University of Cyprus

Registry .cy

Information Security Policy

Version: 1.1

Date of Issue: February 07, 2024

__ATTENTION:__ This document is classified as Public Domain Public
If you are not duly authorized, you should avoid reading, copying, distributing and transmitting its contents.

Contents

1. Introduction-Purpose

This document defines the high-level policy for information security management for the Registry .cy.

The Registry .cy is committed to safeguarding the information systems on which it depends in order to provide services internally and externally. For this reason, this high-level Information Security Management Policy has been devised and agreed upon.

The Registry .cy considers information as a valuable asset of the utmost importance, which is protected in order to ensure the provision of reliable services to stakeholders.

Furthermore, the Registry .cy addresses information security as an ongoing practice, which involves the implementation of the necessary procedures and security safeguards to protect the information of the Registry .cy from potential risks that may adversely affect the operations of the Registry .cy.

This Information Security Policy sets out the .cy Registry's approach to information security management. The objective of this high-level policy is to provide a framework, describing the purpose, guiding principles and responsibilities, for safeguarding the security of the .cy Registry's information systems.

This policy applies to the entire Information Security Management System (ISMS). The users of this document are all .cy Registry employees and related external parties within the scope of the ISMS.

In this light, the Registry .cy has adopted an Information Security Management System consisting of information security policies and procedures for effective risk management. This is aligned with the ISO/IEC 27001:2013 standard.

2. Scope

This policy applies to the entire .cy Registry, including:

- All operational locations and functions,
- All information stored or processed by the Registry .cy (including information provided to the Registry .cy by customers, business partners, and employees), regardless of the form in which it is stored or processed,
- All authorized users, either directly employed by the Registry .cy, or contracted to provide services to it and/or its customers.

Within the broad scope described above, this Policy establishes and authorizes an ISMS to be certified in accordance with ISO 27001:2013.

3. Terms and Definitions

Term	Definition
Availability	Refers to the property of information being accessible and usable by an authorized entity upon request
Confidentiality	Refers to the property of information not to be made available or disclosed to unauthorized persons, entities or processes
Integrity	It refers to the property of validity and completeness of information
IS	Information Security
ISMS	Information Security Management System
ISSC	Information Security Steering Committee
KPI	Key Performance Indicator

4. Information Security Policy Rules

Information can exist in many forms, printed on paper, stored electronically, transmitted by post or electronic means, in documents or through spoken word/conversation. The Registry .cy also relies heavily on computer systems and applications to store, process and manage business and customer information. Whatever form the information takes or the means by which it is communicated or stored, it is always properly protected. Information in any form is a valuable asset to the company and is treated accordingly.

Information security problems include information that is obtained, processed or disclosed inappropriately, modified or incorrectly validated, either intentionally, accidentally, or not available when required.

The Registry .cy considers information to be a valuable asset of the utmost importance that is protected in order to ensure the reliable provision of services to its customers. Therefore, it is the goal of the Registry .cy to protect its information through an ongoing practice of implementing and monitoring appropriate security safeguards to protect important information from potential risks that could adversely affect the business activities or reputation of the Registry .cy.

In this regard, the Registry .cy has adopted an Information Security Management System (ISMS) consisting of policies and procedures to effectively manage information security risks. The ISMS is in compliance with the requirements of ISO/IEC 27001:2013 standard.

5. Information Security Management

5.1 Management commitment

The .cy Registry Administration is committed to ensuring that:

- Confidentiality of information is protected to ensure that valuable or sensitive information is not disclosed.
- The integrity of the information is protected to ensure its accuracy and completeness.
- The availability of information is protected to meet the requirements of the .cy Registry and the requirements and expectations of stakeholders.

- Regulatory and legislative requirements related to the .cy Registry are met.
- Appropriate information security information is provided to all users falling within the scope of the .cy Registry ISMS.
- An incident management process is established and implemented to ensure that all information security breaches (actual or suspected) are reported and investigated.
- Risks are mitigated to an acceptable level through a risk management framework.
- The ISMS is continuously improved.
- Adequate resources are available for the implementation, operation and review of an effective ISMS.

5.2 Objectives and Metrics

The .cy Registry has envisioned its information security objectives to ensure that its related business activities continue to be conducted securely in accordance with the ISO 27001:2013 standard. The primary information security objectives are as follows:

1) Achieve and maintain compliance with ISO/IEC 27001:2013,
2) Demonstrate senior management support for information security,
3) Demonstrate Continuous Improvement,
4) Maintain employee awareness of information security issues,
5) Ensuring that adequate resources and capabilities are assigned to the ISMS,
6) Improving Third Party Security,
7) Ensuring effective reporting and management of security incidents,
8) Ensuring effective risk management.

Detailed information security objectives and associated metrics are documented as part of the ISMS objectives and effectiveness measurement.

5.3 Continuous Improvement

The Management of the Registry .cy is committed to the continuous improvement of the ISMS. Through continuous improvement, the effectiveness of the ISMS and security safeguards are maintained and improved. These processes are further described in the Continuous Improvement Framework document.

KPIs are developed and used to measure the effectiveness of the ISMS and the most appropriate safeguards.

As part of the management review of the ISMS, senior management ensures that recommendations for adjustment and improvement are provided by the Information Security Steering Committee.

As a result of the review, potential improvements to the ISMS are communicated to senior management.

6. Legal and Regulatory Requirements & Contractual Obligations

All relevant legislative and regulatory requirements, as well as contractual obligations, are appropirately identified and complied with.

7. Security in Business Change and Project Management

The Registry .cy recognizes that consideration of appropriate information security safeguards is most effective at the beginning of any business change. Therefore, information security is considered throughout the project lifecycle, with the following specific measures being adhered to:

1) Project managers ensure that information security is addressed at all stages of project management, starting with project briefing.
2) The Information Security Manager together with the Head of IT Infrastructure provides security signage at the end of each stage and prior to the start and/or completion of the project.
3) Risk analyses and security testing are carried out, as appropriate, before the start of the project, during the implementation stage and before its completion.
4) Relevant information security requirements are included in proposals, Requests for Proposals (RFPs) or Requests for Information (RFI).
5) All external parties, such as suppliers, vendors, outsourcers, contractors, etc., sign non-disclosure agreements prior to the start of the project.
6) All External Parties, such as suppliers, vendors, external partners, contractors, etc., sign Data Processing Agreements with the Registry .cy each time personal data is processed by them on behalf of the Registry .cy.

8. Periodic Reviews

In order to ensure the continued relevance, adequacy and effectiveness of the information security framework, the Registry .cy ensures that reviews of this information security policy and related documents are carried out at appropriate intervals and when significant changes occur in the Registry .cy or its information assets.

The revisions and updates are discussed during the meetings of the ISSC and communicated to the Registry .cy management for approval and signature.

9. Compliance

Compliance with this Policy is mandatory for all internal and external users. Compliance checks are carried out on a regular basis by the Information Security Officer of the Registry .cy.

Any violations or alleged violations of this Policy are investigated in accordance with the procedures of the Human Resources Services and are reported directly to the Head of the relevant department/division for disciplinary action.