

cybersafe

Information Security Policy (Public Version)

Classification: PUBLIC

cybersafe

Table of contents

Document Description and Control **3**

Statement of Responsibility 3

Need to Know 3

1. Purpose **4**

2. Scope **4**

3. Information Security Principles **4**

4. Information Security Commitments **4**

5. Information Security Management System and ISO/IEC 27001:2022 Certification **5**

6. Incident Management, Continuity and Resilience **5**

7. Responsibility and Security Culture **5**

8. Compliance, Monitoring and Review **6**

DOCUMENT DESCRIPTION AND CONTROL

Statement of Responsibility

This document and all its contents constitute the intellectual property of CyberSafe, Lda. (hereinafter referred to as CyberSafe) and are protected under Decree-Law No. 63/85 of 14 March – Code of Copyright and Related Rights. The disclosure, transcription or reproduction of this Policy is not permitted without the prior written authorisation of CyberSafe, Lda.

The recipient of the document undertakes to use the aforementioned information exclusively for the purpose of reviewing it, taking into account its respective scope. The use of all or part of the information contained in this document for purposes other than those defined within its scope must be previously authorised by CyberSafe.

Documents classified as “PRIVATE” or “INTERNAL” include information that is not in the public domain and must not be accessible to the general public. Access is authorised only to the entities defined in the “Need to Know” section. The reader undertakes not to disclose, duplicate or make available to any third party any information contained therein.

Classified documents, duly marked with the designations “TOP SECRET”, “SECRET”, “CONFIDENTIAL” and “RESTRICTED”, are distributed only through secure means to individuals or entities holding the respective security clearance issued by the Portuguese National Security Authority (Gabinete Nacional de Segurança – GNS), namely Individual Security Clearance or Corporate Security Clearance, as applicable.

Document Classification

PUBLIC

Document Scope

Public Policy

Need to Know

- CyberSafe
- All recipients

Version Control

VERSION	DATE	AUTHOR	DETAILS	APPROVER	APPROVAL DATE
1.0	15/09/2026	CyberSafe	Development of the Information Security Policy – Public Version		

1. Purpose

CyberSafe considers information an essential asset for the development of its activities and, as such, is committed to protecting it in an appropriate, responsible manner and in proportion to the risks to which it is exposed.

This Information Security Policy defines the principles and commitments that guide CyberSafe in protecting information, seeking to ensure its confidentiality, integrity and availability. Its application aims to protect the organisation's assets, ensure the continuity of activities and services, and strengthen the trust of customers, partners, suppliers and other interested parties.

CyberSafe is also committed to complying with the legal, regulatory and contractual requirements applicable to its activities, as well as to maintaining and continuously improving its Information Security Management System (ISMS).

2. Scope

This Policy applies to information processed by CyberSafe within the scope of its activities, regardless of its format, medium or location.

The principles established in this Policy apply to employees, service providers, partners, suppliers and other interested parties who, within the scope of their relationship with CyberSafe, have access to information, systems or the resources that support them.

This Policy is applied in a manner proportionate to the nature of the information, the associated risks and the applicable legal, regulatory and contractual requirements.

3. Information Security Principles

CyberSafe´s approach to Information Security is governed by the following principles:

Confidentiality — Ensure that information is made available or disclosed only to duly authorised persons, entities or processes.

Integrity — Preserve the accuracy and completeness of information, protecting it against improper or unauthorised changes.

Availability — Ensure that information and the necessary resources are accessible and usable by authorised parties when required.

Risk Management — Identify, assess and treat Information Security risks systematically and in proportion to the criticality of assets, processes and services.

Shared Responsibility — Promote the participation and accountability of all parties involved in protecting information.

Continual Improvement — Continuously monitor, assess and improve Information Security practices and controls, taking into account the evolution of risks, technologies, the business and applicable requirements.

4. Information Security Commitments

Within the scope of its Information Security Management System, CyberSafe is committed to:

- Protecting the confidentiality, integrity and availability of information under its responsibility;
- Implementing and maintaining technical and organisational controls appropriate to the identified risks;
- Protecting information against unauthorised access, alteration, loss, destruction or improper disclosure;
- Managing access to information according to applicable needs, roles and responsibilities;
- Identifying, assessing and treating Information Security risks;
- Classifying and protecting information according to its sensitivity, value, criticality and applicable requirements;
- Considering Information Security requirements in the management of systems, services, processes and their respective changes;
- Promoting continuous training and awareness among employees and other relevant parties;
- Considering Information Security requirements in relationships with customers, suppliers, partners and other third parties;
- Adopting continuity and recovery measures appropriate to the criticality of processes and services;
- Regularly monitoring and assessing the effectiveness of implemented security controls and measures;
- Ensuring compliance with applicable legal, regulatory and contractual requirements;
- Promoting the continual improvement of the Information Security Management System.

5. Information Security Management System and ISO/IEC 27001:2022 Certification

CyberSafe maintains an Information Security Management System (ISMS) through which it establishes a structured and risk-based approach to information protection, the management of security controls and continual improvement.

As part of its commitment to Information Security, CyberSafe's ISMS is certified in accordance with the ISO/IEC 27001:2022 standard, within the scope of the provision of cybersecurity incident monitoring, detection, analysis and response services, provided through Security Operations Center (SOC as a Service) and Managed Detection and Response (MDR) services.

This certification reinforces CyberSafe's commitment to adopting internationally recognised practices for Information Security management, risk management and the continual improvement of the processes covered by the certified scope.

6. Incident Management, Continuity and Resilience

CyberSafe maintains processes for the identification, recording, analysis and handling of Information Security events and incidents.

Identified incidents are assessed according to their nature and impact, and the containment, corrective and recovery measures considered appropriate are adopted. Whenever legally or contractually required, the necessary notifications are made to the competent authorities, customers or other relevant interested parties.

CyberSafe also maintains continuity and resilience measures appropriate to the criticality of its processes and services, with the aim of reducing the impact of adverse situations and supporting the continuity and recovery of its activities.

7. Responsibility and Security Culture

Informartion Security is a shared responsibility of everyone who processes or has access to CyberSafe's information.

Top Management ensures support for the implementation, maintenance and continual improvement of this Policy and the Information Security Management System.

CyberSafe promotes regular training and awareness activities, encouraging the adoption of good practices, responsible behaviour and the reporting of events or situations that may compromise Information Security.

All employees and third parties covered by this Policy must comply with the security principles, policies, standards and procedures applicable to the activities they perform.

8. Compliance, Monitoring and Review

CyberSafe is committed to complying with the legal, regulatory and contractual requirements applicable to Information Security and to the protection of information under its responsibility.

The implementation and effectiveness of Information Security controls are monitored through appropriate monitoring and audit mechanisms. The results of these activities, as well as developments in risks, threats, technologies and applicable requirements, are considered as part of the continual improvement of the ISMS.

This Policy is approved by Top Management and reviewed annually, or whenever significant changes occur in information assets, risks, processes or applicable requirements.

Updates enter into force following their respective approval and publication, replacing previous versions.

Classification: Public

Version: 1.0

Last Updated: September 2026



Alfrapark - Estrada de Alfragide
67 | Edifício H, piso 1 | 2610-008
Alfragide, Portugal

+351 210 360 276
contato@cybersafe.pt