
STATE OF NEW YORK



Statewide Financial System (SFS) Security Policy

Version: 3.0

August 19, 2016

ABSTRACT

The security of information technology resources is a part of the internal controls necessary for the protection of all resources owned by the State of New York. Because of the sensitivity of computer based information, and the fact that information is not tangible, it must be treated in a fashion appropriate to its use and value.

The responsibilities and procedures contained in this policy document are a combination of the same standards and procedures applied within the Statewide Financial System, Office of the State Comptroller (OSC) and Division of the Budget (DOB). This document tailors the information to present what is required of individuals who have been designated to Administrate or Audit security or other sensitive data for the Statewide Financial System (SFS).

SFS Security Administration welcomes questions on the material in this policy document, or any other security matter. We may be reached via telephone at (518) 457-7737 or via e-mail at helpdesk@sfs.ny.gov.

Table of Contents

I information security Overview.....	4
II Definitions / Glossary	5
III User Access	5
IV Process Flow(s) and Description(s).....	7
V SFS Security Administration Reporting.....	9
VI Metrics.....	9
VII SFS Security Roles and Responsibilities.....	10

I INFORMATION SECURITY OVERVIEW

The objective of Statewide Financial System (SFS) security standards and procedures is to:

- Ensure the confidentiality, integrity, and availability of data.
- Prevent unauthorized modification, destruction or disclosure of data.
- Prevent unauthorized use of information technology resources, whether accidental or intentional.

Information technology resources are New York State assets. Access to them must be properly authorized, assigned and accounted for.

All users of SFS applications will be assigned to the appropriate security role(s) by the Agency Security Administrator (ASA), and will be restricted and monitored by that system. A detailed description of the ASA and SFS Security roles can be found in Section VII of this document.

The security implementation will have as its basis individual user accountability, built around password protection and server-side digital certificates, with the understanding that each individual user is solely responsible for, and will be held accountable for, any and all use of their SFS credentials.

The SFS Program takes a decentralized approach to the administration of the security system. Access by any user to SFS applications and data will be determined at the Agency level.

It is the expectation that Agencies have an internal control process in place to monitor ASA activities.

Violations and security breaches are logged and reported by ASAs or Internal Control Officers to the SFS Information Security Officer. Standards and procedures detail actions to be taken in the event of violations and/or security breaches, which may lead to prosecution as a criminal offense.

II DEFINITIONS / GLOSSARY

SFS ROLE ASSIGNMENT

SFS security is provisioned based upon *technical role* assignment. However, identifying *functional roles* is the first step in the role assignment process. After the validation of the roles has occurred, they will be used for three primary downstream activities:

- Functional roles are mapped to technical roles which provide security access based on the job tasks a given role is to perform in the SFS.
- Users are mapped to functional roles which in turn links them with the appropriate security access (users may be mapped to more than one functional role).
- Verification of role assignment occurs via role audits that are conducted by ASAs, Internal Control Officers, and SFS Security to identify any concerns regarding segregation of duties.

A listing of all SFS functional roles is maintained by the SFS Security team and provided on SFS Secure for agencies along with a Separation of Duties matrix and a Role Guide narrative.

New roles and changes to existing roles will only occur via business cases approved by the SFS Change Management process. Any requests to change SFS functional role definitions must be initiated by Agency Security Administrators (ASAs) and forwarded to HelpDesk@sfs.ny.gov, accompanied by a detailed business case and impact summary. The business case must be approved by the requesting Agency's Director or Commissioner. Any requests to create new functional roles should follow the same process as requests for changes to functional role definitions.

III USER ACCESS

PRODUCTION SYSTEM

- Once a user has access to the production system, changes to that user's SFS access will be processed by SFS and must be initiated by an Agency Security Administrator (ASA).
- It is the responsibility of the Agency to provide training for users who are granted access to the SFS production environment. When an ASA requests access to SFS Production for a user, the ASA is validating that the user has or will receive the appropriate training to access and use the system.
- The Service Level Agreement for processing user access changes submitted by ASAs is Priority 3, which is 2-5 business days from the date of the request.
- Users will be loaded into the production system from information provided by each Agency.

