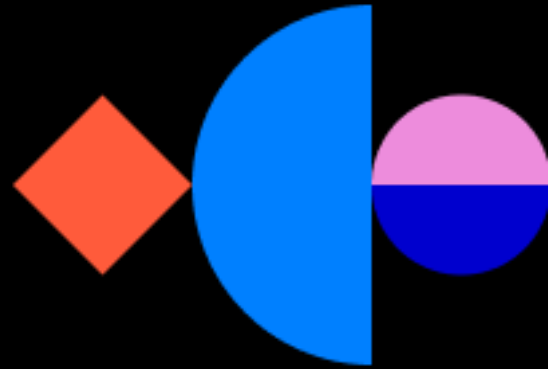


# Information Security Policy



ISMS	ISO 27001 documentation
Title	Information Security Policy
ISO identification	ISO 27001:2022 - Clause 5.2 and 6.2 ISO 27001:2022 - A 5.1 ISO 27001:2017 - A 5.1.1
Type	Mandatory document
Classification	Public
Document owner	Chief Information Security Officer

*Important information: To see the different versions of this document, go to "File", "Version History", "See version history". Choose "Only show named version" to see the different versions. Version that is not named is only for changes concerning spelling errors and grammar.*

## Scope and Purpose

The purpose of this policy is to set out the information security policies that apply to 24SevenOffice to protect the confidentiality, integrity, and availability of data. Information security is managed based on risk, legal and regulatory requirements and business needs. The objective of this policy is that all employees, external consultants and/or third parties should know how to relate to security when processing data within the 24SevenOffice organization. This policy applies to all employees and third parties.

The formal language for all security policies shall be English throughout the organization.

## Information Security Roles and Responsibilities

The CEO is responsible for implementing this policy across the 24SevenOffice organization. Information security is a collective responsibility; all individuals must adhere to policies, follow processes, and report suspected or actual breaches. Specific roles and responsibilities for managing the Information Security Management System (ISMS) are detailed in a separate document named Security Roles and Responsibilities. Management is committed to providing the necessary resources to maintain the Information Security Management System (ISMS). All employees and external consultants must comply with this policy and actively protect the company's information assets.

## Chief Executives Statement of Commitment

This is the chief executives state of commitment:

*“At 24SevenOffice, we recognize that information security is paramount to our operational integrity and the trust we build with our clients, partners, and stakeholders. As the CEO, I am committed to upholding the highest standards of information security by ensuring that our Information Security Management System (ISMS) aligns with the ISO 27001 standard. We pledge to meet all legal, regulatory, and contractual obligations, ensure appropriate access to data, protect personal data in compliance with GDPR, and act as responsible data stewards. Our governance framework involves all levels of the organization in managing risks, implementing stringent controls, and fostering a culture of security awareness. Continuous improvement is integral to our Information Security Management System (ISMS), enabling us to adapt to evolving threats and maintain stakeholder trust. I call upon all members of our organization to join me in this commitment to protect our information assets and ensure our continued success. Thank you for your dedication to information security”*

Eirik Aalvik Stranden, CEO

# Information Security Policy

At 24SevenOffice, we are committed to maintaining the highest standards of information security to protect the confidentiality, integrity, and availability of all information assets. Our Information Security Policy reflects our dedication to safeguarding the data entrusted to us by our customers, partners, and stakeholders to ensure robust and comprehensive security practices. Acknowledging the vital role of information security in protecting our business data and supporting our customers, we've established a robust Information Security Management System (ISMS) and made the following commitments to ensure security:

