ISMS-PO-00 Information Security Policy

Document Information

Classification:	Internal
Title:	ISMS-PO-00 Information Security Policy
Version:	2.10
Status:	Final
Date:	23/08/2024

History

Version	Date	Author	Changes	Checked by	Approved by
0.1	04/05/2022	Dr. Theodoros Ntouskas	Draft		
1.00	24/05/2022	Dr. Theodoros Ntouskas	Final Version		
2.00	05/09/2022	Dr. Theodoros Ntouskas	Updated Version		
2.10	23/08/2024	Dr. Theodoros Ntouskas	Updated Version	Spyros Psomadelis	Spyros Psomadelis

Table of Contents

1 Introduction

1.1 Purpose of the document

This document is ELTRAK's Information Security Policy. The basic security principles for this policy are addressed, and a summary of the main points of all ELTRAK security policies and procedures are provided.

ELTRAK must provide the necessary means for the proper implementation of the ISMS within the ISMS scope.

1.2 Reference documents /records

#	Title	Type
1	All Company Information Security Policies and Procedures	Policy/Procedure
2	All the records that are mentioned in this policy	Records

1.3 Glossary of Terms

At the following table the main definitions and acronyms referred to this document are depicted.

Table 1: Glossary of terms

Term	Description
Assets	Information systems, computer hardware, applications, infrastructures, information and data.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
Availability	Ensuring timely and reliable access to and use of information.
Breach	An event that affects one or more of the following features: authenticity, availability, confidentiality, integrity, validity.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Term	Description
Cryptography	Use of a crypto-algorithm program by a computer to authenticate or encrypt/decrypt information.
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
Information security	Preservation of Confidentiality, Integrity and availability of information as well as of authenticity, accountability, non-repudiation and reliability
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Security	The structured framework of concepts, principles, procedures, techniques and measures required to protect both the Information System elements and the entire Information System from accidental or deliberate threat.
Integrity	The property that data has not been modified or deleted in an unauthorized and undetected manner.
Non- repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities
Partner, Contracted Party	Entities, companies, organizations or individuals with whom they have been, are, or will be labor contractual relationships.
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring
Risk Analysis	Process to comprehend the nature of risk and to determine the level of risk
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation

Term	Description
Security Countermeasure	A measure designed to prevent a violation, reduce a weakness-vulnerability or reduce potential impact.
Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Threat	Any circumstance or event that may cause the loss of one or more security principles (i.e., Confidentiality, Integrity, Availability) of an information asset.
Validity	Absolute accuracy and completeness of information.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

2 Information Security Policy

2.1 Objective

The objective of this policy is to ensure business continuity and to minimize the risk of damage by preventing security incidents and reducing their potential impact on ELTRAK.

2.2 Scope

This policy applies to all ELTRAK systems, people and processes, including board members, directors, employees, contractors and other third parties who have access to ELTRAK information systems.

2.3 Policy

ELTRAK has adopted the *Information Security Policy* and is committed for the effective implementation and provision of resources for the improvement of the Information Security Management System (ISMS).

- The Information Security Policy aims to ensure:
  - Continuous protection of information against unauthorized access.
  - Continuously ensuring the confidentiality of ELTRAK's information, clients and partners.
  - Continuously maintaining the integrity of ELTRAK's information, clients and partners.
  - Continuous assurance of the availability of information and business transactions.
  - Monitoring and compliance with the legislative and regulatory requirements concerning ELTRAK.
  - The *Business Continuity Plan* is maintained and tested for its effectiveness.
  - Adequate training of the ELTRAK employees in information security issues.
  - Confirmed or suspected information security breaches are reported to the Information Security Officer and are thoroughly investigated and dealt in time and effectively.
- Appropriate procedures and individual security policies are in place to support the policy, including technical and organizational measures of protection.
- Compliance with the legislation and requirements of ISO 27001: 2022 is ensured and with the ongoing monitoring of the implementation of the ISMS.
- The Information Security Officer is responsible for maintaining the Information Security Policy and for providing support and advice in its implementation.
- ELTRAK's top management is responsible for the implementation of the *Information Security Policy* as well as for ensuring the compliance of the supervised personnel.
- Compliance with the *Information Security Policy* is mandatory for all parties that have been or are cooperating with ELTRAK.
- Any violations of the *Information Security Policy* are subject to disciplinary actions. The decision depends on the nature and impact of the violation.

