Section 2: Data Classification Standard

2.1 Purpose and Scope

This standard implements the *Information Security Policy*.

2.1.1 Purpose

The purpose of this standard is to provide requirements for the classification and protection of Smooth Sailing Solutions information. The standard governs how information is classified based on its sensitivity, who may have access to the information, and how that information may be distributed, stored, and disposed of or destroyed.

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 information owned, processed, collected, or used by Smooth Sailing Solutions, whether electronic or printed.

2.2 Standard

2.2.1 Information Classifications

These information classifications define how all information (in any physical or electronic medium or format) is classified. The classes of information range from the information that needs the least protection (*Public Information*) to the information that needs the most protection (*Sensitive Information*).

When protecting information, rules associated with higher classes of information can be assigned to lower classes of information (i.e., *Sensitive Information* rules can be applied to *Restricted* data), but rules associated with lower classes of information cannot be assigned to higher classes of information (i.e., *Sensitive Information* cannot be protected with the rules for *Restricted* or *Internal Only Information*).

A single source of information (e.g., document, file, database, etc.) may contain information from more than one class. If the information cannot be segregated and protected separately, the single source must follow the restrictions of its highest information class.

Included with each definition is a listing of nonexclusive examples.

Table 2-1: Information Classifications

Definition	Examples
Public Information	
Information that does not fall within one of the more restrictive categories and that can be or has been made available to the public without any financial, legal, or other implications to Smooth Sailing Solutions.	• Information in the public domain • Information on Smooth Sailing Solutions public websites • Released press releases • Published marketing materials • Publicly filed documents
Internal Only Information	
Information that is not *Restricted* or *Sensitive*, and is not approved for general circulation outside Smooth Sailing Solutions, where its disclosure would inconvenience the company but is unlikely to result in significant financial loss or serious damage.	• Internal project reports • Minutes of management meetings • Unreleased press releases • Unpublished marketing materials • Competitive analysis • Internal non-proprietary policies, standards, or procedures
Restricted Information	
Information that is not *Sensitive*, but is considered critical to Smooth Sailing Solutions ongoing operations, and could seriously impede or disrupt them if disclosed without authorization or made available to the public.	• Client communications • Attorney files • Accounting information • Business plans

Table 2-1: Information Classifications (Continued)

Definition	Examples
Sensitive Information	
Any highly confidential internal information about clients, client customers, or employees, for which the loss of confidentiality, integrity, or availability could be expected to have an adverse effect on Smooth Sailing Solutions, could cause an individual harm if the information were to be misused, and would require public disclosure or notification to the affected individuals. The highest levels of integrity, confidentiality, and restricted availability are vital.	• Client or employee social security or tax identification numbers • Driver's license or state issued identification numbers • Financial or payment card information • Personal health information (PHI) • Passwords

2.2.2 Information Labeling

An appropriate set of procedures for information labeling shall be developed, implemented, and maintained by INFOSEC and IT DEPARTMENT in accordance with the classification scheme found above, both for electronic and for physical information.

The information owner is responsible for correctly classifying documents and files upon receiving or creating any document.

2.2.3 Access, Transmission, and Storage of Information

Appropriate procedures for information access and storage shall be developed, implemented, and maintained by INFOSEC and IT DEPARTMENT in accordance with the sections found below, both for electronic and for physical information.

2.2.3.1 Information Access

These access parameters define the internal and external users who can have access to Smooth Sailing Solutions information under the different classification levels.

Table 2-2: Access

Information Classification	Who May Access, and How
Public	All internal and external users.
Internal Only	Smooth Sailing Solutions employees, contractors, and external parties with approved access and a legitimate business purpose.
Restricted	• Only those Smooth Sailing Solutions employees designated with approved access and a legitimate business purpose. • Only those external parties (contractors, consultants and vendors) with approved access and a business need to know, and who are subject to contractual non-disclosure requirements (NDAs). • The access list must be reviewed at least quarterly by INFOSEC OVERLORD.
Sensitive	• Only those Smooth Sailing Solutions employees designated with approved access and a legitimate business purpose. • Only those Smooth Sailing Solutions contractors/vendors with management approved access and subject to contractual non-disclosure requirements (NDAs). • All external parties must have completed a INFOSEC security assessment. • Access list must be reviewed at least quarterly by INFOSEC OVERLORD.

