Information security policy

ISO27001

Client:	**Adacta d.o.o**.
Project:	**Information Security Policy**
Document version:	**1.5**
Prepared by:	**Tatjana Rojc**
Confidentiality Level:	**Public**
Place & Date:	**Ljubljana, 28h August 2024**

Content

Tables

Figures

Document History

Date	Author	Version	Description
2.9.2019	Gašper Mozetič	1.0	First version
4.11.2021	Tatjana Rojc	1.1	Company name and logo change, design update.
10.10.2022	Tatjana Rojc	1.2	Company information Update
19.11.2023	Tatjana Rojc	1.3	Controls of the ISO/IEC 27001 standard update
30.11.2023	Tatjana Rojc	1.4	Controls of the ISO/IEC 27001:2022
28.08.2024	Tatjana Rojc	1.5	Controls of the ISO/IEC 27001 standard update based on regulatory requirements

Confidentially note

Levels of confidentiality

Information	
Confidential	Defined by ADACTA's Management
Restricted	For individual Department Only (IT procedures, HR procedures, Personal Data)
Internal use only	For employees Only (QMS and ISMS Documents for Internal Use, Internal Acts)
Customer use	Customer use – Project and Contract documentation

1 Introduction

With offices in six countries and more than 180 insurance experts, Adacta grew to become one of the leading software providers for the insurance industry in CEE.

Formed in 1989, the company spent decades helping insurance organisations to grow their digital capabilities and has more than 20 AdInsure implementations in 9 different countries. With over 30 years of experience in consulting, software development and implementation services, Adacta shows a steady organic growth and 18,6 M EUR revenue in 2020.

Adacta offers consultation and implementation services that get insurers off to the best possible start with AdInsure, Adacta's insurance platform for Life and Non-Life insurers.

Adacta collects, stores, and handles a wide range of information regarding existing customers, potential customers, vendors and employees. This type of information are either confidential – commercially sensitive, proprietary or otherwise confidential information - or publicly available data. Some of commercially sensitive information include, but are not limited to financial terms of the deal, work obligations, operational data, cost and expenditures information and employee information. The confidentiality of sensitive business information is established through non-disclosure agreements (one-way or two-way) or through confidentiality agreements.

Clients, regulators, management, employees and contractual workers share Adacta information (see Figure 1 – Organisations originating and sharing Adacta information).

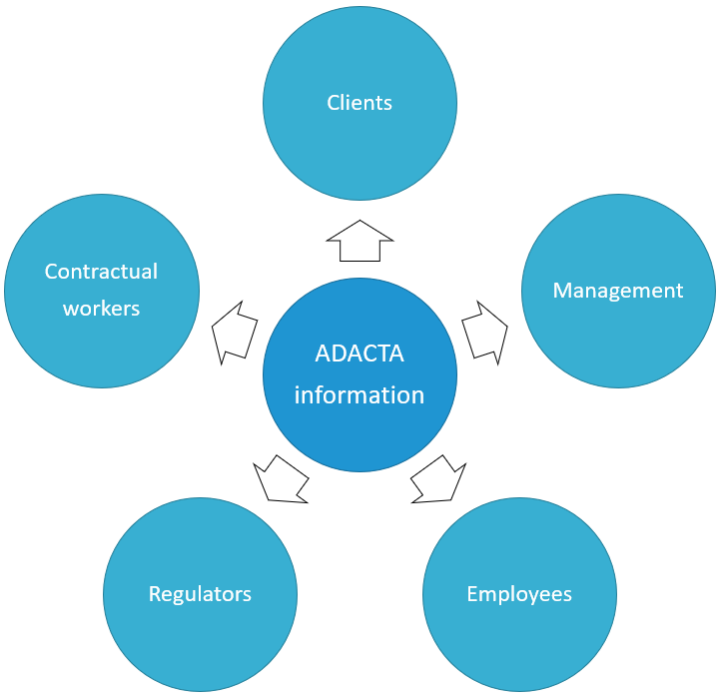

Figure 1Organization's originating and sharing ADACTA information.

