SECTION 2: AUDIT STANDARD

2.1 Purpose and Scope

This standard implements the *Information Security Policy*.

2.1.1 Purpose

The purpose of this standard is to empower INFOSEC to perform periodic information security audits and risk assessments on any system at Smooth Sailing Solutions for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

Audits may be conducted to:

- Ensure integrity, confidentiality, and availability of information and resources,
- Ensure conformance to Smooth Sailing Solutions security policies, standards, and procedures,
- Monitor user or system activity where appropriate, or
- Investigate possible security incidents.

2.1.2 Scope

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

This standard applies to all computer and communication devices owned or operated by Smooth Sailing Solutions. This standard also covers any computer and communications device that are present on Smooth Sailing Solutions premises, but which may not be owned or operated by Smooth Sailing Solutions.

Security audits may be conducted on any entity within Smooth Sailing Solutions or any outside entity that has signed a Third Party Agreement with Smooth Sailing Solutions. Security audits may be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

2.2 Standard

When requested, and for the purpose of performing an audit, any access needed will be provided to members of INFOSEC.

This access may include:

- User level and/or system level access to any computing or communications device,
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on Smooth Sailing Solutions equipment or premises,
- Access to work areas (e.g., offices, cubicles, labs, storage areas, etc.),
- Access to interactively monitor and log traffic on Smooth Sailing Solutions networks.

The execution, development and implementation of remediation programs is the joint responsibility of INFOSEC and the department responsible for the system area being assessed. Employees are expected to cooperate fully with any security audit being conducted on systems for which they are held accountable. Employees are further expected to work with INFOSEC in the development of a remediation plan.

2.3 Compliance and Control

INFOSEC will verify compliance to this standard through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the standard must be approved by INFOSEC in advance.

An employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment.

Section 2: *Audit Standard* 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

2.3.1 Related Policies, Standards, and Procedures

- *Risk Assessment Procedures*
- Third Party Agreements

2.3.2 Change Control

Table 2-1: Amendment History

Version	Date	Person	Description of Change
0.1	June 06 2019	T. Ryng	Initialization per template.

2.3.3 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