3 Management of communications and procedures

3.1 Operational procedures and obligations

Operational procedures are used for the maintenance of ELTRAK's information systems and infrastructures in order to ensure the maximum possible utilization of its assets.

Possible changes to the ELTRAK's Information Systems are controlled by the *ISMS-PR-15 Change Management Procedure*.

Software and application development and testing environments are separate from the active production environments, to reduce the risk of accidental changes as well as unauthorized access to data.

All major changes to the basic infrastructure (e.g., network, servers) should be considered for the impact they may have on the security of ELTRAK information.

Software development and testing environments are separated using appropriate controls, including:

- Running software on different computers, different domain and network domains.
- Use different usernames and passwords.
- Assigning tasks to those who have access to information systems for both control and categorization of the functions that they can access.

3.2 Use of email

Email is a vital tool for communication both internally and with clients and suppliers.

The *ISMS-PO-07 Email Policy* sets the basic rules for the proper use of the email, as well as the permitted actions of the authorized users. The policy applies for every use of the service, regardless of the device or the location (e.g., by smartphone or outside office).

3.3 Use of internet

The goal of the *ISMS-PO-10 Internet Acceptable Use Policy* is to direct all users about:

- Expected practices at work.
- highlighting issues that affect the use of the internet.
- a description of the standards that users must adopt.
- recording the necessary actions to monitor the implementation of the policy.
- alerting users of the consequences of misuse of the internet.

Internet infrastructures are available for the purposes of the ELTRAK operational procedures. Since it is not possible to lay down clear rules covering all available online activities, compliance with them should be integrated in the overall spirit of the policy in order to ensure that the use of the service is sufficiently productive.

The *ISMS-PO-10 Internet Acceptable Use Policy* must be applied every time the Internet service is used. This includes access through any device such as desktops or smartphones.

3.4 Systems design

Information systems and facilities are covered by a needs forecasting plan (see *ISMS-PR-15 Change Management Procedure*) and by equipment replacement procedures that ensure that increased power and data storage requirements can be addressed and met in acceptable time.

ELTRAK users must inform the Information Security Officer for information security issues, new requests or upgrades, service packs, or patches required for the existing systems.

New products must be procured through the prescribed legal procedures. New information systems, product upgrades, and software fixes must undergo proper control prior to their acceptance and availability in the production environment (see *ISMS-PR-12 Secure Development Procedure*).

The selection criteria must be clearly identified, pre-agreed and documented, as well as approved by ELTRAK.

Third-party applications must be tested for possible service packs, as well as for individual patches.

Major upgrades of information systems need to be thoroughly tested in a safe test environment, as a copy of the production system.

3.5 Protection against malicious code

All appropriate measures must be taken to protect information systems, infrastructures and information against malicious code.

There must be effective and up-to-date malware protection software on all servers and computers. To prevent malware and / or portable malware, appropriate access controls (e.g., administrator / user access rights) must be implemented to prevent unauthorized software installation by users.

Some types of malicious code use technologies that include (but are not limited to) ActiveX, Java, JavaScript, VBScript, Macros, HTTPS, HTML.

ELTRAK staff must not introduce malicious code into the information systems of the company.

If an ELTRAK employee detects a virus in an information system, he/she should immediately notify the Information Security Officer.

All servers must have upgrades / patches that are critical to system security as soon as they become available.

The patches must be installed in the software of the entire ELTRAK network.

Requests for installing new software are only accepted if there is adequate technical verification for them.