- Production user access will be updated from ASA-initiated requests following one of three processes:
 - Online using ASA Role Self-Service
 - Online using Magic Self Service
(recommended only if ASA Role Self-Service is unavailable)
 - Upon receipt of an email to HelpDesk@sfs.ny.gov
(only if Magic Self Service is unavailable to the ASA performing the request)

VALIDATION OF ASA SUBMISSIONS

- It is expected that each Agency has internal procedures that ensure effective communication between their Human Resource staff and SFS ASAs. These processes should ensure that before an ASA submits a request to create, change, or remove a user they have validated the following information prior to their incident submission to SFS:
 - NYSDS ids are validated with the PODA/PODSA at their Agency
 - Employee Ids are correctly associated upon confirmation with the Agency Employee Data Administrator
 - Email addresses are validated prior to submission to SFS and upon receipt of the user's credentials
 - Before submitting a new user, it is validated that the user does not already have an existing account in SFS
 - Removals are submitted timely to the date the user is separating from the Agency
 - Account access aligns with the users assigned tasks in SFS.
- Agency Security Administrators can use the employee data and role queries available at SFS Applications>SFS Financials>Reporting Tools>Query>Query Viewer to validate their Security submissions.
- Ensure that you are not duplicating another Agency Security Administrator's submission.
- Where possible consolidate daily requests into a single daily submission for your Agency.
- It is expected that Agency Internal Control Officers are responsible for the monitoring of Agency Security Administrator activity and will run queries from SFS or request activity data from SFS Security as needed to meet their monitoring needs.

IV PROCESS FLOW(S) AND DESCRIPTION(S)

SFS USER CREATION OR CHANGE REQUESTS

SFS user maintenance is administered by each Agency Security Administrator (ASA). For user changes:

1. ASA's will utilize role self service to initiate new users and/or changes to existing users. ASA's should follow the guidance in the job aids posted on SFS Secure under Agency Security Administration when adding and updating existing users. This tool is the recommended method for security submissions as it contains many validations as well as is configured specifically to each ASAs designated authorizations for provisioning.
2. If a change cannot be initiated via the ASA Self-Service tool, ASAs should complete and sign the SFS Agency User Access form (signed PDF) and attach the form to a Security request in either Magic Self Service or to an SFS Help Desk email. In addition to the PDF the request must contain complete details to initiate the change, such as a complete description of the change, and an accompanying Security Mass Upload Excel file in its entirety, including the following required data elements:
 - a. Reason Code
 - b. User name
 - c. NYSDS ID
 - d. Employee ID
 - e. User SFS role assignments
2. Once an Agency Security Administrator has created the PDF and Excel files, the appropriate ASA will log in to Magic Self Service and log an incident using the appropriate quick ticket for Form submissions titled "ASA ACCESS REQUEST".
 - a. The ASA will validate that both the PDF and Excel file is attached to their incident submission
****NOTE: SFS Security will reject all form incident submissions that do not include all the required elements noted above.**
3. SFS user requests for status on changes to assigned roles should be directed to the designated ASAs.
 - ASAs should look up requests within ASA Self Service or Magic Self Service for status on requested user changes. If any questions arise, contact the SFS Help Desk or initiate an incident via Magic Self Service.

USER CREDENTIALS

SFS user credentials are administered by each Agency Security Administrator (ASA).

1. For mass password reset requests, the ASA will send a spreadsheet of 10 or more users for mass reset and SFS Security will issue a secure file containing the new credentials. A follow up communication will provide the password to open the Secure file.
2. ASAs will securely distribute credentials to their agencies' users.
3. ASAs have the ability to reset passwords and unlock accounts for new and existing users who are members of the data permission(s) for which the ASA is authorized to administer. This ASA Self Service tool will create system generated passwords and email them to users based on the email information provided within SFS.
4. SFS user requests for status on credentials should be directed to the designated ASAs.
 - ASAs have the ability to look up requests within ASA Self Service and Magic Self Service for status on requests for new user requests or assistance with password changes or account unlocks. If any questions arise, contact the SFS Help Desk.

