Stansomatic Information Security Policy

Introduction

Information security is a critical component of our overall business strategy and is essential for protecting our information assets, ensuring business continuity and maintaining the trust of our customers and business partners. We are committed to complying with all relevant guidelines and regulations governing information security. We will regularly review and update our information security policy and controls to ensure compliance with these guidelines and regulations. In addition, we will monitor changes to regulations related to information security and adjust our policies and controls accordingly to maintain compliance.

The purpose of this Information Security Policy is to outline the requirements and responsibilities for protecting the confidentiality, integrity and availability of information and information systems within the company. The policy also establishes a framework for the implementation and review of information security controls.

This policy applies to all employees, business partners and third-party vendors who have access to the company's information systems and data. Suppliers or other business partners that violate information security policies and controls may receive a warning or in worst case scenarios, the contract between Stansomatic and you may be suspended or terminated. Stansomatic may pursue legal action against employees, suppliers or other business partners who violate information security policies and controls in a way that causes harm to the company, its customers or its partners.

It is the responsibility of all employees, business partners and third-party vendors to comply with this policy to ensure the security of the company's information assets.

Information Security Controls

The following information security controls are commitments that shall be implemented to protect the company's information systems and data:

a) Access Control: Access to information systems and data shall be granted only to authorized personnel on a need-to-know basis. Access controls shall be reviewed regularly, and any changes shall be documented and authorized by management.

b) Confidentiality: Confidentiality of company information shall always be maintained. Employees, business partners and third-party vendors shall sign a confidentiality agreement before being granted access to company information.
c) Data Protection: Company data shall be protected against unauthorized access, disclosure, modification or destruction. Data encryption and backup procedures shall be implemented to protect against data loss or theft. It is our goal to ensure that all critical data is encrypted both in transit and at rest.
d) Incident Management: The company shall have an incident management process in place to detect, respond to and recover from security incidents. All security incidents shall be reported to the information security officer immediately. We wish to reduce the average time to detect and respond to security incidents by 50% over the next year.
e) Physical Security: Physical access to information systems and data storage locations shall be controlled, monitored and protected against unauthorized access.
f) System Monitoring: Information systems shall be monitored to detect unauthorized access attempts, abnormal system behavior and security breaches.
g) Training and Awareness: All employees, business partners and third-party vendors shall receive information security training and awareness programs to ensure they understand their responsibilities and obligations regarding information security. It is our goal to increase the percentage of employees who complete information security training annually to 100%.

Risk Assessment

Information security risk assessments are a key component of our information security management policy. We will conduct regular risk assessments to identify potential threats and vulnerabilities to our information assets and evaluate the likelihood and potential impact of these risks. The results of these assessments will inform the development and implementation of appropriate and revised information security controls and measures to mitigate identified risks.

We will ensure that our risk assessments are conducted in a systematic and comprehensive manner, utilizing recognized frameworks and methodologies. Our risk assessments will consider a range of factors, including the sensitivity and criticality of our information assets, the potential impact of a breach or compromise and the likelihood and frequency of potential threats. We will also ensure that our risk assessments are conducted on a regular basis, with the frequency of assessments determined by the level of risk posed to our information assets. Our information security officer will be responsible for coordinating

and overseeing risk assessments and the results of these assessments will be documented and communicated to relevant stakeholders as appropriate.

Through our information security risk assessments, we will proactively identify and manage risks to our information assets, ensuring the continued protection, confidentiality and availability of our data and systems.

Review Process

The Information Security Policy shall be reviewed on an annual basis to ensure that it remains relevant and effective. The review process shall include the following steps:

a) Review of the policy by the information security officer to ensure that it is up to date and in compliance with relevant standards and regulations.
b) Consultation with key stakeholders, including IT and HR, to identify any changes or updates required.
c) Review and update of information security controls and procedures.
d) Approval of the updated policy by senior management.

Dedicated Responsibilities

The following individuals have dedicated responsibilities for information security within the company:

a) Information Security Officer: The information security officer is responsible for overseeing the implementation and management of information security controls.
b) IT Department: The IT department is responsible for implementing and maintaining information security controls for the company's information systems.
c) HR Department: The HR department is responsible for ensuring that all employees, business partners and third-party vendors receive information security training and awareness programs.

Stansomatic, 24-04-2023

_____

Søren Bahnsen
CEO