Accounting Solutions

INFORMATION SECURITY POLICY

Code:	SP04001
Version:	0.7
Date of version:	23/08/2022
Created by:	Vassilis Mataios
Approved by:	Managing Partner
Confidentiality level:	Internal

Change history

Date	Version	Created by	Description of change
01/10/2013	0.1	Vassilis Mataios	Basic document outline
28/11/2013	0.2	Vassilis Mataios	Adaptation to Accounting Solutions Requirements
30/04/2014	0.3	Vassilis Mataios	Finalization of document structure
31/10/2017	0.4	Anastasios Pantazis	Change Logo
11/3/2020	0.5	Vassilis Mataios	Reviewed and validated
01/09/2021	0.6	Vassilis Mataios	Reviewed and validated
23/08/2022	0.7	Vassilis Mataios	Reviewed and validated
11/07/2023	0.8	Vassilis Mataios	Reviewed and validated

Table of contents

1. Purpose, scope and users

The aim of this top-level Policy is to define the purpose, direction, principles and basic rules for information security management.

This Policy is applied to the entire Information Security Management System (ISMS), as defined in the ISMS Scope Document.

Users of this document are all employees of Accounting Solutions, as well as relevant external parties.

2. Reference documents

- ISO/IEC 27001 standard, clauses 5.2 and 5.3
- ISMS Scope Document
- Risk Assessment and Risk Treatment Methodology
- Statement of Applicability
- List of Legal, Regulatory and Contractual Obligations
- Business Continuity Policy
- Incident Management Procedure

3. Basic information security terminology

Confidentiality – characteristic of the information by which it is available only to authorized persons or systems.

Integrity – characteristic of the information by which it is changed only by authorized persons or systems in an allowed way.

Availability – characteristic of the information by which it can be accessed by authorized persons when it is needed.

Information security – preservation of confidentiality, integrity and availability of information.

Information Security Management System – part of overall management processes that takes care of planning, implementing, maintaining, reviewing, and improving the information security.

4. Managing the information security

4.1. Objectives and measurement

General objectives for the information security management system are the following: creating a better market image and reducing the damage caused by potential incidents, conformity with regulations/legislation and ISO 27001 security requirements, goals are in line with the organization's

business objectives, strategy and business plans. Security Manager is responsible for reviewing these general ISMS objectives and setting new ones.

Objectives for individual security controls or groups of controls are proposed by department Managers and IT Manager and approved by Managing Partner in the Statement of Applicability.

All the objectives must be reviewed at least once a year.

Accounting Solutions will measure the fulfillment of all the objectives. Security Manager is responsible for setting the method for measuring the achievement of the objectives – the measurement will be performed at least once a year and Security Manager will analyze and evaluate the measurement results and report them to Managing Partner as input materials for the Management review.

4.2. Information security requirements

This Policy and the entire ISMS must be compliant with legal and regulatory requirements relevant to the organization in the field of information security and data protection, as well as with contractual obligations.

A detailed list of all contractual and legal requirements is provided in the List of Legal, Regulatory and Contractual Obligations.

4.3. Information security controls

The process of selecting the controls (safeguards) is defined in the Risk Assessment and Risk Treatment Methodology.

The selected controls and their implementation status are listed in the Statement of Applicability.

4.4. Business continuity

Business continuity management is prescribed in the Business Continuity Management Policy.

4.5. Responsibilities

Responsibilities for the ISMS are the following:

- Security Manager is responsible for ensuring that the ISMS is implemented and maintained according to this Policy, and for ensuring all necessary resources are available
- Security Manager is responsible for operational coordination of the ISMS as well as for reporting about the performance of the ISMS
- Security Manager must review the ISMS at least once a year or each time a significant change occurs, and prepare minutes from that meeting. The purpose of the management review is to establish the suitability, adequacy and effectiveness of the ISMS.
- Security Manager will implement information security training and awareness programs for employees
- the protection of integrity, availability, and confidentiality of assets is the responsibility of the owner of each asset

- All security incidents or weaknesses must be reported to Security Manager.
- Security Manager will define which information related to information security will be communicated to which interested party (both internal and external), by whom and when
- HR Manager is responsible for adopting and implementing the Training and Awareness Plan, which applies to all persons who have a role in information security management

4.6. Policy communication

Security Manager has to ensure that all employees of Accounting Solutions, as well as appropriate external parties are familiar with this Policy.

5. Support for ISMS implementation

Hereby the Security Manager declares that ISMS implementation and continual improvement will be supported with adequate resources in order to achieve all objectives set in this Policy, as well as satisfy all identified requirements.

6. Validity and document management

This document is valid as of 01/07/2014.

The owner of this document is Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- number of employees and external parties who have a role in the ISMS, but are not familiar with this document
- non-compliance of the ISMS with the laws and regulations, contractual obligations, and other internal documents of the organization
- ineffectiveness of ISMS implementation and maintenance
- unclear responsibilities for ISMS implementation

Managing Partner
Vangelis Fakos

_____