SFS AGENCY ADMINISTRATION MONITORING

It is expected that each Agency has a procedure in place for Internal Controls monitoring of ASA activities. SFS offers Internal Control Officer workshops and real time queries that enable monitoring of Security, Employee Data and Credit Card Administration activities at each agency.

1. Access to real time reports on Agency Administration can be provisioned using the ZZ Reports role in SFS which grants access to the Agency Administrator Queries. This access can be granted by Agency Security Administrators via ASA Role Self Service.
2. Access to Separation of Duties and Agency Security Administrator activity reporting can be granted via assignment of the Internal Control Officer View role. This role must be requested by the Agency Head or delegate via a signed form submitted to SFS. This form is available on SFS Secure.

PRODUCTION: PROCEDURE FOR CHANGES TO FUNCTIONAL ROLE ASSIGNMENTS

Creation of new functional roles and changes to existing functional roles cannot be made without approval of the SFS Change Management process.

Any requests to change SFS functional role definitions must be initiated by Agency Security Administrators and forwarded to HelpDesk@sfs.ny.gov, accompanied by a detailed business case and impact summary. The business case must be approved by the requesting Agency's Director or Commissioner. Any requests to create new functional roles should follow the same process as requests for changes to functional role definitions.

The SFS Security team, with input from the SFS Information Security Officer, will review and perform impact analysis on the requests and will initiate the SFS Scope Change process.

If approved, the changes will be made within the SFS Change Management process approved time frame. Notification of any role updates will be published to SFS Security Administrators and SFS users as needed.

V SFS SECURITY ADMINISTRATION REPORTING

The SFS Security team is responsible for initiating and reviewing reports generated as a result of audits and research into PeopleSoft and integrated systems and will address any findings that reflect potential vulnerabilities in these systems.

All Agency Security Administrators have the ability to run reports against their users real time within SFS by navigating to SFS Applications>SFS Financials>Reporting Tools>Query>Query Viewer and searching on %ROLE%. This will show them all role-related security queries.

Requests for ad hoc security reports should be requested through Magic Self Service using the Security Issue Template. If a report is being requested to be given to an individual who is not authorized with in SFS to receive the data type, the request must come from the Chief Financial Officer or another authorized party such as a person who is currently designated with the Agency Security Administrator or Internal Control Officer View role within SFS.

The SFS Security team will report any breaches or suspicious user activity to the SFS Information Security Officer for appropriate action up to and including prosecution.

SFS Security reserves the right to initiate audits on user accounts and will perform actions deemed necessary to provide protection to SFS and its assets.

User account inactivation is at the discretion of the SFS Program and can be performed without prior notice to users of the Statewide Financial System.

Agency Security Administrator identities will not be published by SFS due to confidentiality concerns. Agencies should be careful about publishing ASA identities due to potential security threats such as phishing scams. If an Agency Security Administrator receives a communication from an entity other than SFS asking for ASA detailed information they should confirm with SFS and or their ICO before responding to the inquiry.

VI METRICS

Periodically (at least one time annually) the SFS Security team will provide each Agency Security Administrator with a report of all their Agency's users and roles to review and approve.

Agency Security Administrators will utilize real time reporting within the SFS as needed to respond to audit inquiries and to validate data integrity based on employee movement.

Internal Control Officers will monitor the staff performing SFS administration and provide sign off at least once each fiscal year that they have validated the Security assigned by the Agency Security Administrator and performed periodic activity audits.

Agency Chief Financial Officers (CFO) will validate Agency Security Administrator and Internal Control Officer View role assignments at least annually.

VII SFS SECURITY ROLES AND RESPONSIBILITIES

SFS SECURITY TEAM

The SFS Security Team resides within the SFS Operations Unit, under the direction of the SFS Operations Manager.