This information security policy is aimed at ensuring

- Confidentiality
- Integrity and
- Availability

of information and underlying assets against threats, whether internal or external, deliberate, or accidental.

2 Policy Scope

All processes, activities and assets are within the scope of this information security policy, especially:

1. Implementation and maintenance of information systems
2. Secure development
3. Intellectual property and sales / contractual information protection
4. Human resources security
5. Data and information exchange procedures and interfaces with regulatory authorities, contractual workers, clients, and other relevant parties.

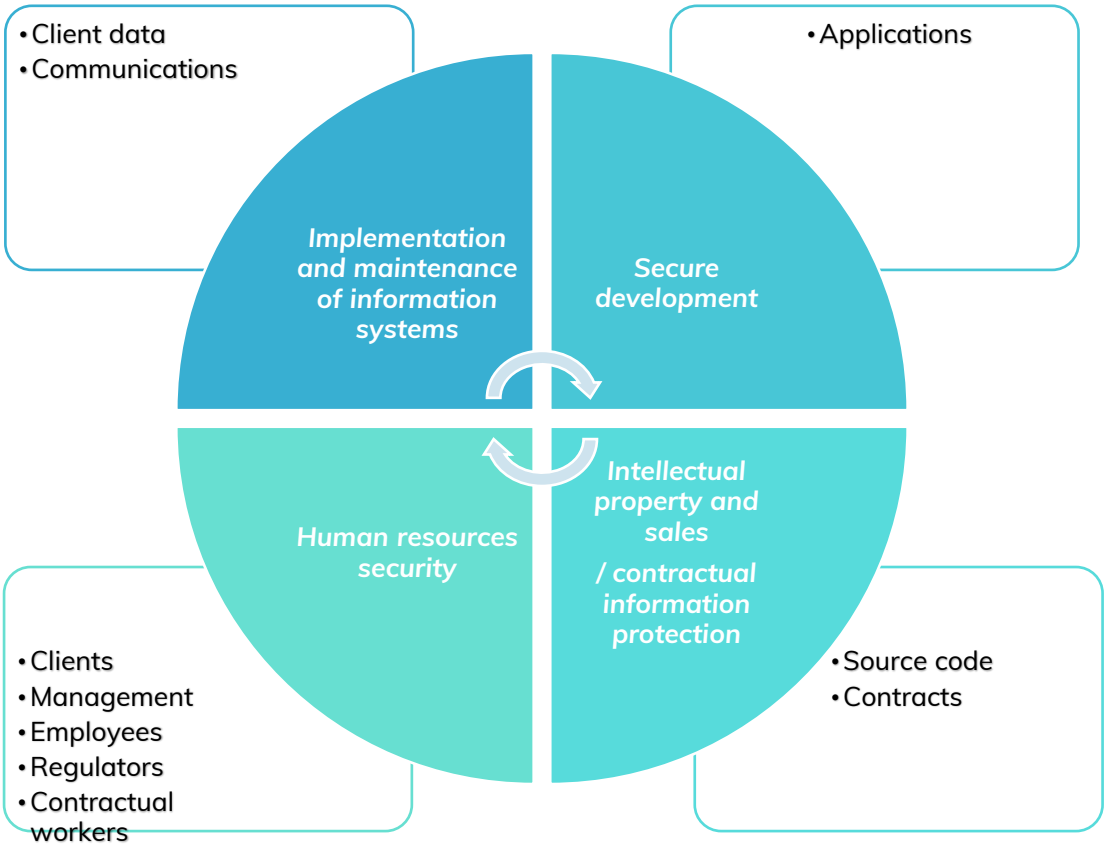

Figure 2ADACTA information.

