SECTION 2: ACCEPTABLE USE STANDARD

2.1 Purpose and Scope

This standard implements the *Information Security Policy*.

2.1.1 Overview

INFOSEC's intentions for publishing an *Acceptable Use Standard* are not to impose restrictions that are contrary to Smooth Sailing Solutions's established culture of openness, trust and integrity. INFOSEC is committed to protecting Smooth Sailing Solutions's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Business computing systems provided for company users, including but not limited to computer or networking equipment, software, services or credentials, are the property of Smooth Sailing Solutions. These systems are to be used as defined in this standard in serving the interests of the company, and of our clients and customers in the course of normal operations.

Computer systems or services owned by third parties, including employees, contractors, or other agents may be used for business purposes in accordance with this standard.

Effective security is a team effort involving the participation and support of every Smooth Sailing Solutions employee and affiliate. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly.

2.1.2 Purpose

The purpose of this standard is to outline the acceptable use of computer equipment at Smooth Sailing Solutions. These rules are in place to protect both the employee and Smooth Sailing Solutions. Inappropriate use exposes Smooth Sailing Solutions to risks including virus attacks, compromise of network systems and services, and legal issues.

Outlining the circumstances for proper use of Smooth Sailing Solutions and services protects the employee in the use of equipment for personal, yet authorized, tasks and equipment.

2.1.3 Scope

This standard applies to the use of information, electronic and computing devices, and network resources to conduct Smooth Sailing Solutions business or interact with internal networks and business systems, whether owned or leased by Smooth Sailing Solutions, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Smooth Sailing Solutions and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Smooth Sailing Solutions policies and standards, and local laws and regulation. Exceptions to this policy are documented in Section 2.3: *Compliance and Control* on page 10.

This standard applies to employees, contractors, consultants, temporaries, and other workers at Smooth Sailing Solutions, including all personnel affiliated with third parties. This standard applies to all equipment that is owned or leased by Smooth Sailing Solutions.

2.2 Standard

2.2.1 General Use and Ownership

1. Smooth Sailing Solutions proprietary information stored on electronic and computing devices whether owned or leased by Smooth Sailing Solutions, the employee or a third party, remains the sole property of Smooth Sailing Solutions. You must ensure that proprietary information is protected in accordance with the *Data Classification Standard*.
2. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Smooth Sailing Solutions proprietary information.
3. You may access, use or share Smooth Sailing Solutions proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
4. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

5. For security and network maintenance purposes, authorized individuals within Smooth Sailing Solutions may monitor equipment, systems and network traffic at any time, per INFOSEC's *Audit Standard*.

2.2.2 Security and Proprietary Information

1. All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Standard*.
2. System level and user level passwords must comply with the *Password Standard*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
3. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
4. Postings by employees from a Smooth Sailing Solutions email address to public Internet forums, mailing lists, or other publications should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Smooth Sailing Solutions, unless posting is in the course of business duties.
5. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.
6. Users performing duties remotely must take reasonable precautions to protect sensitive materials and information from access by non-authorized personnel as though located in a physical company office.

2.2.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Smooth Sailing Solutions authorized to engage in any activity that is illegal under local, state, federal or international law while using Smooth Sailing Solutions-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

2.2.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Communication or activities that violate the *Code of Conduct* of the intended medium or platform, the Smooth Sailing Solutions *Ethics Standard*, or applicable standards of behavior regarding the abuse, discrimination, or persecution of any individual or group on the basis of race, ethnicity, gender identity or expression, religious affiliation, or other protected classes.
2. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Smooth Sailing Solutions.
3. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Smooth Sailing Solutions or the end user does not have an active license is strictly prohibited.
4. Accessing data, a server or an account for any purpose other than conducting Smooth Sailing Solutions business, even if you have authorized access, is prohibited.
5. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
6. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
7. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
8. Using a Smooth Sailing Solutions computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
9. Making fraudulent offers of products, items, or services originating from any Smooth Sailing Solutions account.
10. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

11. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
12. Port scanning or security scanning is expressly prohibited unless prior notification to INFOSEC is made.
13. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job or duty.
14. Circumventing user authentication or security of any host, network or account.
15. Introducing honeypots, honeynets, or similar technology on the Smooth Sailing Solutions network.
16. Interfering with or denying service to any user other than the employee's host (e.g., denial of service attack).
17. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
18. Providing information about, or lists of, Smooth Sailing Solutions employees to parties outside Smooth Sailing Solutions.

2.2.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT DEPARTMENT.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Smooth Sailing Solutions's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Smooth Sailing Solutions or connected via Smooth Sailing Solutions's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

2.2.3.3 Blogging and Social Media

1. Smooth Sailing Solutions's *Confidential Information Standard* also applies to blogging. As such, Employees are prohibited from revealing any Smooth Sailing Solutions confidential or proprietary information, trade secrets or any other material covered by Smooth Sailing Solutions's *Confidential Information Standard* when engaged in blogging.
2. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Smooth Sailing Solutions and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Smooth Sailing Solutions's *Non-Discrimination and Anti-Harassment Standard*.
3. Employees may also not attribute personal statements, opinions or beliefs to Smooth Sailing Solutions when engaged in blogging. Employees assume any and all risk associated with blogging.
4. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Smooth Sailing Solutions trademarks and logos, and any other Smooth Sailing Solutions intellectual property may also not be used in connection with personal social media activity except as noted below.
5. In the course of personal professional development and networking, it is expected and understood that employees and other users may disclose their professional relationship with Smooth Sailing Solutions, including the use of Smooth Sailing Solutions logos, published materials, and other intellectual property, so long as

this use does not disclose confidential information or the non-consensual use of information relating to or owned by individuals or companies affiliated with Smooth Sailing Solutions even if public.

2.3 Compliance and Control

The INFOSEC team 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 policy must be approved by the INFOSEC team 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: *Acceptable Use 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

- *Data Classification Standard*
- *Ethics Standard*
- *Minimum Access Standard*
- *Password Standard*
- *Remote Access Standard*
- *Remote Access Tools Standard*
- *Social Media Standard*

2.3.2 Change Control

Table 2-1: Amendment History

Version	Date	Person	Description of Change
0.1	May 22 2019	T. Ryng	Initialization per template.
0.2	June 05 2019	T. Ryng	Edits per M. Beland.
0.3	June 05 2019	T. Ryng	Edit per M. Beland.
0.4	June 10 2019	T. Ryng	Correct reference to *Data Classification Standard*.

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