Information Security Policy

Policy on the security of network and information systems [ISO27001 5.2] [NIS 1.1]

Last update: 2025-02-07
Owner: CEO
Author: Hans Olof Edblom

Classifications:

| Public: Okay to put on our website. **| Internal**: Elastisys use only.

| Confidential: As needed internally depending on working group **| Customer data:** Never shared

Public

Change Log			
Author:	**Version:**	**Date:**	**Change History:**
CISO	1.0	2022-11-16	Initial release of previous document
CISO	2.0	2024-03-05	Implemented the new template added Purpose Section. Updated Information security objective, and Information security management process
Hans Olof Edblom	3.0	2025-02-07	• *Initial release of stand-alone document.* • *Updated to new template* • *Added sections 1, 2, 3, 8.* • *Rearranged information into new structure.* • *Added ISO2700X and NIS2 references to sections where applicable.* • *Changed information classification from internal to Public.* • *Removed soft wording such as "may".* • *Added requirements on developing KPIs for IS Objectives.*

1 Definition and purpose [ISO27002 A5.1]

Text in brackets [] indicate references to topic-specific requirements in standards or regulations.

- [ISO2700**X**] references the "SS-EN ISO/IEC 2700**X**"-standard where X varies depending on which 27000-standard is referenced.
- [NIS] references are related to "Commission Implementing Regulation (EU) 2024/2690 Annex 1" and indirectly to the EU NIS2 directive, 2022/2555.

Information security refers to the tools and processes that Elastisys employ to protect sensitive information from unauthorized access, disclosure, alteration, or destruction.

The purpose of this Information Security Policy is to:

- **S**ecure Elastisys against cybersecurity threats and data breaches.
- **A**dhere to legal, regulatory, and contractual obligations, including GDPR, NIS2 and other applicable European laws.
- **F**ortify the confidentiality, integrity, and availability of information assets.
- **E**ncourage a culture of security awareness and accountability.

2 Scope [ISO27001 4.3]

This policy applies to:

- All employees, contractors, third-party suppliers, and partners.
- All organizational information, regardless of format (digital, printed, or verbal).
- All information systems, applications, and networks owned, operated, or managed by Elastisys.

More details on the scope of the ISMS can be found in the Statement of Applicability and the ISMS Dashboard.

3 Roles and Responsibilities [ISO27002 A5.2] [NIS 1.2]

3.1 Chief Executive Officer

- Ensure adequate resources are allocated for information security.
- Approve and monitor compliance with this policy.

3.2 Chief Information Security Officer (CISO)

- Develop and implement security strategies for continuous improvement of the Information Security Management System.
- Conduct regular risk assessments, selecting and implementing controls and measures aimed at improving the organizations information security posture
- Oversee incident response and business continuity planning.
- Ensure adequate information security awareness and training for the organization.

3.3 Employees and Contractors

- Comply with all security policies and procedures.
- Report any security events, incidents, risks, exemptions or suspicious activities to CISO@Elastisys.com

Details can be found in the ISMS Dashboard.

4 Management commitment [ISO27001 5.1] [NIS 1.1]

The Elastisys management team is dedicated to maintaining the information security requirements, and recognizes that the protection of information assets is critical to company success and the trust placed in Elastisys by clients, partners, and stakeholders.

As part of the commitment to excellence, the management team prioritizes information security as a fundamental aspect of operations and are dedicated to establishing, implementing, and maintaining a comprehensive information security management system.

Management commitment is demonstrated through strong leadership support, resource allocation, compliance with legal and contractual regulations, proactive risk management, and continuous improvement efforts. Elastisys regularly monitors and assesses our Information Security Management System (ISMS), conducts internal audits and management reviews, provides ongoing employee awareness training, and engages with stakeholders to gather feedback.

