



docSpace srl

via Molo Cagni, Pal. Servizi
16128 Genova - Italy

P.I.: 02646920997

PEC: docspace@legalmail.it

web: www.doc-space.net

tel +39 010 0985000

Information Security Policy

DocSpace S.r.l.



Contents

1	Acronyms	3
2	History	3
3	Introduction	4
3.1	Purpose	4
4	Scope	4
5	Information Security Objectives	5
5.1	Principles	5
5.2	Roles and Responsibilities	6
5.3	Management Commitment	6
5.4	Risk Assessment and Treatment	7
5.5	Information Security Controls	7
5.6	Compliance and Legal Requirements	8
5.7	Employee Awareness and Training	8
5.8	Continual Improvement	8
6	Monitoring and Review	8



Author	Reviewer	Approver
Carlo Andreotti (CSO)	Pierpaolo Baglietto	Massimo Maresca

1 Acronyms

CSO	Chief Security Officer
GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization

2 History

Version	Date	Notes
1.0	07/05/2025	First issue.
1.1	24/11/2025	Change approvers according to organization chart
1.2	18/09/2026	Rename DocSpace Sheets in SpreadSheetSpace



3 Introduction

This Information Security Policy outlines the principles, goals, and guidelines for maintaining confidentiality, integrity, and availability of information for DocSpace S.r.l., a SW house developing a distributed data sharing platform named SpreadSheetSpace for collaborative use of parts of Excel files and more in general data tables from any data source.

SpreadSheetSpace operates through a data synchronization process, always ensuring maximum confidentiality. Sharing data is simple, users select the area of the spreadsheet they want to share and click a button. As soon as the owner of the data makes changes to the document, the individual whom the document has been shared with, will be automatically notified of the updates.

Data owners can decide whether to share the data as read-only or allow his collaborators to modify it. To import data from company information systems or other users, the users just open an Excel sheet and click a button. Whenever a new version becomes available, users will be notified, and the document will automatically update, keeping all authorized users working in sync.

Users can choose to provide certified, unmodifiable data to their collaborators, or work together on a shared document. Every change made to a shared document is tracked, notified, and logged, allowing users to view the history of updates and perform detailed analyses of the data while considering its changes over time.

3.1 Purpose

The purpose of this policy is to establish a framework for managing and protecting DocSpace S.r.l. information assets, ensure compliance with relevant laws and regulations, and support the development of a secure environment for the software application. DocSpace S.r.l. will take all necessary steps to protect information from unauthorized access, alteration, or destruction. This policy is aligned with the requirements of ISO/IEC 27001:2022, aiming to ensure effective management of information security risks and to safeguard business assets and sensitive data.

4 Scope

This policy applies to all information, systems, and employees involved in the development, maintenance, and usage of SpreadSheetSpace platform. It covers the following areas:

- Development and maintenance of the platform.
- Storage, transmission, and processing of data associated with the application.
- Devices, networks, and services used by employees to access DocSpace S.r.l. resources.

Security Governance represents a focal point for the business growth of DocSpace S.r.l., considering its influence on:

- Preserving DocSpace S.r.l. assets.
- Strengthening DocSpace S.r.l. brand.
- Increasing profits, reducing risk and optimizing resources.
- Increasing customer confidence.
- Achieving compliance against regulations and contracts



5 Information Security Objectives

To ensure that DocSpace S.r.l. achieves its goal of protecting its information assets, the following information security objectives are defined:

- Maintain the **confidentiality** of sensitive information, preventing unauthorized disclosure.
- Ensure the **integrity** of all data, ensuring that information is accurate, consistent, and trustworthy.
- Ensure the **availability** of information and systems, guaranteeing that critical resources are accessible when required.

The information security objectives are achieved by SpreadSheetSpace plug-in through sharing of data without ever leaving customer administrative domain, with maximum security guaranteed by RSA-based end-to-end encryption, ensuring that only the authorized recipient can decrypt and interpret the content.

