SFS Security Updates
*** An Overview for NYSICA ***

September 27, 2018

Agenda / Key Takeaways for Today

- Annual User and Role Validations (Quarterly Report Improvements project)

- External Audit
    - Attachments within ASA Self-Service
    - Attachments within Annual User and Role Validations

- Travel Proxy Tool Updates

- Security Lessons Learned

- Questions

- References for Your Use

Annual User and Role Validations

Kristen Pelcher

Importance of Annual Review

Why is it important to you and SFS:

- To ensure confidentiality, integrity and availability of the data in the SFS by your periodic review of user and role information.

- OSC is subject to an Annual Financial Audit to which SFS is included. Each agency that uses SFS is subject to be included in the audit. You are responsible for the compliance review of user and role information for your agency.

- Critical success factors for the Annual Financial Audit are:
  - Timely review and maintaining the documentation related to the review.
  - Your agency maintaining documentation around user provisioning.

STATEWIDE FINANCIAL SYSTEM

Annual User and Role Validations

- SFS has implemented an online solution for the quarterly reports process beginning this fiscal year. 4/1/18.

- Static files are no longer being distributed.
  - Agencies must use real-time queries to complete reviews online.
  - A new work center has been deployed for easy access.
  - Sign off form are now completed online
    - Snail-mail of forms will no longer be required

  - A mapping exercise was deployed to agencies requesting 100% compliance. Every agency must map at least one ASA, Financial Certifier, and Compliance Reviewer in SFS.

  - **If your agency does not have someone mapped to each of these roles, your agency will be unable to provide the required sign off.**

STATEWIDE FINANCIAL SYSTEM
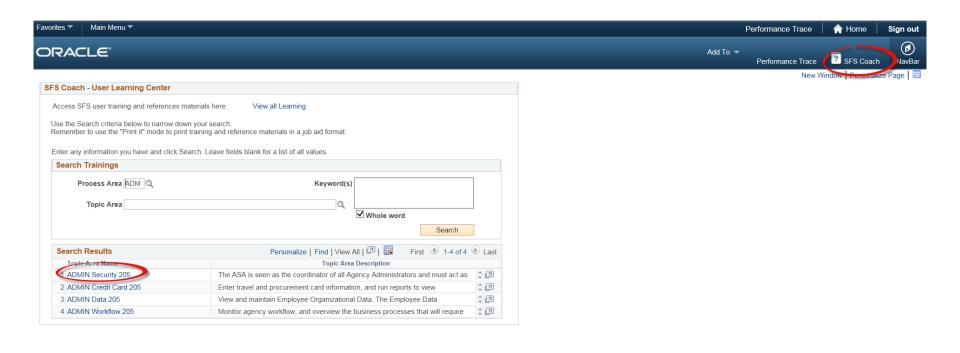
Updated Training Materials

- Self-Paced Training in SFS Coach
  - Process Area: ADM
    - ADMIN Security 205
    - Compliance Reviewer 205
    - Financial Certifier 205

