Senbee A/S

Information Security Policy

Version: 1.0

Version Control

Version	Modified By	Date	Document Changes
1.0		5/5/2025	Policy created

Contents

1. Purpose

The purpose of this policy is to establish information security guidelines that will protect the confidentiality, integrity, and availability of the company's data.

2. Scope

This policy applies to all employees and third-party users.

3. Information Security Policy

3.1 Principles

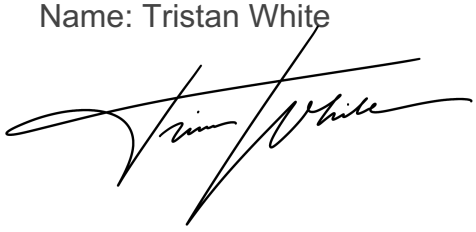
Information security is managed according to risk assessments, legal and regulatory requirements, and business needs.

3.2 Chief Executive's Statement of Commitment

"Information processing is fundamental to our company's success, and protecting the security of that information is a top priority at the executive level. Whether it is employee or customer data, we take our obligations under the GDPR and Data Protection Act 2018 very seriously. We have allocated the necessary resources to develop, implement, and continually improve our information security management system to meet the needs of our business."

Date: 5/5/2025

Name: Tristan White



3.3 Introduction

Information security is crucial for protecting the information entrusted to our organization. Failing to properly manage information security can have significant adverse impacts on our employees, customers, reputation, and finances. By implementing an effective information security management system, we can:

- Fulfill our legal, regulatory, and contractual obligations related to information security.
- Ensure the right people have the right access to the right data at the appropriate times.
- Provide proper protection for personal data as defined by the GDPR.
- Fulfill our responsibilities as good data citizens and custodians.

An effective information security management system allows us to safeguard the confidentiality, integrity, and availability of our information assets. This protects us from the potentially devastating consequences of data breaches, unauthorized access, information tampering, and service disruptions.

3.4 Information Security Defined

Information security is defined as the preservation of:

Confidentiality	Information access is granted to individuals with proper authorization. *Authorized access for the appropriate individuals.*
Integrity	Information is complete and accurate *for the appropriate data.*

Availability	Information is accessible as needed *at the right time.*

3.5 Information Security Objectives

The primary objectives of our information security program are:

- **Confidentiality, Integrity, and Availability**

  Ensure the confidentiality, integrity, and availability of all company information assets, including personal data as defined by the GDPR. This is achieved through a robust risk management approach that aligns with legal, regulatory, and contractual obligations, as well as business requirements.

- **Resource Information Security Management**

  Provide the necessary resources to develop, implement, and continually improve the organization's information security management system. This includes allocating appropriate funding, personnel, and technology to support effective information security practices.

- **Third-Party Risk Management**

  Effectively manage information security risks associated with third-party suppliers who process, store, or transmit company information. This involves implementing controls, monitoring, and ongoing risk assessment to reduce the likelihood and impact of security incidents.

- **Security Culture and Awareness**

  Foster a strong culture of information security and data protection through comprehensive training and awareness programs. Educate employees on their roles and responsibilities in safeguarding information assets and promote security-conscious behaviours across the organization.

3.6 Information Security Policy Framework

The information security management system is founded on an information security policy framework. Alongside this policy, the following policies constitute the framework:

- DP 01 **Data Protection Policy**
- DP 02 **Data Retention Policy**
- IS 01 **Information Security Policy** (this policy)
- IS 02 **Access Control Policy**
- IS 03 **Asset Management Policy**
- IS 04 **Risk Management Policy**
- IS 05 **Information Classification and Handling Policy**
- IS 06 **Information Security Awareness and Training Policy**
- IS 07 **Acceptable Use Policy**
- IS 08 **Clear Desk and Clear Screen Policy**
- IS 09 **Mobile and Teleworking Policy**
- IS 10 **Business Continuity Policy**
- IS 11 **Backup Policy**
- IS 12 **Malware and Antivirus Policy**
- IS 13 **Change Management Policy**
- IS 14 **Third Party Supplier Security Policy**
- IS 15 **Continual Improvement Policy**
- IS 16 **Logging and Monitoring Policy**
- IS 17 **Network Security Management Policy**
- IS 18 **Information Transfer Policy**
- IS 19 **Secure Development Policy**
- IS 20 **Physical and Environmental Security Policy**
- IS 21 **Cryptographic Key Management Policy**
- IS 22 **Cryptographic Control and Encryption Policy**
- IS 23 **Document and Record Policy**

3.7 Information Security Roles and Responsibilities

- ### Shared Responsibility

  Information security is the responsibility of everyone within the organization. All employees and third-party users are expected to understand and adhere to the relevant policies, follow established processes, and report any suspected or actual security breaches.

- ### Defined Roles and Responsibilities

  The specific roles and responsibilities for the effective operation of the Information Security Management System (ISMS) are clearly defined and documented in the "Information Security Roles Assigned and Responsibilities" document.

- ### Monitoring and Compliance

  Compliance with the policies and procedures of the ISMS is monitored through the Management Review Team. Additionally, independent reviews are conducted by both Internal and External Audit periodically.

- ### Legal and Regulatory Obligations

  The company takes its legal and regulatory obligations seriously. All applicable requirements are recorded in the "Legal and Contractual Requirements Register" to ensure comprehensive compliance.

- ## Training and Awareness

  Policies are readily and easily accessible to all employees and third-party users. A comprehensive training and communication plan is in place to educate personnel on the relevant policies, processes, and concepts of information security. Training needs are identified, and the associated requirements are captured in the **"Competency Matrix."**

4. Policy Compliance

4.1 Compliance Measurement

The Information Security Management team is responsible for verifying compliance with this policy through various methods, including but not limited to:

- Reviewing relevant business tool reports
- Conducting internal and external audits
- Obtaining feedback from the policy owner

4.2 Exceptions

Any exception to the requirements of this policy must be approved and recorded in advance by the Information Security Manager. All approved exceptions will be reported to the Management Review Team.

4.3 Non-Compliance

Employees found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

This policy is regularly updated and reviewed as part of the organization's continuous improvement process for the Information Security Management System.