2.2.3.2 Physical Transmission

How information may be transmitted in a physical format depends on its classification, whether the information exists as paper records or as physical media (e.g., backup tapes, CDs, etc.) that contain electronic information.

Table 2-3: Physical Transmission

Information Classification	Transmission Methods
Public	No restrictions.
Internal Only	• Standard interoffice mail and U.S. mail and other public or private carriers. • If physical media contains electronic data, then it also must be protected pursuant to Section 2.2.3.3: *Electronic Transmission*. • Only to authorized recipients (see Section 2.2.3.1: *Information Access*).
Restricted	• Standard interoffice mail and U.S. mail and other public or private carriers. • If delivered via carrier, then tracking number and/or receive receipt must be used. • If physical media contains electronic data, then it also must be protected pursuant to Section 2.2.3.3: *Electronic Transmission*. • Only to authorized recipients (see Section 2.2.3.1: *Information Access*).
Sensitive	• When possible, hand-deliver this information; otherwise, only send via standard interoffice mail or approved, bonded private carriers. • If delivered via carrier, package should be delivered directly to recipient and should require recipient's signature. • If delivered via interoffice, Information must be placed in sealed envelope prior to being placed in interoffice envelope and the recipient should be alerted of delivery in advance. • If physical media contains electronic data, then it also must be protected pursuant to Section 2.2.3.3: *Electronic Transmission*. • Only to authorized recipients (see Section 2.2.3.1: *Information Access*).

2.2.3.3 Electronic Transmission

How information may be transmitted when in an electronic format depends on its classification. This includes automated and computer-to-computer transfers of information.

For any assistance in using approved email or file transmission methods, or in password protecting or encrypting any files, please contact IT DEPARTMENT.

Table 2-4: Electronic Transmission

Information Classification	Transmission Methods
Public	No restrictions.
Internal Only	• Must send using approved email and electronic file transmission methods, such as work email or a secure FTP site that has been reviewed by INFOSEC. • Only to authorized recipients (see Section 2.2.3.1: *Information Access*).
Restricted	• Must send using approved email and electronic file transmission methods, such as work email or a secure FTP site that has been reviewed by INFOSEC. • Must not be sent via email unless the information is in an attachment that is password protected or encrypted (see *Encryption Standard*). • Only to authorized recipients (see Section 2.2.3.1: *Information Access*).
Sensitive	• Must not be sent wirelessly (access point or phone) or over public network unless data or transmission path is encrypted. See *Encryption Standard*. • May be sent over a secure FTP site that has been reviewed by INFOSEC. • Must not be sent via email unless the information is in an attachment that is encrypted. See *Encryption Standard*. • Only to authorized recipients (see Section 2.2.3.1: *Information Access*).

2.2.3.4 Physical Storage

How information may be physically stored depends on its classification, whether the information exists as paper records or as physical media (e.g., backup tapes, CDs, etc.) that contain electronic information.

Table 2-5: Physical Storage

Information Classification	Storage Methods
Public	No restrictions.
Internal Only	• Protect from inadvertent or unauthorized disclosures (keep from view, erase white boards, do not leave in view on desktops, etc.) • If physical media contains electronic data, then it also must be protected pursuant to Section 2.2.3.5: *Electronic Storage*. • Storage under lock and key recommended. • Only authorized users may have access (see Section 2.2.3.1: *Information Access*).
Restricted	• Protect from unauthorized access or disclosure. • If physical media contains electronic data, then it also must be protected pursuant to Section 2.2.3.5: *Electronic Storage*. • Storage under lock and key required. • Only authorized users may have access (see Section 2.2.3.1: *Information Access*). • Access list must be reviewed periodically by business owner.
Sensitive	• Access to or removal of information may only be granted with management approval. • If physical media contains electronic data, then it also must be protected pursuant to Section 2.2.3.5: *Electronic Storage*. • Must be kept under double lock and key (locked room or building inside of a locked container). • Access list must be reviewed on a quarterly basis by business owner. • Attempted or actual unauthorized access, use or disclosure must be immediately reported to the INFOSEC OVERLORD.