- The "print it" function within SFS Coach will print the training in the same format as the job aids.
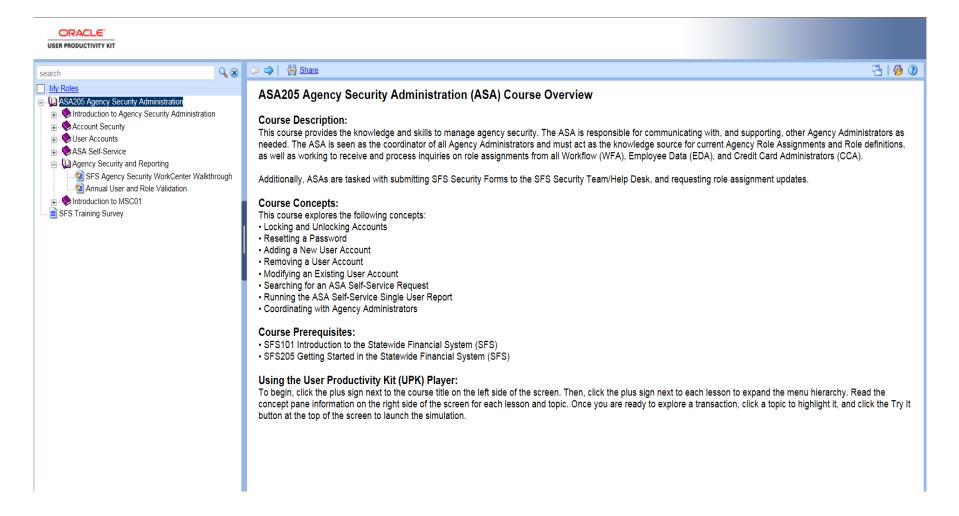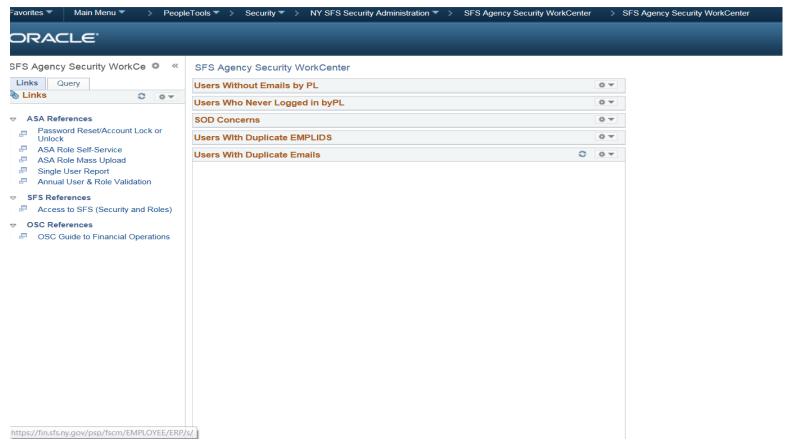
Updated Training Materials - SFS Coach

Statewide Financial System (Internal Use Only).
Contents subject to change.

SFS Coach

ORACLE
USER PRODUCTIVITY KIT

search 🔍 ⊗

☐ My Roles
⊟ 📖 ASA205 Agency Security Administration
  ⊞ ◆ Introduction to Agency Security Administration
  ⊞ ◆ Account Security
  ⊞ ◆ User Accounts
  ⊞ ◆ ASA Self-Service
  ⊟ 📖 Agency Security and Reporting
      📄 SFS Agency Security WorkCenter Walkthrough
      📄 Annual User and Role Validation
  ⊞ ◆ Introduction to MSC01
  📄 SFS Training Survey

⇦ ⇨ | 👥 Share

ASA205 Agency Security Administration (ASA) Course Overview

Course Description:
This course provides the knowledge and skills to manage agency security. The ASA is responsible for communicating with, and supporting, other Agency Administrators as needed. The ASA is seen as the coordinator of all Agency Administrators and must act as the knowledge source for current Agency Role Assignments and Role definitions, as well as working to receive and process inquiries on role assignments from all Workflow (WFA), Employee Data (EDA), and Credit Card Administrators (CCA).

Additionally, ASAs are tasked with submitting SFS Security Forms to the SFS Security Team/Help Desk, and requesting role assignment updates.

Course Concepts:
This course explores the following concepts:
• Locking and Unlocking Accounts
• Resetting a Password
• Adding a New User Account
• Removing a User Account
• Modifying an Existing User Account
• Searching for an ASA Self-Service Request
• Running the ASA Self-Service Single User Report
• Coordinating with Agency Administrators

Course Prerequisites:
• SFS101 Introduction to the Statewide Financial System (SFS)
• SFS205 Getting Started in the Statewide Financial System (SFS)

Using the User Productivity Kit (UPK) Player:
To begin, click the plus sign next to the course title on the left side of the screen. Then, click the plus sign next to each lesson to expand the menu hierarchy. Read the concept pane information on the right side of the screen for each lesson and topic. Once you are ready to explore a transaction, click a topic to highlight it, and click the Try It button at the top of the screen to launch the simulation.

Statewide Financial System (Internal Use Only).
Contents subject to change.

STATEWIDE FINANCIAL SYSTEM

Annual User and Role Validations

- SFS Agency Security WorkCenter

Statewide Financial System (External Use Only).
Contents subject to change.

