Information security objectives and principles

OWNER	CEO
REVIEW FREQUENCY	ANUALLY
LAST UPDATE/REVIEW	13/11/2023
DOCUMENT NAME	Circeo_Information_security_objectives_and_principles
CLASSIFICATION	INTERNAL PUBLIC

VERSION	2.4

Contents

Revision history

VERSION	DATE	DESCRIPTION	AUTHOR/EDITOR	APPROVED BY
0.1	16/04/2019	Template	Andras Vegh	
0.2	24/04/2019	Draft - Added elements to exclusions based on SOA documents	Attila Temesvari	
1.0	25/04/2019	Initial version - Changed the definition in the scope from branch to company	Matthieu M. Job	Matthieu M. Job
1.1	15/08/2019	- Removed exclusions to reflect current version of SOA	Attila Temesvari	Matthieu M. Job

1.2	09/10/2019	- Modified scope according to the agreement done on the opening meeting of ISO 27001 audit	Attila Temesvari	Matthieu M. Job
2.0	29/07/2020	- Moved document to general document format	Attila Temesvari	
2.1	04/08/2020	- Updated objectives list	Attila Temesvari	Matthieu M. Job
2.2	20/07/2021	- Updated objectives list and modified the educational objective to include measured efficiency	Attila Temesvari	Matthieu M. Job
2.3	29/09/2022	- Updated the Objectives with adding endpoint protection for TheLoanFactory Updated the Objectives with adding a suitable differentiation method for external and internal emails	Peter Farkas	Matthieu M. Job
2.4	13/11/2023	Moved to the new document template Added Chapter 6.1	Peter Farkas	Matthieu M. Job

1. Terminology, meaning, interpretation

ISMS – Information security management system.

SOA – Statement of applicability document.

2. Purpose of document

Circeo is committed to providing its services to the satisfaction of its customers in a high-level information security environment. In line with its mission Circeo has developed and implemented an Information Security Management System (ISMS) in compliance with the ISO 27001:2013 standard which enables us to:

- Manage information security assets in an organized way that facilitates continual improvement and adjustment to organizational goals.
- Assess and treat information security risks in accordance with our particular needs.
- Demonstrate commitment and compliance to global best practice.
- Compliance with regulations, legislation, and industry mandates.
- Demonstrate to customers, suppliers, and stakeholders that security is paramount to the way we operate.
- Better secure all financial and confidential data, so minimising the likelihood of it being accessed illegally or without permission.

3. Scope of the ISMS

Our Information Security Management System (ISMS) applies to the control of the entire business, premises, and resources of Circeo Zrt.

Our core processes that are subject to this information security management system:

- **Security in software development and maintenance, application operation and support related to TheLoanFactory complete end-to-end loan management solution in accordance with the Statement of Applicability,**

Circeo determined the external and internal issues, interested parties and the requirements of these interested parties (including legal and regulatory requirements and contractual obligations) that are relevant to the information security management system established (see: *ISMS Inventory of Interested Parties*).

4. Leadership

The Management demonstrates leadership and commitment to achieving the objectives of our ISMS by taking accountability for the effectiveness of our ISMS and ensuring that:

- An Information Security Policy and Information Security Objectives are established for the management system and that they are compatible with our strategic direction and context.
- Our ISMS requirements are integrated into our business processes as appropriate.
- Our ISMS is suitably resourced.

- There is clear communication on the importance of effective information security management and of conforming to the management system requirements.
- Our ISMS achieves its intended results.
- All personnel are encouraged to contribute to the effectiveness of the management system.
- Continual improvement is actively promoted.
- Our information security policies, objectives and targets are, where appropriate, reflected in individual responsibilities and performance objectives.

5. Information security principles

To ensure the confidentiality, integrity, and availability of our data, we intend to evolve the following information security principles:

- **Risk proportionality:** When designing and developing the information security system, we apply the principle of risk proportionality, so the protection measure is always proportional to the values to be protected. The implementation of the directive is based on our risk management methodology by regular risk analysis on information assets.
- **Comprehensiveness:** Information security is extended to all resources, processes, and all life cycles (development, test, deployment, operation, termination). We keep our information asset records up to date, define information security requirements, and regularly review their performance.
- **Least Privilege & Need to know:** Principle of necessary and sufficient access. The levels of access to data are clearly defined so that employees have access to all the data absolutely necessary for their work. It is particularly important that employees have only the necessary privileges in every case, not having access to information that is not strictly related to their job. Access requests are granted through multi-level approval, reviewed regularly by data owners. Access is changed or revoked accordingly when an employee's role changes or leaves the company.
- **Accountability:** Access to the resources of the electronic information system is provided in a clearly identifiable way. All activities are being logged and the monitoring of changes is prioritized in our development activities.

The following fundamental principles also contribute to the successful implementation of an ISMS:

- Awareness of the need for information security;
- Assignment of responsibility for information security;
- Incorporating management commitment and the interests of stakeholders;
- Risk assessments determining appropriate controls to reach acceptable levels of risk;
- Security incorporated as an essential element of information networks and systems;

- Active prevention and detection of information security incidents;
- Ensuring a comprehensive approach to information security management;
- Continual reassessment of information security and making of modifications as appropriate.

6. Objectives

In accordance with the overall strategy and business objectives of Circeo, the following general Information security objectives can be identified:

- To ensure the ISMS is effectively protecting the organization's information assets on an ongoing basis, it is necessary that the PDCA (Plan-Do-Check-Act) cycle gets continually repeated to identify changes in risks or in the organization's strategies or business objectives.
- To ensure that risks are reduced to an acceptable level by risk treatment plan and by implementation a control system.
- Our objectives to monitor, evaluate and improve the efficiency and effectiveness of information security controls to support Circeo's aims. The selection and implementation of controls are documented within a statement of applicability to assist with compliance requirements.
- The aim of continual improvement of an ISMS is to increase the probability of achieving objectives concerning the preservation of the confidentiality, availability, and integrity of information. The focus of continual improvement is seeking solutions for better and more efficient security.
- The proper implementation of ISMS ensures compliance with success factors resulting in improved incident management capabilities, while exact test criteria list makes business continuity process more effective.
- Effective and measured information security awareness, training, and education programme, informing all employees and other relevant parties of their information security obligations set forth in the information security policies, standards, etc., and motivating them to act accordingly.
- Inquire the most suitable endpoint protection solution from the market with central management to improve high level visibility on malware and virus infection attempts.
- Inquire the most suitable endpoint protection solution to verify all file transfers going through the TheLoanFactory application including the uploaded documents, configuration files and any other file transfers are scanned for virus.
- Integrate state of the art security solutions (Web Application Firewall, Transparent Data Encryption) into the product to make it more robust in the security area and more appealing to existing and prospective customers.

- Adopt the latest hosting solutions offered in the cloud space developed specifically for financial institutions, the main clients of Circeo (IBM Financial Services Cloud),and have it as a selectable option for new clients.
- Review and modify the Information Security Management System in order to be able to onboard external resources into the company aiding rapid growth requirements and ensuring continued high quality and secure client support
- Suitable differentiation of external and internal emails to provide an increased level of awareness against phishing attempts

According to our Customer's expectation and our own business goals, Circeo is committed to maintain its ISO 27001 certification acquired in 2019 for the following periods.

6.1. Security objectives for the year

The following concrete security objectives were identified which were derived from the 2023-24 business goals:

- Implement the FS Cloud architecture and offer it to our Customers
- Implement a DLP Solution
- Create a detailed Security Incident Response Plan and gradually create a Security Operations Center and the related process

7. Appendices