SFS SECURITY TEAM RESPONSIBILITIES

Responsibilities of the SFS Security Team include:

1. Develop standard security procedures for all users internal and external to the SFS.
2. Administer security within the guidelines of the SFS security policies, standards, and procedures and in support of OSC Enterprise Information Security Office (EISO) security standards.
3. Ensure that access to data and resources is authorized and accountability for the access is assigned and maintained.

AGENCY SECURITY ADMINISTRATOR

DESIGNATION OF AGENCY SECURITY ADMINISTRATOR

Proper use and control of resources is a responsibility of management at an Agency or facility. For each Agency/facility connected to an SFS application, system or network, this responsibility will be discharged through one or more Agency Security Administrators (ASAs), acting as management's representative. All Agencies should designate backup Agency Security Administrator(s) to account for on leave scenarios. If all Agency Security Administrators are unavailable, responsibility for any needed action will revert to the Agency Head or Chief Fiscal Officer to advise SFS a user update is authorized.

An Agency Security Administrator (ASA) shall be designated by each Agency for SFS applications utilized by the Agency. ***This is not a clerical activity.*** SFS strongly recommends that only

personnel with knowledge of SFS functionality and its relationship to Agency human resource and security processes be appointed. Depending on the Agency's organization, the same person may be designated for multiple business unit, or responsibility for each business unit may be split among several people. Designations are to be made in writing by the Agency Head, or by the Chief Fiscal Officer in the Agency.

Since the ASA is the designated representative of management at the Agency, a new designation must be made if the current Administrator leaves the Agency, or is no longer able to perform this duty.

The SFS Information Security Officer, and/or SFS Security Team reserve the right to require an Agency or facility to designate a new ASA.

A new or changed designation shall be made by completing and submitting the Agency Security Administrator (ASA) Designation Form.

All ASA Designation Forms are to be addressed and mailed as follows:

Via U.S. Mail: Statewide Financial System

SFS Security
Building 5, Floor 3
1220 Washington Avenue
Albany, NY 12226-1900

Forms can also be sent via interoffice mail.

AGENCY SECURITY ADMINISTRATOR RESPONSIBILITIES

Responsibilities of the Agency Security Administrator (ASA) include:

1. Comply with the SFS Information Security Officer and SFS Security Team guidelines of security policies, standards and procedures.
2. Ensure that access to data and resources is authorized and accountability for the access is assigned and maintained.
3. Request via ASA Self Service or Magic Self Service, SFS Security to add, delete, modify user roles, or reactivate access for users within assigned roles when a change in the user's status occurs (e.g., resignation, leave, employee agency transfer, change of work assignment, etc.).
4. Follow required SFS guidelines for use of ASA Self Service, form submission and inquiry requests.
5. Reset passwords and lock/unlock accounts for end users within their designated data permission(s). See Job Aids available on SFS Secure for full procedures.
6. Assist Agency SFS users with password and logon issues.
7. Ensure that confidential electronic files containing initial login credentials are kept in a secure location and issued only to the user.

8. ASAs must securely dispose of the confidential login credential file once credentials are communicated to users.
9. Report online password reset functionality failures to SFS via Magic Self Service incident or by emailing HelpDesk@sfs.ny.gov.
10. Work with the Agency's Internal Control Office to validate user access permission guidelines; user access should not be in conflict with legislation and separation of duties requirements. See [SFS Secure](#) for the the Role Restrictions matrix and Separation of Duties guidance. See the OSC website for guidance provided in the [Guide for Financial Operations](#).
11. Quarterly review and yearly return of periodic user access and role assignment audits.
12. Notify the SFS Program of any suspected abuse or breaches in security related to access to the SFS.
13. Be familiar with all of the job aids related to the ASA duties marked with ADM or ASA as the module on the SFS Job Aid website within the SFS Secure website.