Annual User and Role Validations

- ASA Section

Statewide Financial System (External Use Only).
Contents subject to change.

Annual User and Role Validations

- Compliance Reviewer & Financial Certifier sections:

Compliance Reviewer

☐ I have reviewed the reports generated by the ASA. Any updates to SFS Security were validated and submitted if updates were required.

☐ I am aware of the available queries to monitor Administrator activity within SFS. In addition I am aware of the SFS published SFS Internal Control Compliance Review and the Agency Security Maintenance Procedure

Please select one of the following:

☐ In accordance with OSC Advisory 28, I have validated there are no separation of duties concerns. I have reviewed the listing of users provided and have reviewed any Separation of Duties Concerns with the Agency Security Administrator. Any updates required in relation to SOD Concerns were validated and submitted by the ASA.

☐ I have reviewed the listing of users provided and accept that some Separation of Duties concerns exist. Compensating controls are implemented, such as monitoring, for the areas where role mapping cannot be updated at this time.

Compliance Reviewer:

Email:

[Sign and Verify]   **Signed:**

Financial Certifier

☐ I acknowledge the generation of the SFS User & Role Validation Reports and have validated that the list of Agency Security Administrators and Compliance Reviewers assigned is up to date. If any corrections to assignment are required, I am aware of the process to update the required designations.

Financial Certifier:

Email:

[Sign and Verify]   **Signed:**

Comments [   ]   [Reject & Delete Validation]

[💾 Save]

SFS STATEWIDE FINANCIAL SYSTEM

Annual User and Role Validations

- Each quarter, SFS distributes an email to all agencies as a reminder that SFS user and role validation must be completed at least once annually.

- Your agency can decide when it is most appropriate for your agency to complete the review.
  - You may choose to complete the review more than once a year.
  - Refer to the Agency Role Guide on SFS Secure to ensure you have the most updated guidance.

Yearly Follow-up Cycle

- October: SFS sends reminder email to ASAs for agencies who have not completed annual sign-off

- January: SFS sends follow-up email to ASAs <u>AND</u> Internal Control Officers

- February: SFS conducts phone outreach to ASAs

- **<u>March: Escalation via phone call to agency Chief Financial Officer</u>**

Reminders: Annual User and Role Validations

- Ensure that your agency:
  - Is aware of new training materials

  - Has mapped to all the required roles

  - Built the new roles into your onboarding, off-boarding and transfer processes

  - Ensure your separation processes for retirement, transfer, and terminations have immediate notification to your SFS Admin team

External Audit

Roger Aucoin and Kristen Pelcher

External Audit

- As a reminder, any agency with ability to provision users to the SFS is subject to external audit.
- Your agency may be selected for the Annual Financial Audit and you will be required to provide documentation for user and role provisioning and your annual user and role reviews.

- Ensure you have required documentation in relation to:
  - Annual user and role review:
    - Spreadsheets
    - Email correspondence
    - Notify your ASA of your review outcome so changes are made within 30 days of review
  - User provisioning processes:
    - Refer to the following resource materials on SFS*Secure*
      - SFS Agency Security Maintenance Procedure
      - SFS User Provisioning Request Form

Attachments within ASA Self-Service

- ASA Self Service will now require attachments that support the details of the provisioning changes being requested and the needed approvals.
  - User provisioning form or email correspondence documenting approval of changes

- Compliance Reviewers and Financial Certifiers will be provided with inquiry access to the ASA self-service request page so that they can review user provisioning requests and attachments and approver details provided on the requests.

- Agencies are responsible for ensuring that the documentation attached supports the changes being requested.

- Benefits: Having the supporting documentation attached to each request ensures that all information related to the request is available upon external audit.

