



Security Policy

SFS Version 8.8

Introduction

This document provides guidelines regarding confidentiality, user authentication, and access control as well as best practices for the business units to use to secure SFS data (**Also See Appendix A**).

It is important to understand the SFS security structure consists of roles and permission lists. A permission list is a set of specific authorizations to perform a business task. A role can consist of multiple permission lists. In addition, other security functionality is attached to the role. Roles are assigned to a user profile.

SFS Version 8.8 Security Policy Guidelines

Guidelines for UW business units (BU)

Each UW Business Unit (BU) must designate a Security Coordinator for SFS operations. All BU requests for SFS security changes must be approved by the Security Coordinator who then submits the security change request to the UWSA Security Administrator. Each BU must also designate a secondary Security Coordinator who is authorized to submit security change requests to UWSA when the primary Security Coordinator is absent. The list of all primary and secondary BU Security Administrators will be maintained on the SFS web site.

Procedurally, when setting up a new user in SFS, the BU Security Administrators must request a 3-character login from DoIT at <http://www.doit.wisc.edu/restricted/authorization/3char.asp>.

The BU Security Coordinator must e-mail security changes to the UWSA Security Administrator. The security request must contain the full user name and user ID, and specify the nature of the request. The BU Security Administrator should be familiar with the access each permission list provides. PeopleSoft provides delivered reports to define page level access associated with each permission list. BU Security Administrators should request the appropriate level of security based on the campus business practices and the separation of duties employed. If the business practice does not allow for the proper separation of duties in relation to security roles needed, documentation for compensating controls must be provided to the Director Financial Reporting (See semi-annual "Certification of Adequate Separation of Duties").

If a current user profile exists that mirrors the user's requested security profile, this specific user ID should be provided in the e-mail.

When a new user is set up, they are assigned a temporary (default) password. The default password will be the same for all new users. The BU Security Administrator must ensure the new user's temporary password is replaced with a personal password within 2 business days from the original date of authorization.

The BU Security Administrator is required to verify and set up the User Preferences.

The BU Security Administrator must review SFS security access on an on-going basis to ensure proper authorization. Semiannually, the BU Security Administrator must certify access information by signing and submitting the SEC_ROLE nVision report pivot table.

Guidelines for the UWSA Security Administrator

The UWSA Security Administrator will maintain the permission lists and roles in SFS.

When a security request is received from a BU Security Coordinator, the UWSA Security Administrator reviews the request to verify appropriateness (if for new user or a change). Once authorized, s/he completes processing the request. The UWSA Security Administrator files all email requests from the BU Security Coordinators.

When the security change has been established in SFS, the UWSA Security Administrator contacts the BU Security Coordinator to inform him/her that their request has been completed. When a new user is set up or a password is

reset, the UWSA Security Administrator will check the 'Expire password at next login box' to ensure the user must enter a new password when they first log in to SFS.

The UWSA Security Administrator will verify whether a new user has replaced the default password with their personal password. If that change has not taken place within 2 business days after the SFS access was established, the UWSA Security Administrator will check the 'Account Locked Out?' box which will lock the user account. The BU Security Coordinator will have to request to have the account unlocked.

Guidelines for SFS Users

Users also have a responsibility for ensuring security over access to SFS. A list of procedural recommendations addresses this responsibility.

SFS Users must change the default password immediately.

SFS Users must change their passwords when expired. Any requests to reset a user password must go to the BU Security Administrator, who will forward it to the SFS Security Administrator.

SFS Users must not share User ID's or passwords with others.

SFS Users should lock workstation desktops or logout of SFS before leaving their work area. Although enabling a password protected screen saver with a fairly short wait time (5 minutes) is a good precaution, you should manually secure your desktop before you leave your computer.

Appendix A

SFS Version 8.8 Security Password Requirements/Controls

Guidelines	
1	<p>Password requirements:</p> <ul style="list-style-type: none"> • Length minimum is 6 characters. • Password should contain the following character types: <ul style="list-style-type: none"> ○ At least one uppercase Alphabetic (A-Z) ○ At least one lowercase Alphabetic (a-z) ○ At least one special character. ○ At least one number (0-9) • Password does not contain: <ul style="list-style-type: none"> ○ Any of your names (first, middle, last) ○ Your own user ID ○ Repetitive characters (sequences) <p>Names, person, places, or things found in a common dictionary</p>
2	Require password be changed every 180 days.
3	Lock access to the application after 5 failed signon attempts.
4	Prevent password reuse.
5	Business Unit Security Coordinator distributes passwords to users in a secure manner (either via telephone or site visit).
6	Change access rights to SFS when people's work assignments change or when they move to a different department or no longer require SFS access.
7	Terminate inactive SFS sessions. Inactive session timeout should not exceed 60 minutes.

Last Revised: 03/01/06

Revision Final

Title: SFS Security Guidelines

Author: SFS Functional User Group

File Reference: 8.8 Security Policy.doc