5 Information security management process

Elastisys performs recurring risk assessments as part of the Risk Management Process. Analysis is conducted quarterly as part of our Risk Management Forum and aims both to identify the critical information assets requiring protection as to provide a documented rationale for what is worth protecting. The risk analysis also relates the identified assets to the threats that the business may be exposed to, and the vulnerabilities that the business may be afflicted with. Finally, the risk analysis is aimed at developing a decision basis for the introduction of controls with the purpose of:

- protecting information from unauthorized access. (**C**onfidentiality);
- keeping information trustworthy, complete, and not accidentally altered or modified by an unauthorized user. (**I**ntegrity),
- ensuring information is accessible when it is needed (**A**vailability), and
- to ensure the origin of each operation (Authenticity).

The ISMS processes are reviewed and evaluated continuously or at least one time per year. Discrepancies and inadequacies as well as the occurrence of

incidents are systematically documented for drawing upon experience of such events, which can be considered in the work for continuous improvement. The result of the information security related activities, ongoing activities and the estimated risk levels are handled as part of the recurring management meetings and management review, and are subject to continuous improvement.

6 Information security objectives [ISO27002 A5.1]

Elastisys' management team commits to developing clear performance indices related to each of the below objectives on an annual basis, or review existing ones for update annually.

Cyber Resilience Assurance: Establish robust mechanisms to ensure the resilience of cloud-native infrastructure, focusing on data security, system availability, and rapid incident response, thereby safeguarding business continuity and customer trust.

Regulatory and Contractual Compliance: Develop a comprehensive compliance framework to navigate regulatory requirements effectively while proactively managing risks associated with vendor relationships and internal operations, ensuring long-term sustainability and market credibility.

Security-Centric Culture Development: Foster a culture of security awareness and accountability across the organization through targeted training and communication initiatives, embedding security considerations into every aspect of business operations and decision-making processes.

Strategic Partnerships and Vendor Management: Forge strategic partnerships with trusted vendors and service providers, emphasizing stringent security standards and ongoing risk assessment protocols to enhance the overall security posture and reliability of our services.

Continuous Improvement and Innovation: Drive continuous improvement and innovation in security practices by leveraging cutting-edge technologies and industry best practices, enabling the company to stay ahead of emerging threats and maintain a competitive edge in the dynamic cloud-native computing landscape.

Confidence and Transparency: Build confidence and trust through transparent communication and proactive engagement, demonstrating a commitment to security excellence and accountability in delivering value-added cloud-native solutions that meet or exceed client expectations.

7 Information Classification [ISO27002 A5.12]

Information classification is crucial for our company's compliance to regulations, standards and customer expectations. It enables efficient risk management by identifying and prioritising sensitive assets. This classification ensures legal compliance, sets clear data handling guidelines, and facilitates effective resource allocation.

Public Information: This category includes information that is intended to be outward facing and accessible to anyone. Examples of public information may include commercial materials, training material and press releases. This data does not pose any significant risk to the organisation if disclosed and is typically intended for external stakeholders or the general public.

Internal Information: Internal information is restricted to authorised employees within the organisation. It encompasses operational details, and non-sensitive business data that are essential for the day-to-day functioning of the company. While this information is not intended for public consumption, it is vital for facilitating internal processes and decision-making.

Confidential Information: Confidential information comprises sensitive data that, if disclosed, could potentially harm the company's reputation, finances, or operations. This category includes, strategic plans, and other proprietary or sensitive information. Safeguarding this data is crucial to maintaining the integrity and security of the organisation.

Customer Data: As data processors, customer data is handled with the highest degree of confidentiality, and treated as medical patient data, in terms of protection and handling. This category encompasses personal and sensitive information provided by customers, including contact details, financial information, and other personally identifiable information (PII). Due to the sensitivity of this data and our role as data processors, it is automatically classified as confidential by default and cannot be reclassified to a lower level. Our responsibility as data processors mandates stringent security measures and

compliance with relevant data protection regulations to ensure the privacy and security of customer information.

8 Topic-specific policies

Elastisys employs a number of topic-specific information security policies, documented throughout this document, process documents and repositories. Below are the general requirements for the topic-specific information security policies as well as guidance to more detailed ways of working.