Enhancement - Attachments

- There are two areas on the ASA self-service page to provide attachments:
  - Attached File for All User Requests

  - Attached File for Single Request Only

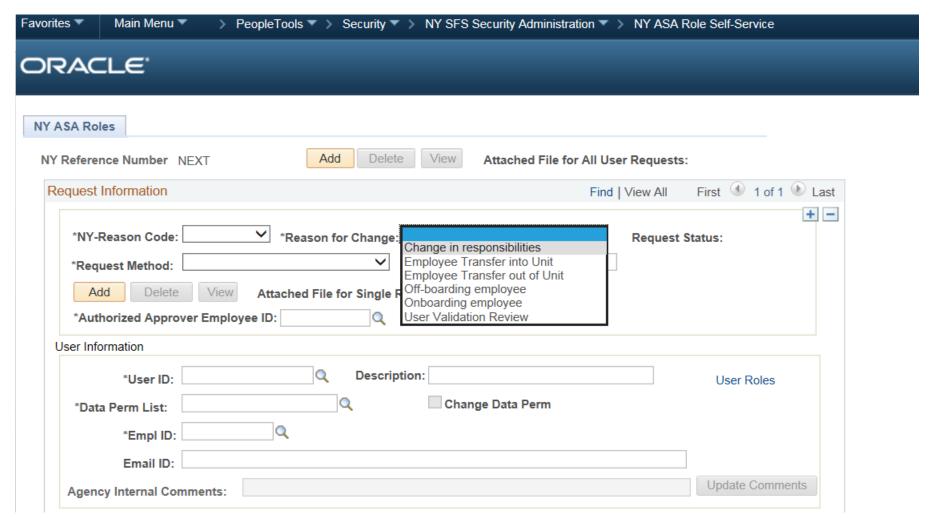- Note: Only one type of attachment can be provided for each ASA self-service request number

Enhancement - Attachments

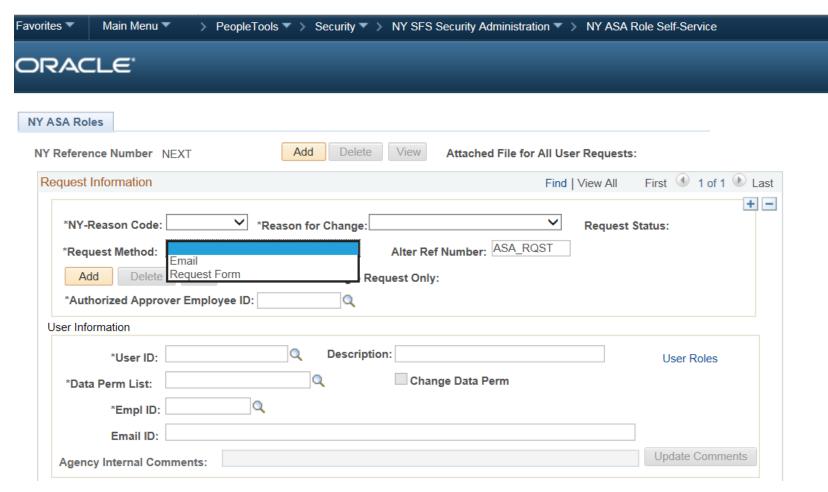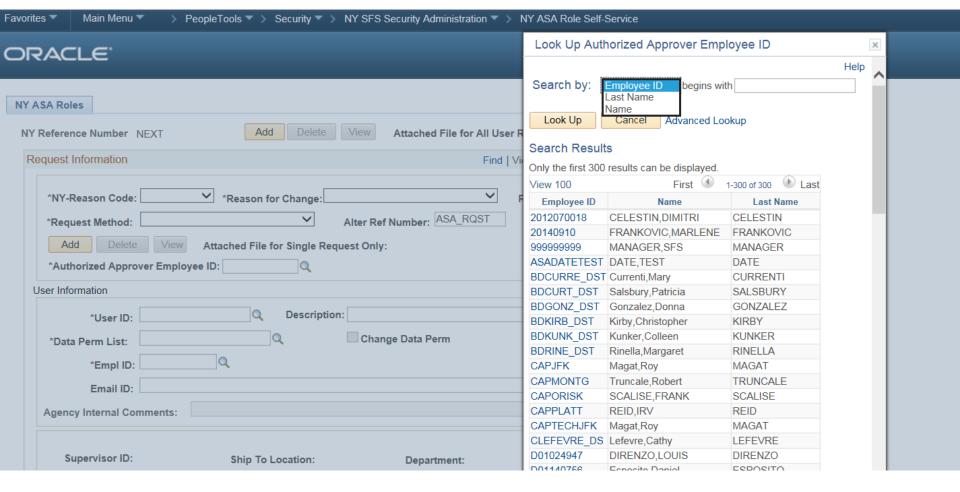- Attached File for All User Requests
  - When the attachment is provided at this level, the attachment **MUST** contain the justification and approval for **ALL** users that are part of the ASA self-service request number. The person who approved the change should be listed in the Authorized Approver Employee Id field.

