Information Security Policy

Version: 1.2

Publish Date: 15 March 2024

__Attention:__ This document has classified for Public.
If you are not property authorized, you should avoid reading, copying, distributing, and transmitting of its context.

1. Introduction - Purpose

The current document defines the high-level policy for Information Security Management for the Registry .cy. The current Information Security Policy defines .cy Registry's approach to Information Security Management. The purpose of this Policy is to provide a framework, describe the scope, guiding principles, and the responsibilities for safeguarding the security of the .cy Registry's information Systems.

2. Scope

The current policy applies to the entire Registry .cy, including:

- All operational sites and functions,
- All information stored or processed by the Registry .cy (including that provided to the Registry .cy by customers, commercial partners, and employees), regardless of the format in which it is stored or processed,
- All authorized users, whether directly employed by the Registry .cy, or contractors providing services to it and/or its customers.

Within the broader scope described above, current policy establishes and authorizes an ISMS certified, according to the ISO 27001:2013 Standard.

3. Information Security Policy Rules

Our ISMS continuously and actively seeks to improve the resilience of the Registry .cy and ensures that a proper scope is in place, so that in case of a disruption, any potential impact is minimized and managed effectively. Our aim is to protect the assets of the Registry from internal or external threats, whether intentional or accidental, in a manner that:

- Confidential information is appropriately safeguarded,
- Integrity of the information is maintained to ensure its accuracy and completeness,
- Information about individuals is processed in a way that respects their legal rights,
- Information is available only to those individuals that have a business need for that information and only what is needed for their particular role ("least privilege" concept),
- Relevant legal, regulatory, and contractual obligations are met,
- Our commitments referenced below constitute the Information Security Policy ('Policy') of the Registry .cy and applies to all its activities. This Policy has been developed, according to the requirements of the International Standard ISO 27001:2013 and is reviewed annually or when important changes occur. It is communicated to all employees and is available as required to all interested parties.

To ensure compliance with all applicable legal, regulatory, and other requirements to which the Registry .cy is subject to, we undertake the following actions:

- Provide all necessary resources for the effective implementation and continual improvement of the ISMS,
- Assign specific roles, responsibilities, and authorities within the Registry .cy to ensure the effective management, support, and governance of the ISMS,
- Establish, review, monitor and update information security objectives that are compatible with the requirements of NIS, the strategic priorities of the Registry .cy, and the business plan,
- Actively build and embed an IS culture throughout the Registry .cy through various awareness-raising activities,
- Ensure that appropriate communication channels & mechanisms are in place so as to facilitate timely, accurate and structured internal and external communication,
- Carry out IS Risk Assessments to systematically identify, analyse and evaluate relevant risk,
- Implement appropriate risk treatment actions to proactively minimise impacts and efficiently manage potential incidents,
- Regularly carry out exercising & testing to assess and improve responding and recovery procedures,
- Regularly evaluate the performance and effectiveness of the ISMS,
- Continually improve the ISMS of the Registry .cy.