DESIGNATION OF AGENCY INTERNAL CONTROL OFFICER VIEW ACCESS

Proper use and control of resources is a responsibility of management at an Agency or facility. For each Agency/facility connected to an SFS application, system or network, this responsibility will be discharged through one or more Agency Security Administrators (ASAs), acting as management's representative. All Agencies should designate internal audit access to monitor ASA activities as appropriate.

Agency Internal Control Officers and Internal Audit staff may be designated by each Agency to receive access to real time queries for use in monitoring Administrator activities including but not limited to Separation of Duties concerns and ASA activity reports. ***This is not a clerical activity.*** SFS strongly recommends processes and procedures be implemented around monitoring as an audit best practice related to financial reporting. Depending on the Agency's organization, the same person may be designated for multiple business unit, or responsibility for each business unit may be split among several people. Designations are to be made in writing by the Agency Head, or by the Chief Fiscal Officer in the Agency.

Since the ICO is a designated representative of management at the Agency, a new designation must be made if the current ICO leaves the Agency, or is no longer able to perform this duty.

The SFS Information Security Officer, and/or SFS Security Team reserve the right to require an Agency or facility to designate a new ICO.

A new or changed designation shall be made by completing and submitting the Agency Internal Control Officer View (ICO) Designation Form.

All ICO View Designation Forms are to be addressed and mailed as follows:

Via U.S. Mail: **Statewide Financial System**
SFS Security
Building 5, Floor 3
1220 Washington Avenue
Albany, NY 12226-1900

Forms can also be sent via interoffice mail.

AGENCY INTERNAL CONTROL OFFICER RESPONSIBILITIES

Responsibilities of the Internal Control Officer (ICO) include:

1. Comply with the SFS Information Security Officer and SFS Security Team guidelines of security policies, standards and procedures.
2. Monitor Agency Administrator activities to ensure that access to data and resources is authorized and accountability for the access is assigned and maintained.
3. Follow required SFS guidelines for use of real time Administrator queries.
4. Monitor Agency Administrator activities to ensure that confidential electronic files containing initial login credentials are kept in a secure location and issued only to the user.
5. Monitor ASAs to ensure they securely dispose of the confidential login credential file once credentials are communicated to users.
6. Work with the Agency's Security Administrators to validate user access permission guidelines; user access should not be in conflict with legislation and separation of duties requirements. See [SFS Secure](#) for the the Role Restrictions matrix and Separation of Duties guidance. See the OSC website for guidance provided in the [Guide for Financial Operations](#).
7. Quarterly review and yearly return of periodic user access and role assignment audits.
8. Notify the SFS Program of any suspected abuse or breaches in security related to access to the SFS.
9. Be familiar with all of the job aids related to the ASA duties marked with ADM or ASA as the module on the SFS Job Aid website within the SFS Secure website to ensure that Administrators comply with security standards and make use of available tools.

STATEWIDE FINANCIAL SYSTEM USERS

SFS users include any person with access to the SFS. All SFS users are provided with the ability to reset their password online.

SFS USER RESPONSIBILITIES

SFS user responsibilities include:

1. Be familiar with the information contained in the SFS Security User's Guide regarding SFS policy, procedures and system utilization.
2. Create a shared secret upon initial sign on to allow for online password resets capability.
3. Validate that your email address associated to your account is correct. If the address is incorrect, please correct.
4. Be familiar with the related SFS Job Aid material related to your assigned roles. SFS Job Aids are located on the SFS Secure site.
5. Sign on using only the credentials assigned to the user, sign off at completion of the session, and not leave unattended a device that is signed on. Use of another person's credentials for any reason is considered a security risk. The owner of an account will be held liable for any account misuse.
6. Keep all passwords used to access information technology resources confidential.
 - a. All passwords should be memorized and never written down as a reference.
7. Revise the password as required by SFS security policy.
8. Contact your Agency Security Administrator for any login issues.
9. Utilize online password reset functionality when unable to sign on to the system (e.g., forgotten password, inactive too long, etc.).
10. Immediately notify the appropriate Agency Security Administrator or Internal Control Officer of suspected abuse of an ID and password.