Additionally, users can share only specific parts of their spreadsheet, controlling who has access. Customer data privacy is central to DocSpace S.r.l.

Overall Information Security Objectives include the following:

- Compliance with current impacting national laws, regulations and guidelines as well as DocSpace S.r.l. internal policies.
- Establish controls for protecting DocSpace S.r.l. information and information systems against theft, abuse and other forms of harm and loss.
- Motivate all employees to improve their security awareness to better protect and safeguard DocSpace S.r.l. information.
- Have a Business Continuity Plan (BCP) in place to reduce the negative impacts of major security incidents.
- Availability and reliability of the network infrastructure and the services supplied and operated by DocSpace S.r.l.
- Comply with methods from international standards for Information Security, e.g. ISO/IEC 27001:2022.
- Flexibility and an appropriate level of security for accessing information systems.

5.1 Principles

DocSpace S.r.l. security vision is based on protecting information assets, managing security risks, enabling business strategies in an effective and efficient way, fully supported by executive leadership and underpinned by all DocSpace S.r.l. employees.

The main drivers involved in a security strategy plan definition are:

- **DocSpace S.r.l. Security Ambition:** The DocSpace S.r.l. expectation and ambition that are the main input to define the security plan and the investment in a long-term vision.
- **Risk Management:** the outcomes from a risk management perspective regarding the top security risks for DocSpace S.r.l. in terms of information security; for this reason, DocSpace S.r.l. conducts annual information and cybersecurity risk assessments. These assessments encompass identifying, evaluating, and managing threats, facilitating prompt responses to incidents.
- **Regulatory and Compliance:** external pressure based on regulatory and compliance needs drive DocSpace S.r.l. to actively promote security and regulatory compliance



practices. Cybersecurity is seamlessly integrated into its business agenda, considering it an integral aspect of its operations.

- **Needs and Expectations of Other Interested Parties:** DocSpace S.r.l. recognizes the importance of addressing the needs and expectations of various stakeholders, including customers, partners, regulators, and employees. By aligning its cybersecurity practices with stakeholder expectations, DocSpace S.r.l. fosters trust, strengthens relationships, and supports its commitment to operational excellence and regulatory adherence.
- **Security Posture:** the security posture resulting from either technical (e.g. Vulnerability Assessments) or internal/external audits and assessments that can influence priorities on business activities.
- **Awareness Campaign:** the outcomes of the awareness campaign are an indicator of the employees' readiness on security matters.
- **Personal Data Protection:** DocSpace S.r.l. is dedicated to respecting customer personal data protection. DocSpace S.r.l. endeavors to process personal data in accordance with applicable laws while striving to implement effective data protection solutions. This commitment is aimed at delivering to DocSpace S.r.l. customers the best user experience possible.

These drivers and objectives are established and reviewed every year, to consider them as the basis for an organization-wide strategy and to set the correct level of Information Security.

This means that the security matter will be considered as a high priority in making any business decisions. This will help DocSpace S.r.l. to allocate sufficient human, technical and financial resources to Information Security Management and to take appropriate actions in response to all the potential Information Security violations.

The security efforts will be:

- **Coordinated:** security measures based on a common framework and all staff will be involved in maintaining compliance with it
- **Proactive:** detect, identify and manage vulnerabilities, threats and security gaps to prevent security incidents
- **Supported at the highest level:** security management actively committed to Information Security and with full support to implement the required security controls that are identified through a continuous risk assessment process

5.2 Roles and Responsibilities

- **Management:** Senior management is responsible for setting the direction of information security, approving policies, and ensuring adequate resources are allocated for information security initiatives.
- **Chief Security Officer (CSO):** The appointed CSO will oversee the implementation of security measures, monitor compliance, and assess risks.
- **Employees:** All employees must adhere to DocSpace S.r.l. information security practices, report potential security incidents, and follow prescribed procedures for safe use of systems and data.