3.6 Backups

Regular backups of key business information are regularly taken to ensure that ELTRAK can recover from a disaster, digital media failure or the consequences of a human error.

A suitable backup cycle, which is well documented (*ISMS-PO-03 Backup Policy* and *ISMS-PR-13 Backup Procedure*), is in place.

Anyone who stores information must ensure that it is backed up.

A full backup is stored in a location outside the main storage location of the information systems. This location is selected so as not to be affected by a catastrophic event (e.g., fire) that is likely to take place in the main building.

3.7 Storage media management

The categories of storage media covered by this procedure include the following:

- Laptops.
- CDs /DVDs.
- USB memory sticks.
- External portable drives.
- Mobile phones.

Removable media (such as USBs, discs and printed documents) must be protected to prevent damage, theft or unauthorized access.

Storage media that are transported must be protected against unauthorized access, abuse, or intrusion of the data they store.

Documentation of the information systems must be protected against unauthorized access. These include documents created by ELTRAK or another user of the information systems (not including the manuals that accompany the software).

There are documented procedures regarding the backups that need to be recovered from ELTRAK buildings.

The backup media is kept in a safe environment.

3.8 Monitoring

Log entries contain at least the following information for each event, where available:

- User ID
- Event date and time
- system identity (e.g., name and/or IP address)
- Event-related information (message or code)

- Event success or failure indication.

Logs that record security-related exclusions and events are kept for at least six (6) months as required by the relevant legislation (see *ISMS-PO-11 Logging and Monitoring Policy*).

Access to logs is protected against unauthorized access.

It is forbidden for system administrators to delete or disable logs of their own activities.

Where necessary, classified data must be kept separate from non-classified.

System administrators must keep a record of (and) their own activities.

Log must include (see *ISMS-PO-11 Logging and Monitoring Policy*):

- Backup times, along with details of how to change your backup media.
- The boot and shutdown events of any system and any user involved.
- System errors (type, date, time), along with corrective actions.

Records must be checked regularly to ensure that the necessary procedures are followed.

Computer clocks are synchronized to ensure the accuracy of the system logs.

3.9 Network management

Proper network management is vital for providing services.

Connections to ELTRAK's network infrastructure are made in a controlled manner.

Wireless networks apply data protection controls that pass through them, as well as prevent unauthorized access.

There are clear responsibilities and procedures for remote access to ELTRAK Information Systems.

The network architecture is recorded and stored along with the hardware and software settings that compose the network.

The network equipment is recorded in the *Asset Inventory*.

At regular intervals (at least once a year), the software is tested, and any unnecessary programs and services are terminated.

ELTRAK's wireless network implements encryption techniques for the data it handles. The WPA-2 wireless network protocol is used.

3.10 System development and maintenance

Personal data that may be used when developing and testing software must be protected. Access to them must be controlled in accordance with the data protection legislation.

Where feasible, data must be used depersonalized.

If data are being processed during the development or testing of ELTRAK software, then specific measures must be implemented, including:

- Licensing process.
- Removal of all operational data from the test system after use.
- Complete recording of all related activities.
- Any personal or confidential information must be protected as if it were data in use by an active-productive information system.

3.11 Annual vulnerability assessment

At least once a year, a vulnerability assessment of information systems must be carried out. Vulnerability assessment should include the following:

- Systematic penetration tests.
- Scan the network, locate and record all addressable devices.
- Network Analysis, including vulnerable switches and gateways.
- Analysis of vulnerabilities, patches, vulnerable access codes, and network services.
- Analysis of exploitation of vulnerabilities.

4 Information systems infrastructure

4.1 Secure areas

The Risk Assessment determines the appropriate level of protection that needs to be in place to adequately safeguard the data stored on the ELTRAK premises.

The *Physical and Environmental Security Policy* sets out the protection measures that need to be taken to create a safe space and explains how one should take care of it, so that this space remains safe.