8.1 Acceptable use of IT resources [ISO27002 A5.10][NIS 12.2]

All employees, contractors, and third parties must use organizational information and assets responsibly, ethically, and in alignment with business objectives. Information and associated assets, including devices, networks, and applications, are to be used only for authorized purposes and must not be exploited for personal gain or activities that violate laws, regulations, or organizational policies. Users are prohibited from introducing malicious software, accessing unauthorized data, or engaging in activities that compromise the confidentiality, integrity, or availability of information assets.

Detailed information on use of information assets can be found in the Elastisys IT Policy, in the Elastisys Policies document.

8.2 Information Transfer [ISO27002 A5.14][NIS 12.2]

The transfer of information, whether internal or external, must be conducted securely to protect its confidentiality, integrity, and availability. Approved methods and technologies, such as encryption and secure communication channels, shall be used to mitigate risks during transmission. Any unauthorized or unprotected transfer of sensitive or confidential information is strictly prohibited.

Detailed information of information transfer can be found in the Elastisys IT Policy, in the Elastisys Policies document and the Terms of Service Appendix 1.

8.3 Access Control [ISO27002 A5.15][NIS 11.1]

Access to information and systems is granted based on the principle of least privilege, ensuring that users only have access necessary for their roles. All access (including third party) must be authorized by the people or system manager to safeguard the confidentiality, integrity, and availability of information assets and to ensure access is modified accordingly upon change of employment. Annual reviews of access rights registry are conducted to ensure compliance.

Detailed information on access control can be found in the Elastisys IT Policy, in the Elastisys Policies document and in the ISMS Dashboard Roles & Responsibility and IT Systems Registry tabs.

8.4 Information Security in Supplier Relationships [ISO27002 A5.19][NIS 5.1-5.2]

The organization ensures that all supplier relationships are managed to protect the confidentiality, integrity, and availability of information assets. Suppliers must adhere to defined security requirements, which are documented in contracts or agreements and include compliance with applicable laws and regulations. Regular risk assessments and reviews of supplier practices will be conducted to verify their adherence to security standards. Any information security incidents involving suppliers must be reported and managed in accordance with the organization's incident management process.

Detailed information on supplier management can be found in the Elastisys Policies document and the Supplier Management process.

8.5 Information Security for use of Cloud Services [ISO27002 A5.23][NIS 6.1]

Cloud service providers must implement robust security measures, including data protection, access control, and encryption, to safeguard the confidentiality, integrity, and availability of organizational information. Contracts with cloud providers must define clear security responsibilities, including incident management and compliance with applicable regulations. Regular assessments and audits will be conducted to verify the security practices and compliance of cloud service providers.

Detailed information on use of cloud services can be found in the Elastisys Policies document and the Supplier Management process.

8.6 Intellectual Property Rights [ISO27002 A5.32][NIS 6.9]

Elastisys protects intellectual property rights (IPR) in compliance with applicable laws, regulations, and contractual obligations. All employees, contractors, and third parties must respect and safeguard intellectual property, including copyrights, trademarks, patents, and trade secrets, during all business activities. Unauthorized use, reproduction, or distribution of intellectual property is strictly prohibited. The organization will implement measures to ensure proper licensing, usage rights, and monitoring to prevent IPR violations and promote ethical practices.

8.7 Privacy and protection of PII [ISO27002 A5.34][NIS 6.1]

Protecting the privacy and security of personally identifiable information (PII) is essential to ensuring compliance with applicable laws, regulations, and industry standards, including GDPR. Appropriate technical and organizational measures, such as encryption, access controls, and data minimization, will be implemented to safeguard PII against unauthorized access, disclosure, or loss. Employees, contractors, and third parties must handle PII responsibly and only for authorized purposes. Regular assessments will be conducted to ensure compliance with privacy obligations and to address evolving threats to data protection.

Detailed information on PII can be found in the Elastisys Policies document and the Privacy Policy.

8.8 Remote Working [ISO27002 A6.7]

Ensuring the security of information during remote working is critical to maintaining the confidentiality, integrity, and availability of organizational assets. Employees must follow defined security practices, including the use of secure connections, encryption, and organization-approved devices. Access to sensitive information must be restricted to authorized personnel and conducted in a secure environment. Regular training and monitoring will support compliance with information security requirements while working remotely.

