commitment to safeguarding information assets by ensuring their confidentiality, integrity, and availability. It serves as the guiding framework for all security practices, ensuring alignment with business goals, legal, regulatory, and organizational requirements.
Information Owner	Aaron Winkler
Creation Date	15 Apr 2025
Revision	1.0
ISO/IEC 27001	5 Leadership 5.1 Leadership and commitment 5.2 Policy
ISO/IEC 27002	5 Organizational Controls 5.1 Policies for information security 5.36 Compliance with policies, rules, and standards for information security 5.4 Management Responsibilities
Approving Roles	CEO & CFO
Release Date	25 Apr 2025
Signed Document	
Classification	Internal

- Implementation and Performance Review

Preamble

At Cloudflight, we are committed to maintaining the highest standards of information security. Our management ensures that security is deeply integrated into all aspects of our operations, reflecting our core competencies and our dedication to protecting sensitive data.

Information security is an ongoing process, adapting to emerging threats and evolving technologies. We align our practices with the core principles of confidentiality, integrity, and availability (CIA), in support of Cloudflight's broader business goals.

This policy is for internal use only, with disclosures managed by management. To ensure continued effectiveness, the policy will be reviewed regularly to stay aligned with industry standards and Cloudflight's needs.

Together, we work to safeguard our information and maintain a secure environment for everyone at Cloudflight.

Introduction

Scope and Application of the ISMS Policy

This policy applies to all employees, partners, and service providers who interact with the organization's information systems and data. It encompasses all physical, technical, and organizational measures required to ensure information security.

Approval and Update Procedures

This information security policy is approved by Cloudflight's top management, which is accountable for the ISMS. Cloudflight's Information Security Officer (ISO) is responsible for its update and maintenance while considering the internal regulations on document control.

Information Security Objectives and Principles

Information Security Objectives

Cloudflight's Information Security Objectives are founded on the three fundamental protection goals:

- **Confidentiality**
- **Integrity**
- **Availability**

By aligning these protection goals with the requirements of our interested parties, we establish a consistent thread throughout our entire **Customer Application Lifecycle Management (CALM)** – spanning Design, Build, and Operate. This ensures that every phase of our software development and operational activities adheres to our highest information security standards.

Confidentiality

Objective: Ensure that sensitive information is accessible only to authorized individuals:

- **Design:**
  - Securely handle proprietary source code, design documents, and customer data from the outset.
- **Build:**
  - Protect development environments, code repositories, and testing systems against unauthorized access.
- **Operate:**
  - Enforce continuous monitoring and access management for live systems and operational data.

Stakeholder Alignment:
This approach satisfies customer, regulatory, and management requirements by ensuring that contractual and legal obligations regarding information privacy and protection are met throughout the entire CALM.

Integrity

Objective: Maintain the accuracy, consistency, and trustworthiness of information and software components:

- **Design:**

    - Verify detailed specifications and architectural plans to prevent errors that could compromise data integrity.
- **Build:**
    - Integrate automated testing, code reviews, and version control systems.
- **Operate:**
    - Continuously monitor production systems.
    - Employ integrity checks and logging mechanisms.

Stakeholder Alignment:
By ensuring the reliability and consistency of our software and data, we preserve trust and compliance — addressing the expectations of customers, regulators, and management.

Availability

Objective: Guarantee that IT systems and information remain accessible and fully operational when needed by authorized users:

- **Design:**
    - Embed availability requirements from the start by planning for scalable and redundant architectures.
    - Consider fault tolerance and resource allocation during system design.
- **Build:**
    - Construct robust IT components — including development platforms and integration systems — with features like load balancing and efficient backup processes.
    - Ensure that systems are built to withstand operational stresses.
- **Operate:**
    - Maintain continuous monitoring, proactive incident management, and effective disaster recovery strategies.
    - Regularly test recovery plans and system resilience.