2.2.3.5 Electronic Storage

How information may be electronically stored depends on its classification.

Table 2-6: Electronic Storage

Information Classification	Storage Methods
Public	No restrictions.
Internal Only	• May be stored in unencrypted format. • Should have individual access controls where possible and appropriate. • Only authorized users may have access (see Section 2.2.3.1: *Information Access*).

Restricted	• May be stored in unencrypted format.
	• Must have the following access controls:
	  • Must have individual access controls that restrict access to active Users and active User account only;
	  • Must assign unique IDs and passwords, which are not vendor supplied defaults, to each Users; and
	  • When being accessed via a public network, login credentials may not be passed in clear text.
	• Only authorized users may have access (see Section 2.2.3.1: *Information Access*).
	• Access list must be reviewed periodically by business owner.

Sensitive	• Information must be encrypted. See *Encryption Standard*.
	• Must have the following access controls:
	  • Must have individual access controls that restrict access to active Users and active User account only;
	  • Must restrict access to those who need such information to perform their legitimate job duties;
	  • Must block access to any User ID after multiple unsuccessful attempts to gain access;
	  • Must assign unique IDs and passwords, which are not vendor-supplied defaults, to each User;
	  • When being accessed via a public network, login credentials may not be passed in clear text; and
	  • Access must be logged for a minimum of 30 days.
	• Access list must be reviewed on a quarterly basis by business owner.
	• Attempted or actual unauthorized access, use or disclosure must be immediately reported to the INFOSEC OVERLORD.

2.2.4 Disposal / Destruction

Information media must be disposed of or destroyed in accordance with the *Media Destruction Standard*. Minimum guidelines for each Information Classification may be found in the table below. The electronic media category includes physical media containing electronic data.

Table 2-7: Disposal and Destruction

Information Classification	Type	Disposal/Destruction Methods
Public	All	No restrictions.
Internal Only	Physical	Paper must be deposited in disposal bins on Smooth Sailing Solutions premises.
	Electronic	Electronic data must be erased or rendered most likely unreadable.
Restricted	Physical	Paper must be disposed of only in specially marked bins or shredded on Smooth Sailing Solutions premises; or disposed of by a third-party with a contractual obligation to adequately protect documents in transit and storage and then adequately rendered unreadable.
	Electronic	Electronic media must be disposed of only in specially marked bins on Smooth Sailing Solutions premises and will be completely erased and overwritten or rendered difficult to retrieve by a third party.
Sensitive	Physical	Paper must be disposed of only in specially marked bins or cross-cut shredded on Smooth Sailing Solutions premises; or disposed of by a third-party with a contractual obligation to adequately protect documents in transit and storage and then cross-cut shredded or otherwise adequately rendered unreadable. If shredded, the diameter should not exceed one-quarter of an inch.
	Electronic	Electronic media must be disposed of only in specially marked bins on Smooth Sailing Solutions premises and will be completely erased and overwritten or rendered reasonably unrecoverable by a third party.

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: *Data Classification 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

- *Acceptable Use Standard*
- *Clean Desk Standard*
- *Email Standard*
- *HIPAA Workstation Security Standard*
- *Media Destruction Standard*

2.3.2 Change Control

Table 2-8: Amendment History

Version	Date	Person	Description of Change
0.1	June 10 2019	T. Ryng	Initialization per template.
0.2	June 27 2019	T. Ryng	Reorganization of section, addition of procedures language to Section 2.2.3: *Access, Transmission, and Storage of Information*.

2.3.3 Review and Approval

This document is valid as of [date].

The owner of this document is indicated in Table 2-9. This person must review and, if necessary, update the document at least annually.

Table 2-9: Approval

Name	Title	Signature	Date