Information Security Policy

- ISP -

Creditro A/S
Sankt Annæ Plads 13
DK-1250 Copenhagen K
CVR: 39181169
Denmark

Purpose and Scope

This information security policy defines the purpose, principles, objectives and basic rules for information security management.
This document also defines procedures to implement high level information security protections within Creditro, including definitions, procedures, responsibilities and performance measures (metrics and reporting mechanisms).
This policy applies to all users of information systems within Creditro. This typically includes employees and contractors, as well as any external parties that come into contact with systems and information controlled by Creditro (hereinafter referred to as "users"). This policy must be made readily available to all users.

Background

This policy defines the high level objectives and implementation instructions for Creditro's information security program. It includes Creditro's information security objectives and requirements; such objectives and requirements are to be referenced when setting detailed information security policy for other areas of Creditro. This policy also defines management roles and responsibilities for Creditro's Information Security Management System (ISMS). Finally, this policy references all security controls implemented within Creditro.

Within this document, the following definitions apply:

- Confidentiality : a characteristic of information or information systems in which such information or systems are only available to authorized entities.
- Integrity : a characteristic of information or information systems in which such information or systems may only be changed by authorized entities, and in an approved manner.
- Availability : a characteristic of information or information systems in which such information or systems can be accessed by authorized entities whenever needed.
- 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.

Document version

Created by: MK
Approval: MK/RB

Date	Initials	Edit
16-03-2021	MK	Policy creation

Table of Contents

Policy

1. **Managing Information Security**
   - Creditro's main objectives for information security include the following:
     - Reduced risk of data breaches and compromises
     - Compliance with legal, regulatory, and contractual requirements.
     - Better market image

   - Creditro's objectives for information security are in line with Creditro's business objectives, strategy, and plans.

   - Objectives for individual security controls or groups of controls are proposed by the company management team, including but not limited to the CEO, the CTO, and others as appointed by the CEO; these security controls are approved by the CEO in accordance with the Risk Assessment Policy.

   - All objectives must be reviewed at least once per year.

   - The company will measure the fulfillment of all objectives. The measurement will be performed at least once per year. The results must be analyzed, evaluated, and reported to the management team.

2. Information Security Requirements

- This policy and the entire information security program must be compliant with legal and regulatory requirements as well as with contractual obligations relevant to Creditro.

- All employees, contractors, and other individuals subject to Creditro's information security policy must read and acknowledge all information security policies.

- The process of selecting information security controls and safeguards for Creditro is defined in our Encryption Policy .

- Creditro prescribes guidelines for remote workers as part of the Remote Access Policy.

- To counter the risk of unauthorized access, Creditro maintains a Data Center Security Policy.

- Security requirements for the software development life cycle, including system development, acquisition and maintenance are defined in the Software Development Lifecycle Policy .

- Security requirements for handling information security incidents are defined in the Security Incident Response Policy .
- Disaster recovery and business continuity management policy is defined in the Disaster Recovery Policy.

- Requirements for information system availability and redundancy are defined in the System Availability Policy.