Stakeholder Alignment:
This comprehensive approach meets the expectations of both customers and internal management by providing uninterrupted service and ensuring operational resilience—crucial for business continuity and digital transformation initiatives.

At Cloudflight, these objectives are not treated as standalone targets but are interwoven into every stage of our CALM:

- **Design:**
    - Security requirements drive the initial planning and architecture.
- **Build:**
    - Secure coding practices, rigorous testing, and controlled development environments.
- **Operate:**
    - Continuous monitoring, redundancy, and proactive incident management ensure that our IT components remain available and resilient.

Information Security Management

An information security management system (ISMS) is used for the development, introduction, operation, and further development of Cloudflight's information security capabilities to ensure that relevant information security objectives are met. It is adequately equipped by the top management and supported with the necessary resources. The ISMS specifies the tools and methods utilized to comprehensibly guide, monitor, implement and improve the tasks and activities within the information security. The desired level of information security can only be achieved if the ISMS is implemented holistically. This overarching nature of information security results in the need to define the key roles of stakeholders in relation to information security within Cloudflight. Key stakeholders include:

- the workforce,
- the legislative body,
- the project partners and customers.

Other interested parties are documented in the interested parties document and the context of the ISMS. Only with the help of an ISMS, it can be guaranteed that all important aspects and requirements are taken into account and that all tasks are carried out efficiently and effectively. This is subject to a continuous process within Cloudflight to continuously review the implemented strategies and concepts for their performance and effectiveness.

Information Security Management System

Cloudflight's ISMS is based on the ISO/IEC 27001 standard. The ISMS itself, as well as the implemented information security processes and measures in it, apply to all users who interact with the organization's information systems and data. The core of the ISMS is therefore the PDCA cycle. With the help of this cycle, Cloudflight is able to initiate the management system in a structured manner (PLAN), to implement and operate it in compliance with the standard (DO), to monitor it continuously (CHECK) and to implement continuous improvements (ACT).

Roles and Responsibilities

An information security organization is established to achieve the information security objectives. All employees are obligated to understand and comply with information security requirements.

In order to meet the requirements and information security objectives, Cloudflight’s information security management is composed by several roles. In the following section the central roles are listed in brief.

Top Management

The top management consists of the "CEO" and the "CFO".

The top management is accountable for implementing the requirements of the ISMS. It provides the necessary resources (including finances, infrastructure, personnel, etc.) while considering economical aspects. The top management keeps the overall accountability for information security. It initiates and directs overarching activities, ensures the necessary priority and attention for information security issues is given. The top management supports other roles within the ISMS organization.

Information Security Officer (ISO)

The management has established the role "Information Security Officer (ISO)" for the implementation of information security and assigned the task of drawing up uniform specifications for the information security process, ensuring that all employees are sufficiently sensitized, and appropriately checking compliance with all security guidelines or having them checked to this role.

The ISO is responsible for the technical management, independent monitoring function and methodological authority of the ISMS. The person in the role of ISO has the competence to define further roles and responsibilities in the ISMS and to assign them in coordination with the respective technical or disciplinary superiors. Furthermore, the person in charge establishes management processes for planning, implementation and operation, evaluation of performance, continuous updating and improvement of the ISMS.

Implementation and Performance Review

The responsible roles for this regulate the enforcement of the requirements of information security policy. Improvements achieved through the implementation of an ISMS are reviewed in frequent intervals. The information security objectives defined in the information security are considered in this review. Accordingly, it must be checked whether the general conditions with regard to information security have changed and whether the defined security objectives are still appropriate. If necessary, updates are made in order to achieve a continuous improvement of the ISMS. The top management obtains information on the status of the ISMS at least once a year within dedicated management reviews.

The information security policies are fully communicated within Cloudflight so that the principles and objectives of the information security policies are understood and lived by every stakeholder. The policies will be provided to external stakeholder upon request.

The information security policies within Cloudflight are binding. Violations of the information security guidelines are documented and, if necessary, appropriately addressed by disciplinary actions.