Information Security Policy

Policy governing information security in a high level.

SHA-256: 71e837e8fb14e91c2f1477a5b95d1fe525bdc1e0ac158af7a74778cc527dfe6d

Contents

Purpose
This document serves to describe Storegate AB's Information Security Policy.

Scope
This document applies to all information and communication technology that falls under the scope of the Information Security Management System (ISMS).

Users of this document are all employees and contractors of Storegate AB. Changes is done by authors within the Storegate Information Security Work Group (ISWG).

Key Principles
The key principles of adhering to the Information Security Policy are listed below:

- To create a culture of employee responsibility in relation to the handling and care of personal data and other confidential information
- To promote assurance and confidence in our customers
- To reduce the risk of confidential or sensitive information / documentation being stolen or accessed by unauthorized individuals which could damage the integrity of **Storegate**
- To help demonstrate compliance with Data Protection legislation

Information Security Policy

Storegate is a software company headquartered in Karlshamn, Sweden founded in 2003. Storegate offers cloud-based content security compliance and collaboration tools for businesses and the public sector. The platform offers a wide range of services such as, but not limited to, File sharing and content collaboration, Online backup, Digital signing, and ID-control on distance. Security is a key aspect of all its activity, and it is therefore vital that **Storegate** ensures that any information security risks to its ongoing business are mitigated.

To maintain Storegates competitive edge, cash flow, profitability, legal, regulatory, contractual compliance, and commercial image, the Board and management of the company are dedicated to maintaining the confidentiality, integrity, and availability of all physical and electronic information assets throughout the organization. Information and information security requirements will continue to be aligned with **Storegate** objectives and the Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information-related risks to acceptable levels.

The organization's current strategic business plan and information security strategy provide the context for identifying, assessing, evaluating, and controlling information-related risks through the establishment and maintenance of the ISMS. Information-related risks are to be identified and controlled via routine reviews of business operations and individual risk assessments of all changes within the business. The Board is responsible for the management and maintenance of risk treatment.

Business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are being reviewed and implemented where necessary supported by specific, documented policies and procedures as detailed in the information security strategy.

All employees of **Storegate** and certain external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy.

The ISMS is subject to continuous, systematic review and improvement as a living management framework.

Storegate has established an Information Security Working Group including executives/technical specialist's/risk specialists to support the ISMS framework and to periodically review the security policy.

Storegate is committed to achieving certification of its ISMS to ISO27001 standard upon completion of its implementation.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, "information security" is defined as:

Preserving
This means that management, all full time or part time staff, sub-contractors, project consultants and any external parties have, will be made aware of, their responsibilities to preserve information security, to report security breaches (in line with the policy and procedures) and to act in accordance with the requirements of the ISMS. All staff will receive information security awareness training and more specialized staff will receive appropriately specialized information security training.

The Confidentiality
This involves ensuring that information is only accessible to those authorized to access it and therefore to preventing both deliberate and accidental unauthorized access to **Storegate** information and its systems including networks, websites, portals, and other systems.

Integrity
This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial, or complete, destruction, or unauthorized modification, of either physical assets or electronic data. There must be appropriate contingency (for networks, web sites and other systems), data back-up plans, and security incident reporting. **Storegate** must comply with all relevant data-related legislation in those jurisdictions within which it operates.

And Availability
This means that information and associated assets should be accessible to authorized users when required and therefore physically secure. Information resources must be resilient, and **Storegate** must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems, and information. Disaster recovery and business continuity plans are to be reviewed, implemented, and documented to ensure appropriateness.

Of the physical (assets)
The physical assets of the **Storegate** including but not limited to computer hardware, filing systems and physical data files.

And information assets

The information assets include information printed or written on paper, transmitted by post, or shown in films, or spoken in conversation, as well as information stored electronically on servers, web site(s), intranet(s), PCs, laptops, and mobile phones as well as on USB sticks, backup media and any other digital or magnetic media, and information transmitted electronically by any means. In this context “data” also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.).

The ISMS is the Information Security Management System, of which this policy, the **information security manual** (“the Manual”) and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO27001:2022

A **SECURITY BREACH** is any incident or activity that causes or may cause a breakdown in the confidentiality, integrity, or availability of the physical or electronic information assets of the Organization.

All security breaches either actual or suspected, will be reported, and investigated in a structured and formal manner as detailed within the ISMS.

The **CEO** is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements of the standard.

A current version of this document is available to all employees on the **Storegate Common area**. It does not contain confidential information and can be released to relevant external parties.

This Information Security Policy was updated and approved by the **Storegate** ISWG, on **2026-04-23.**

Document Record

Change

Author	Date	Version	Change
Torbjörn Lindkvist & ISWG	20250403	1.1	Second revision
Torbjörn Lindkvist & ISWG	20260416	1.2	Third revision

Reviewers

Name	Date	Position
Axel Hermansen	20260420	CEO
Storegate ISWG	20260420	N/A

Approvers

Name	Date	Position
Axel Hermansen	20260423	CEO
Storegate ISWG	20260420	N/A

Distribution

Location	Date
Storegate Common	20260423

Information Security Policy 2026.pdf

This document was signed and sealed with timestamp 2026-04-23 13:01:08 (UTC). It contains the following original(s):

SG-ISMS-PO-1.2 Information Security Policy.pdf

124669 byte
SHA-256: 902d69237aa366166f8208b13b5e8ee4e5ab79ae7d5970da5814df0e18a27908

Signed by

Axel Hermansen

axel.hermansen@storegate.com
Signed with BankID (**Axel Ove Jörgen Hermansen**)
2026-04-23 12:59:27 (UTC)
Role: Signer
IP: 185.57.104.18

Verify the authenticity and integrity of this document by scanning the QR code on the left. You can also do it by visiting https://web1.storegate.com/share/signing/verify/71e837e8fb14e91c2f1477a5b95d1fe525bdc1e0ac158af7a74778cc527dfe6d

This document has been signed electronically in accordance with eIDAS, Regulation (EU) No 910/2014 of the European Parliament and of the Council through the Storegate signing service. Electronic signatures may not be denied legal effect or validity as evidence in legal proceedings. A qualified electronic signature has the same legal status as a signature written by hand. Storegate Signing is provided by Storegate AB, org. no. 556623-6179, Pirgatan 13, 374 35 Karlshamn, Sweden

storegate

SHA-256: 71e837e8fb14e91c2f1477a5b95d1fe525bdc1e0ac158af7a74778cc527dfe6d