## Our Commitment to Information Security

- We shall safeguard the integrity, confidentiality, and availability of both our own and our customers' data, recognizing this commitment as essential for maintaining a strong reputation, operational integrity, and financial stability, while working towards ensuring compliance, controlling access, protecting personal data, and acting as responsible data processors.
- We shall continuously assess and mitigate risks through risk management practices, ensuring that our services are resilient against evolving threats.
- We shall rigorously adhere to all relevant laws, regulations, and industry standards, including GDPR and ISO 27001 frameworks. We are committed to maintaining compliance through regular policy updates, comprehensive training programs, storage within accepted areas, and thorough internal audits, thereby fostering a culture of accountability and ensuring ongoing adherence to all legal and regulatory requirements.
- We shall prioritize the ongoing education and training of our personnel, empowering them to proactively recognize and address security challenges.
- We shall regularly review and enhance our security controls to stay ahead of emerging threats.
- We shall maintain transparency and open communication with our customers, fostering trust and collaboration in our collective efforts to protect sensitive information.
- We shall strive for excellence in information security, recognizing it as a fundamental cornerstone of our commitment to delivering reliable and trustworthy services.

## Information Security Principles

Our Information Security Policy is based on risk management, legal and regulatory requirements, and business need to ensure:

- Confidentiality  
We work to ensure that access to information is restricted to those with authorized privileges, so only the right people have access.
- Integrity  
We work to maintain the accuracy and completeness of information, ensuring it is reliable and accurate.
- Availability  
We work to ensure that information is accessible when needed, so it is available at the right time.

These principles guide our actions as we strive to maintain the trust and confidence of our customers while delivering exceptional services.

## Information Security Objectives

24SevenOffice is committed to a set of security objectives regulated in a separate document. These objectives guide our efforts to enhance our security posture and align with our strategic goals.

## Information Security Policy Framework

The ISO 27001 standard provides the framework for an effective Information Security Management System (ISMS), setting out the necessary policies and procedures to protect the business. These include all the risk controls (legal, physical, and technical) required for robust IT security management. The framework is available on a need-to-know basis to all personnel or auditors.

## Security Controls

To protect information assets, 24SevenOffice have implemented a range of security controls, including:

- Access Control  
Restricting access based on the principle of least privilege in different Cloud Services.

- **Physical Security**  
Protecting our facilities and physical assets from unauthorized access, damage, and interference.
- **Information Classification**  
Categorizing information based on its sensitivity and applying appropriate protection measures.
- **Risk Management**  
Conducting regular risk assessments, implementing appropriate controls, and continuously monitoring to mitigate potential threats and vulnerabilities.
- **IT Protection**  
Use of antivirus systems, monitoring of systems that are in use, as well as stable operation and necessary updates/maintenance to prevent unwanted incidents.
- **Supplier Relationships**  
Extending the information security requirements to suppliers and partners, ensuring they adhere to equivalent security standards.
- **Incident and Business Continuity Management**  
Establishing procedures for detecting, reporting, and responding to security incidents or business continuity situations to minimize impact and ensure swift recovery.
- **Intellectual Property Rights (IPR) Protection**  
Implementing measures to safeguard intellectual property rights to ensure secure handling, storage, and transmission of IPR-related information.
- **Training and Awareness**  
Providing ongoing training and awareness programs to ensure all personnel understand their roles in protecting information and staying informed about best practices and emerging threats.

## Monitoring

Compliance with the policies and procedures of the Information Security Management Systems (ISMS) are monitored via the management review, together with independent review by both external and internal audit on a periodic basis.

## Legal and Regulatory Obligations

24SevenOffice takes its legal and regulatory obligations seriously and these requirements are recorded in the Statutory, regulatory, and contractual requirements.

## Continuous Improvement

We are dedicated to the continuous improvement of our Information Security Management System (ISMS). This involves regular reviews, audits, and updates to adapt to evolving threats, technological advancements, and business needs. We actively seek feedback from stakeholders to enhance our security posture.

## Policy Compliance, Exceptions and Non-Compliance

The information security management team will verify compliance with this policy through various methods, including business tool reports, audits, and feedback. Any exception to this policy must be approved and recorded by the Chief Information Security Officer (CISO) and reported to top management. Personnel who violate these policies may face disciplinary action, up to and including termination.

24SevenOffice commitment to security is public availability for all stakeholders at [www.24SevenOffice.com](http://www.24SevenOffice.com).