In the event of a security incident (see *ISMS-PR-05 Incident Management Procedure*) or if a staff member leaves ELTRAK without following the appropriate procedure of the job termination, the system passwords, as well as the alarm codes, must be changed immediately.

4.2 Safety of documents and equipment

Any confidential documents are stored in secure (locked) cabinets. Only authorized ELTRAK employees have access to them.

Documents kept at offices accessible to all staff and / or external visitors must be protected by physical access control measures, including:

- Locked cabinets and keys stored away from the drawer.
- Safe areas protected (e.g., locked file room).

Computer equipment must be in appropriate physical locations to:

- Limit environmental risks (e.g., heat, fire, smoke, water, dust, etc.).
- The risk of theft is reduced.
- Limit the risk of unauthorized people seeing information on monitor screens.

4.3 Equipment life cycle management

ELTRAK and its suppliers must ensure that the equipment of the information systems is maintained in accordance with the manufacturer's instructions and in accordance with documented internal procedures to ensure that it remains in good condition.

5 Information systems access

5.1 General

User passwords in the information changed regularly, according to the *ISMS-PO-02 Access Control Policy* and the *ISMS-PO-14 Password Policy* or whenever the software explicitly requests a user to change the password.

Access to ELTRAK’s information systems is protected through the following security measures (the list is indicative):

- Each user has a username and password.
- The use of shared accounts is forbidden.
- Password retrieval process is protected.
- User access to information systems is monitored and recorded.
- Each user has roles in information systems that provide him / her with access according to his / her responsibilities.
- Passwords are not allowed to be exchanged between users.
- Procedures for the correct use of administrators' passwords are in place.

When an employee leaves ELTRAK, his access to information systems must be suspended upon completion of the last day of his work. It is the responsibility of the HR department to request the suspension of access rights through the Information Security Officer.

5.2 Access control to servers and software

Access to servers is controlled by a secure connection process that complies with the *ISMS-PO-02 Access Control Policy* and the *ISMS-PR-08 Access Control Procedure*.

Access to information systems is through a unique username that can be associated with a particular individual.

5.3 Suppliers/partners remote access

Remote access of suppliers/partners to ELTRAK's information systems is controlled (see *ISMS-PO-02 Access Control Policy* and *ISMS-PR-08 Access Control Procedure*).

Any changes in suppliers/partners’ connections must be notified immediately to the Information Security Officer, so that access can be controlled or interrupted.

All rights and methods of access are controlled by the Information Security Officer.

Suppliers/partners must contact the Information Security Officer before connecting to ELTRAK’s network. A record of their activity must be kept.

Any remote access software must be disabled when not in use.

6 Software

ELTRAK uses licensed software. ELTRAK does not accept the use of non-licensed software.

7 Compliance with personal data protection rules

ELTRAK must comply with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the protection of individuals with regard to the processing of personal data, the free movement of such data and the repeal of Directive 95/46 / EC (General Regulation on Data Protection) and the legislation for the personal data protection (Law 4624/2019).

Legal Team is responsible to ensure that all requirements from applicable legislation are communicated to the Information Security Officer.

Additionally, an Employees Privacy Policy is in place in order to inform ELTRAK employees for the protection of their personal data.

The Information Security Officer and Legal Team are responsible for reviewing the policies and procedures in order to achieve compliance with the regulatory requirements.

8 Disciplinary Procedure

It must be ensured that security policies and procedures are respected by all users and partners of ELTRAK.

The disciplinary procedure is triggered in the event of an information security breach and after the conduction of a full investigation. This investigation is documented.

This disciplinary procedure ensures fair treatment of employees taking into account the following factors:

- the nature of the breach.
- the effect of the breach on ELTRAK.
- the training received by the employee (quality and quantity of training).
- if the employee has committed a security breach in the past.
- relevant legal factors.

9 Control of Policy

The ELTRAK Information Security Officer and/or Internal Auditor carries out audits at regular intervals (at least once a year) to ensure that this policy is fully followed.