Section 2: Information Security Policy

2.1 Purpose and Scope

2.1.1 Purpose

The purpose of this top-level policy is to define the purpose, direction, principles, and basic rules for information security management at Smooth Sailing Solutions.

2.1.2 Scope

This policy applies to all employees, contractors, consultants, temporary and other workers at Smooth Sailing Solutions and its subsidiaries.

This policy is applied to the entire Information Security Management System (ISMS), as defined in the *ISMS Scope Document*.

2.2 Policy Statement

2.2.1 Objectives and Measurement

The general objectives for the information security management system are to create a better market image, conform Smooth Sailing Solutions to applicable regulations and legislation, increase user satisfaction, and reduce the number of security incidents and the damage they cause.

These goals are in line with our business objectives, strategy and business plans. EXECUTIVE-TYPE PERSON is responsible for reviewing these general ISMS objectives and setting new ones.

Objectives for individual security controls or groups of controls are proposed by INFOSEC, and approved by INFOSEC OVERLORD in the *Statement of Applicability*.

All the objectives must be reviewed at least once a year.

Smooth Sailing Solutions will measure the fulfillment of all the objectives. INFOSEC OVERLORD is responsible for setting the method for measuring the achievement of the objectives. The measurement will be performed at least once a year and IT OVERLORD will analyze and evaluate the measurement results and report them to EXECUTIVE-TYPE PERSON as input materials for the Management review.

2.2.2 Information Security Requirements

This policy and the entire ISMS must be compliant with legal and regulatory requirements relevant to Smooth Sailing Solutions in the areas of information security, data privacy, and business continuity, as well as with contractual obligations.

A detailed list of all contractual and legal requirements is provided in the *List of Legal, Regulatory, and Contractual Obligations*.

2.2.3 Information Security Controls

The process of selecting the controls (safeguards) is defined in the *Risk Assessment and Risk Treatment Methodology*. The selected controls, their specific implementing standards, and their implementation status are listed in the *Statement of Applicability*.

2.2.4 Implementing Standards

- *Acceptable Encryption Standard*
- *Acceptable Use Standard*
- *Acquisition Assessment Standard*
- *Audit Standard*
- *Baseline Workstation Configuration Standard*
- *Bluetooth Baseline Requirements Standard*
- *Certificate Practice Statement Standard*
- *Clean Desk Standard*
- *Data Classification Standard*
- *Database Credentials Coding Standard*
- *Digital Signature Acceptance Standard*
- *Disaster Recovery Standard*
- *DMZ Equipment Standard*
- *Email Standard*
- *Encryption End User Key Protection Standard*
- *HIPAA Workstation Security Standard*
- *Incident Response Standard*

- *Information Logging Standard*
- *Lab Security Standard*
- *Media Destruction Standard*
- *Minimum Access Standard*
- *Password Construction Standard*
- *Password Protection Standard*
- *Privacy Standard*
- *Records Retention Standard and Schedule*
- *Remote Access Standard*
- *Remote Access Tools Standard*
- *Router and Switch Security Standard*
- *Server Security Standard*
- *Social Media Standard*
- *Software Installation Standard*
- *Web Application Security Standard*
- *Wireless Communications Standard*
- *Security Response Plan Standard*

2.2.5 Business Continuity

Business Continuity management is prescribed in the *Business Continuity Policy*.

2.2.6 Responsibilities

1. EXECUTIVE-TYPE PERSON is responsible for ensuring that the ISMS is implemented and maintained according to this policy, and for ensuring all necessary resources for its implementation are available.
2. INFOSEC OVERLORD is responsible for operational coordination of the ISMS as well as for reporting about the performance of the ISMS.
3. Senior company management (e.g., Board of Directors) must review the ISMS at least annually, or each time a significant change occurs, and prepare minutes from that review meeting. The purpose of the management review is to establish the suitability, adequacy, and effectiveness of the ISMS.
4. The protection of integrity, availability, and confidentiality of assets is the responsibility of the owner of each asset.
5. All security incidents or weaknesses must be reported according to the *Incident Response Standard*.

6. COMMUNICATIONS OVERLORD will define which information related to information security will be communicated to which interested party (both internal and external), by whom and when.
7. TRAINING OVERLORD will implement information security training and awareness programs for employees. They are also responsible for adopting and implementing the *Information Security and Privacy Training and Awareness Plan*, which applies to all persons who have a role in information security management

2.2.7 Policy communication

INFOSEC OVERLORD must ensure that all employees of Smooth Sailing Solutions, as well as appropriate external parties, are familiar with this Policy.

2.2.8 Support for ISMS implementation

EXECUTIVE-TYPE PERSON hereby declares that ISMS implementation and continual improvement will be supported with adequate resources in order to achieve all objectives set in this Policy, as well as satisfy all identified requirements.

2.3 Policy Justification

The language and scope of this policy statement is designed to meet the requirements of section 5 of the ISO/IEC 27001 standard.

2.4 Compliance and Control

INFOSEC will verify compliance with this policy as indicated in the various implementing standards.

No exceptions to this policy are anticipated.

An employee found to have violated this policy, or the standards that implement it, may be subject to disciplinary action, up to and including termination of employment.

Section 2: *Information Security Policy* is a controlled document. While this document may be printed, the electronic version maintained on the Smooth Sailing Solutions POLICY DOCS LOCATION is the controlled copy. Any printed copies of this document are not controlled.

Document Section Classification: Internal Only

2.4.1 Reference Documents

- *ISO/IEC 27001 standard, clauses 5.2 and 5.3*
- *ISMS Scope Document*
- *Risk Assessment and Risk Treatment Methodology*
- *Statement of Applicability*
- *List of Legal, Regulatory, and Contractual Obligations*
- *Business Continuity Policy*
- *Information Security and Privacy Training and Awareness Plan*

2.4.2 Change Control

Table 2-1: Amendment History

Version	Date	Person	Description of Change
0.1	June 19 2019	T. Ryng	Initialization per template.

2.4.3 Review and Approval

This document is valid as of [date].

The owner of this document is indicated in Table 2-2. This person must review and, if necessary, update the document at least annually.

Table 2-2: Approval

Name	Title	Signature	Date
	EXECUTIVE-TYPE PERSON