- Note: Only one type of attachment can be provided for each ASA self-service request number

Enhancement – Attachments

Statewide Financial System (Internal Use Only).
Contents subject to change.

Enhancement - Attachments

- Attached File for Single Request Only
  - When the ASA self-service request has multiple user changes, but there are separate files containing justification and approval, attach the appropriate file for the user request **on each page** of the ASA self-service request.

    Example, if you have two user accounts that need to be changed, and there are two separate files that need to be attached, attach the appropriate file to each user request under the Single Request only file attachment.

- Note: Only one type of attachment can be provided for each ASA self-service request number

Enhancement – Attachments

Statewide Financial System (Internal Use Only).
Contents subject to change.

Enhancement – Reason for Change

Enhancement – Request Method

Statewide Financial System (Internal Use Only).
Contents subject to change.

Enhancement – Authorized Approver

Attachments – ASA Mass Upload

Statewide Financial System (Internal Use Only).
Contents subject to change.

Attachments - Annual User/Role Validation

- Annual User/Role Validation will now require attachments that supports the details that the annual review has been completed and of the provisioning changes being requested and the needed approvals.
  - Spreadsheets noting changes or any other form of documentation showing the review was completed
  - Any changes needed should be made in a timely manner within SFS
  - The ASA Mass Upload functionality will be linked to User/Role Validation page to make this easier for everyone

- A new query will be available that lists the reviews completed, who signed off and the related dates

- Benefits: This ensures that the documentation needed for Audit is available if your agency is selected.

Travel Proxy Tool Update

Mary Alber

Travel Proxy Tool Updates

- We have two change requests being developed to improve the maintenance and reporting of Travel proxy Assignments.

    - The travel proxy mass update tool is being updated to include the ability to export and import the proxy authorization level – View, Edit, Full.

    - Travel Proxy Assignment Queries and the export are being updated to include visibility into the authorization level and also will include a new filter that will allow agencies to elect to include or exclude BSC travel proxies from the query/export results.

    Watch for the announcement for Administrators and Compliance Reviewers to test these new features in Agency Business Process test in the next couple of weeks.
    As always we appreciate your feedback to ensure new tools meet your needs.

Security Lessons Learned

Mary Alber

Internal Controls

- Regularly SFS sends out Retired, Terminated, Deceased reminders when we observe an agency employee is tied to an active SFS account when their Payserv employee status is marked as Retired, Terminated, Deceased.

- Lessons:
  - The SFS notice is meant to be a control reminder for agency review.
    - Some employees on the report may have left the same day the report is distributed.
    - The goal of this notice is to test the results against your Agency business process.
      - If your agency control established in your business process catches these and the only employees observed on the report sent to your agency are within 24-48 hours of your control point, then it demonstrates your controls are working.
      - If your agency control established in your business process is NOT catching these and the employees observed on the report sent to your agency are aged by days or weeks then it demonstrates your controls are not working and your agency internal business process for separation needs to be reviewed.
      - If an employee is being reported on this report in error, contact SFS.

Employees with a status of Retired, Terminated or Deceased should be actioned by the agency as soon as they receive notice. It is the responsibility of each agency to establish a process for clear communication between Human Resources, Supervisors and their Agency Security Administrators.

Social Engineering

- Recently an agency ASA was asked to reset an SFS users password via an email that mimicked a formal request. Later the agency ASA found out that the reset request was really phishing and the new password was sent via email to an unknown party.