5.3 Management Commitment

Management shall actively support Information Security through clear direction, leadership, commitment, explicit assignments and recognition of Information Security responsibilities.



The management commitment is implemented through a structure whose tasks are:

- Identify all objectives relating to Information Security in line with DocSpace S.r.l. requirements.
- Establish DocSpace S.r.l. roles and responsibilities for the development and maintenance of the Information Security Management System.
- Provide sufficient resources for the planning, implementation, organization, control, review, management and continual improvement of the Information Security Management System.
- Communicate to staff about the need to meet the objectives, policies, applicable statutory and regulatory requirements (laws, regulations).
- Monitor that the Information Security Management System is integrated into all business processes and that procedures and controls are effectively developed.
- Approve and support all initiatives aimed at improving the quality and security of information.
- Activate programs to spread information security awareness and culture.
- Assess the information security performance and the effectiveness of the governance.
- Pursue continual improvement by supporting initiatives proposed by all involved internal functions.

5.4 Risk Assessment and Treatment

DocSpace S.r.l. will conduct regular risk assessments to identify, evaluate, and address information security risks. Risk treatment will include:

- Identifying vulnerabilities and potential threats to systems and data.
- Implementing appropriate controls and safeguards to mitigate identified risks.
- Continuously monitoring and reviewing the effectiveness of controls.

5.5 Information Security Controls

To safeguard confidentiality, integrity, and availability of information, the following controls will be implemented:

- **Access Control:** Access to the SpreadSheetSpace plug-in software code will be restricted based on roles, as well as to other critical information. Only authorized personnel will have access to sensitive data.
- **Authentication and Authorization:** Strong user authentication (e.g., multi-factor authentication) will be enforced to ensure that only authorized individuals can access sensitive resources.
- **Data Encryption:** Data, including SpreadSheetSpace plug-in software code, will be encrypted during storage and transmission to prevent unauthorized access or tampering, according to the specific criticality
- **Backup and Recovery:** Regular backups of critical data will be made, and a disaster recovery plan will be established to ensure business continuity in case of a security incident.
- **Network Security:** Firewalls, intrusion detection systems (IDS), and secure VPNs will be used to protect DocSpace S.r.l. network and systems from external and internal threats.
- **Incident Management:** A clear incident response plan will be in place to detect, report, and respond to information security incidents, minimizing damage and ensuring timely recovery.



5.6 Compliance and Legal Requirements

DocSpace S.r.l will ensure compliance with all applicable data protection laws and regulations, including GDPR (if applicable) and any other regional specific security standards. Employees must also be trained in relevant legal obligations regarding information security and data protection.

5.7 Employee Awareness and Training

Regular training and awareness programs will be provided to employees to ensure they understand the importance of information security and are familiar with DocSpace S.r.l policies and procedures. Employees will be trained in:

- Secure handling and sharing of data.
- Recognizing and responding to phishing and social engineering attacks.
- Maintaining good password hygiene and secure authentication practices.

5.8 Continual Improvement

DocSpace S.r.l. is committed to continually improve its information security posture. All identified weaknesses or non-conformities will be addressed, and lessons learned will be applied to strengthen the ISMS.

DocSpace S.r.l. is also committed to ensuring the security of its information assets and the integrity of the software application it develops. By adhering to the guidelines set forth in this policy and following ISO/IEC 27001:2022 standards, DocSpace S.r.l. aims to provide a secure environment for both its employees and users of its plug-in.

6 Monitoring and Review

The effectiveness of the Information Security Management System (ISMS) will be regularly monitored through:

- Regular internal audits and assessments.
- Monitoring and reviewing of events (e.g. security incidents) and corrective actions taken.
- Periodic management reviews to ensure continual improvement.

This Information Security Policy will be reviewed on an annual basis, or more frequently, if necessary, to ensure its ongoing effectiveness.