Section 2: Password Protection Standard

2.1 Purpose and Scope

This standard implements the *Information Security Policy*.

2.1.1 Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to Smooth Sailing Solutions systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.1.2 Purpose

The purpose of this standard is to provide protection of user passwords.

2.1.3 Scope

This standard applies to all personnel who have or are responsible for an account or any form of access that supports or requires a password on any system that resides at any Smooth Sailing Solutions facility, has access to the Smooth Sailing Solutions network, or stores any non-public Smooth Sailing Solutions information.

2.2 Standard

2.2.1 Password Creation

1. All user-level and system-level passwords must conform to the *Smooth Sailing Solutions Password Construction Standard*.

2. Users must use a separate, unique password for each of their work-related accounts.
3. Users may not use any work-related passwords for their own, personal accounts.
4. User accounts with system-level privileges granted through group memberships must have a unique password from all other accounts held by that user to access system-level privileges. In addition, INFOSEC highly recommends that some form of multi-factor authentication is used for any privileged accounts

2.2.2 Password Change

1. Passwords should be changed only when there is reason to believe a password has been compromised.
2. Password cracking or guessing may be performed on a periodic or random basis by INFOSEC or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the *Password Construction Standard*.

2.2.3 Password Protection

1. Passwords must not be shared with anyone, including supervisors and coworkers.
2. Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.
3. Passwords may be stored only in password managers authorized by Smooth Sailing Solutions.
4. Do not use the "Remember Password" feature of applications (e.g., web browsers).
5. Any user suspecting that their password may have been compromised must report the incident immediately and change all passwords.

2.2.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

1. Applications must support authentication of individual users, not groups.
2. Applications must not store passwords in clear text or in any easily reversible form.
3. Applications must not transmit passwords in clear text over the network.

4. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

2.2.5 Multi-Factor Authentication

Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work-related accounts but also for personal accounts.

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 policy 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: *Password Protection 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

Password Construction Standard

2.3.2 Change Control

Table 2-1: Amendment History

Version	Date	Person	Description of Change
0.1	June 03 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