



Code:	Π02
Version:	02
Date:	22/09/2026

Π02 Information Security Policy

Introduction

This policy applies to Krypto Security (Cyprus) Ltd and in particular to the company's staff, equipment and IT applications, with the aim of ensuring the effective security of the information the company processes, by taking organisational and technical measures to safeguard the Confidentiality, Integrity and Availability of that information.

The scope of the Policy covers all Departments of the company and, consequently, all its activities.

The primary means of reducing and mitigating cyber-threat risks in the company is the use of the secure information technology infrastructure provided for the daily work of staff.

Objectives

The company has set the following information security objectives; the measurable targets and their indicators are set annually and monitored in accordance with Δ15:

- To provide staff with direction and support on information security in accordance with business requirements and the relevant laws and regulations.
- To establish an appropriate management framework able to control the implementation and operation of information security within the company.
- To ensure that the company's staff and partners know, understand and fulfil their information security responsibilities.
- To identify and protect the company's assets by defining appropriate organisational and technical security measures.
- To ensure that information is protected according to its importance to the company.
- To ensure security measures for the network and information processing infrastructure.
- To ensure the protection of the company's assets and information that are accessible to partners.
- To ensure the availability of the information processing infrastructure.
- To comply with legal, regulatory and contractual requirements and with the requirements of interested parties relating to information security.

To achieve the above objectives, Management will provide the necessary resources for the implementation of technical and organisational measures. These include, but are not limited to:

- Technical measures for the security of servers (firewall and security passwords, domain, Microsoft)
- Technical measures for the security of systems (firewall, multi-factor authentication – MFA)



Code:	Π02
Version:	02
Date:	22/09/2026

Π02 Information Security Policy

- Organisation of roles and responsibilities (confidentiality and non-disclosure agreements with staff and partners)
- Appointment of a Data Protection Officer (external partner)
- Seminars for awareness and for building a security culture among staff
- Periodic audits to review the suitability and effectiveness of the security measures (ISO 9001 & ISO 27001)
- Network segmentation
- Physical security of servers
- Risk Assessment and Data Protection Impact Assessment where required
- Signing of Data Processing Agreements with external partners where data processing takes place
- Password Security Policy
- Clean Desk Policy
- Backup Policy
- Data Protection Policy
- Off-Premises Equipment Security Policy
- Business Continuity Policy
- Acceptable Use Policy
- Policy on Contact with Special Interest Groups
- Cloud Security Policy
- Threat Intelligence Policy
- Project Management Policy
- Information Transfer Policy
- Intellectual Property Rights Management Policy
- Policy on Storage, Management, Retention and Destruction of Electronic Records
- Protection against Viruses and Malware Policy
- Vulnerability and Penetration Testing Policy
- Logging Policy
- Data Encryption Policy
- Patching Policy
- Equipment Disposal or Re-use Policy
- Web Filtering Policy
- Secure System Architecture and Engineering Principles Policy
- Policy on the Protection of Systems during Audit
- Cookies Policy



Code:	Π02
Version:	02
Date:	22/09/2026

Π02 Information Security Policy

- A set of Policies and Procedures under the International Standard ISO/IEC 27001:2022

Data processing

Data is a critical asset of the company and its protection at all stages of processing is essential. For this reason, data must:

- be classified according to its level of confidentiality (Public, Internal Use, Confidential, Secret), with the corresponding restrictions on use, disclosure and processing applied.
- be treated confidentially and used exclusively for the purpose for which it is processed.
- be stored only on approved company systems (company servers, Microsoft OneDrive / SharePoint).

In addition

- The use of removable storage media (USB, external drives) is permitted only with the approval of the Information Security Officer and with encryption.
- Passwords must be protected.
- Unnecessary printing and copying of information must be avoided, reducing the risk of it reaching unauthorised persons.
- Each user prints to a specific, pre-assigned printer.
- Confidential information must be disclosed only to authorised persons.
- Shredders of appropriate specification must be used for the destruction of confidential information / documents.
- A clean desk policy must be applied.
- Secure storage of confidential documents is mandatory.

Commitment

The Management of the company is responsible for, and committed to, providing all the resources necessary to meet all of the company's information security requirements and to continually improve the information security management system.

Within the framework of the company's general staff training policy, the company will provide training opportunities in the areas covered by this policy, so as to maximise the benefits that technology offers while reducing the risks that may arise from its incorrect use. Staff are required to take part in the relevant training programmes.

This policy is available to all interested parties, the competent authorities and the company's staff.



Code:	Π02
Version:	02
Date:	22/09/2026

Π02 Information Security Policy

This policy will be reviewed periodically, at least annually, as part of the Management Review, and amended accordingly where necessary.

CEO

22/09/2026