Detailed information on remote working, customer premises and working while traveling can be found in the Elastisys Policies document.

8.9 Clear desk and clear screen [ISO27002 A7.7] [NIS 12.3]

Maintaining a clear desk and clear screen environment is essential to protecting sensitive information and preventing unauthorized access. Employees must ensure that all confidential documents are securely stored when not in use and that screens are locked when leaving their workstation. Physical and electronic information must not be left unattended in public or shared spaces. These practices help reduce the risk of information exposure and promote a secure working environment.

Detailed information on protection of physical resources, removable media and clean desk/screen can be found in the Elastisys Policies document.

8.10 Storage Media [ISO27002 A7.10] [NIS 12.2, 12.3]

Proper management of storage media is essential to ensuring the confidentiality, integrity, and availability of information. All storage media must be securely handled, stored, and disposed of in accordance with the organization's information security requirements. Sensitive data stored on media must be encrypted, and access must be restricted to authorized personnel only. Regular checks and secure disposal methods, such as shredding or degaussing, must be employed to prevent unauthorized access or data leakage.

Detailed information on protection of physical resources and disposal of information can be found in the Elastisys Policies document and in the Document Control Process.

8.11 User endpoint devices [ISO27002 A8.1]

Securing user endpoint devices is vital to protecting organizational information and minimizing security risks. All endpoint devices, such as laptops, desktops, and mobile devices, must be configured with up-to-date security measures, including antivirus software, firewalls, and encryption. Users must ensure that devices are used only for authorized purposes, kept physically secure, and locked when unattended. Regular updates, monitoring, and compliance checks will be conducted to maintain the security of endpoint devices and prevent unauthorized access.

Detailed information on user endpoint devices and protection of physical devices can be found in the Elastisys IT Policy, in the Elastisys Policies document.

8.12 Management of technical vulnerabilities [ISO27002 A8.8] [NIS 6.10]

Elastisys employs rigorous management of technical vulnerabilities to maintain security and resilience of organizational systems. All systems and applications must be regularly assessed for vulnerabilities, with identified issues prioritized and remediated based on their risk level. Security patches and updates must be applied promptly to reduce exposure to threats, and monitoring tools should be used to detect new vulnerabilities. Regular vulnerability assessments and compliance with industry best practices will ensure a proactive approach to risk management.

Detailed information on management of technical vulnerabilities can be found in the Operations Manual.

8.13 Information Backup [ISO27002 A8.13] [NIS 4.2]

All sensitive and business-critical information must be regularly backed up using secure methods, with backup copies stored in protected locations. Backups must be tested periodically to verify their integrity and the effectiveness of the restoration process. Access to backups must be restricted to authorized personnel, ensuring compliance with organizational security requirements. Business information backups for important systems (i.e. Google Suite) shall be managed by the service provider and Terms and Conditions shall be reviewed and approved by Elastisys before operations begin.

Detailed information on management of information backup and supplier management can be found in the Elastisys IT Policy, in the Elastisys Policies document.and the Supplier Management process.

8.14 Logging [ISO27002 A8.15] [NIS 3.2]

Comprehensive logging is essential for monitoring system activities and ensuring accountability. All critical systems and applications must generate and retain logs that capture relevant security events, including access, modifications, and anomalies. Logs must be securely stored, protected from unauthorized access or alteration, and regularly reviewed to detect potential security incidents. Retention periods for logs must comply with regulatory and organizational requirements to support investigations and audits.

Detailed information on logging, log reviews and monitoring can be found in the Operations Manual.

8.15 Use of Cryptography [ISO27002 A8.24] [NIS 9]

Cryptography must be used to protect the confidentiality, integrity, and authenticity of sensitive information. All cryptographic methods and protocols must comply with recognized industry standards and organizational requirements. Cryptographic keys must be securely managed throughout their lifecycle, including generation, storage, usage, and disposal. Regular reviews and updates of cryptographic controls will ensure they remain effective against evolving security threats.

Detailed information on encryption can be found in the Elastisys IT Policy, in the Elastisys Policies document.