3 Structure of the Information Security Policy

Table 1 Documentation of the ADACTA information security framework

External documents	Internal documents	Records
Legislation	Information security policy	
Contracts	Policies and procedures	Reports
Orders	Process documentation	Logs
Standards	Forms	

Processes

The Information Security Management System (ISMS) includes all aspects of information security that are presented in the information security policies within 4 pillars of controls:

Organizational controls:

- Information security policies

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

- Organization of information security

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

- Information security incident management

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

- Information security aspects of business continuity management

Objective: Information security continuity shall be embedded in the organization's BCM systems.

- Compliance

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

People Controls:

- Human resource security

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

- Supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

Physical controls:

- Physical and environmental security

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

Technical controls:

- Asset management

Objective: To identify organizational assets and define appropriate protection responsibilities.

- Access control

Objective: To limit access to information and information processing facilities.

- Cryptography

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information

- Operations security

Objective: To ensure correct and secure operations of information processing facilities.

- Communications security

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

- System acquisition, development and maintenance

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

4 Basic Principles

1. ADACTA manages the Information Security Management System (hereafter ISMS). The ISMS is a set of policies, procedures, guidelines and associated resources and activities, managed by ADACTA with the purpose to protect information assets in scope of this policy.
2. Managers at all levels are responsible for the implementation of the Information Security policy and for ensuring staff adherence to the policy and guidelines.
3. All employees and contractual workers are, according to their functions and authorities, responsible for abiding the Information Security Policy.
4. The approach to ADACTA information security is risk-oriented and conforms to international standards and established good practices.
5. ADACTA information in all forms is protected coherently and commensurately, from its source, through ADACTA, to its recipients.
6. Security measures are effective and consistent.
7. The ADACTA Information Security Management System follows ISO/IEC 27002 Code of practice for information security management and ISO 27005 Information security risk management and also aims to satisfy ISO/IEC 27001 Information Security Management SystemsRequirements.
8. An information security awareness and education program is established to provide stakeholders sufficient training to perform their responsibilities.
9. Deviations from this Information Security Policy and any security breaches must be reported to the ISMS Officer of ADACTA.

5 ANNEX:

5.1 List of ADACTA Information Security Procedures

- Risk management
- IT Asset management
- Information management
- Access management
- System development life cycle
- Change management
- Log management
- IT Support management
- Teleworking
- Cryptography
- HR Management
- Physical security
- Business continuity management
- Incident management
- Security Awareness Training Policy

5.2 Definition of Terms and Acronyms

Table 2 Always put table title above the table. Format this table title using the CAPTION style.

Term	Description
Information	Knowledge or data that has value to the organization or third party.
Asset	An asset is a resource with economic value that an organization owns or controls with the expectation that it will provide future benefit
Data group	Unit of information required to be controlled and maintained by an organization and the medium on which it is contained
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Integrity	Property of accuracy and completeness.
Availability	Property of being accessible and usable upon demand by an authorized entity.

5.3 Policy Applicability

Referring to the structure of policy documents, the basic principles and requirements laid out in policies that are part of the information security framework are binding for ADACTA and all organizations originating and sharing ADACTA information.

The Information security framework is defined by a set of security policies. Each policy is structured as follows:

- Introduction
  - Scope
- Applicability
- Definition of terms and acronyms
- Basic principles
- References
  - Responsibilities
  - Requirements
  - Implementation guidance

Basic principles and requirements laid down in each policy are applicable to the collecting, storing, processing and sharing of information in all processes, activities and assets within the scope.

Any implementation guidance is intended to assist in meeting the requirements and is binding for ADACTA . Some requirements in the implementation guidance are presented in tables according to sensitivity marking level.

5.4 Responsibilities

In each information security policy responsibilities are described in a table defining the requirements and the responsible, accountable, consulted or informed (RACI) roles.

Table 3 Described responsibilities

R	Refers to the person who must ensure that activities are completed successfully.
A	The person that is ultimately responsible for a subject matter, process or scope.
C	Refers to the person whose opinion is sought on an activity (two-way communication).
I	Refers to the person who is kept up to date on the progress of an activity (one-way-communication).