- Actions/Lessons:
  - *Compromised Accounts should be immediately locked.* ASA should immediately lock the SFS user account themselves, then contact SFS Security to report the issue and have the users password reset in the system
  - *Emails can be compromised.* This email was not sent from the employee and it was discovered that the employees email credentials were compromised. The appropriate IT Desktop team should determine that the email and their devices are no longer compromised.
  - *Compromised Emails Impact SFS processes.* Before using ASA Self Service password reset again for the compromised user the ASA is responsible to follow up and ensure:
    - The compromised email situation had been addressed.
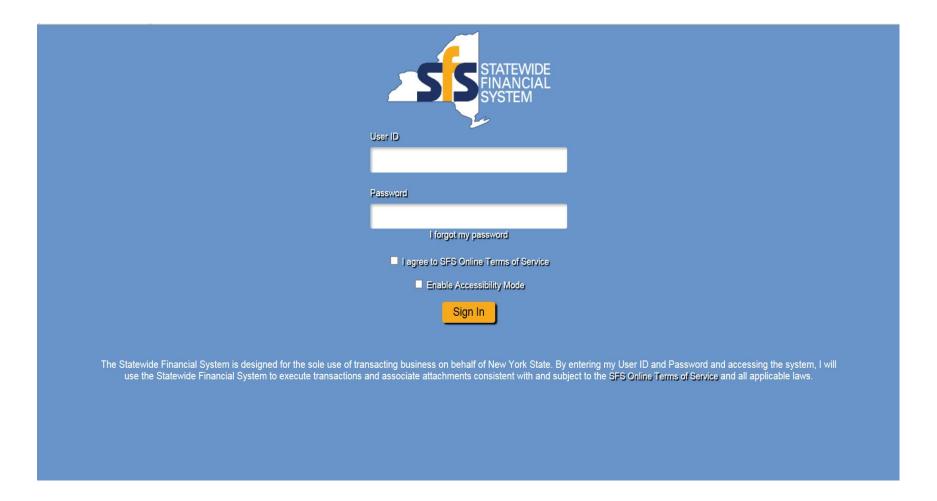
Social Engineering

- Recently an Agency ASA asked an agency user for their SFS Forgotten Password question and answer to attempt resolution of a password reset issue.

- Lessons:
  - An end user's forgotten password hint question and answer should be treated as confidential.
  - ASAs can use the password reset feature within ASA Self Service to reset a users password.
  - ASAs may contact SFS in order to resolve password reset issues.
  - **Credential sharing is not allowed per the SFS Online Terms of Service**

Online Terms of Service reminder

Online Terms of Service reminder

- The Statewide Financial System is designed for the sole use of transacting business on behalf of New York State. By entering my User ID and Password and accessing the system, I will use the Statewide Financial System to execute transactions and associate attachments consistent with and subject to the SFS Online Terms of Service and all applicable laws.

Online Terms of Service reminder

SFS ONLINE TERMS OF SERVICE

FOR STATE EMPLOYEES ON BEHALF OF STATE AGENCIES AND PUBLIC AUTHORITY EMPLOYEES ON BEHALF OF PUBLIC AUTHORITIES

When accessing and using the Statewide Financial System (SFS), I certify that:

1. I have been authorized by the head of a state agency or public authority to execute these transactions, which may include, but are not limited to: Billings, Travel Authorizations, Expense Reports, Budget Journals, Budget Transfers, General Ledger Journal Entries, Purchase Requisitions, and Purchase Orders;

2. I am familiar with the Ethics in Government Act (Public Officers Law sections 73 and 74; the "Act") and my conduct in the use of the SFS Program Online Services is in accord with the Act.

3. I am familiar with and agree to comply with the Comptroller's policies on Confidential, Personal and Private Information, as described in the Office of the State Comptroller's *Guide to Financial Operations, Section III.8*.

4. Accounts Payable Vouchers certified/approved by me and submitted to the Office of the State Comptroller are for claims that are just, true and correct and, therefore, appropriate to pay; and the goods or services rendered or furnished are for use in the performance of the official functions and duties of this agency.

5. Employee Expense Voucher certified/approved by me and submitted to the Office of the State Comptroller are for claims that are just, true and correct and, therefore, appropriate to pay; and the employee's supervisor certified that the expenses have been examined and to the best of the supervisor's knowledge and belief, the amounts claimed therein were necessary for the performance of the employee's authorized official duties.

6. Imaged records accurately, legibly and completely reflect all the information in the original records except where redacted. For redacted images, the agency has retained the unaltered, original document.

FOR INDEPENDENT CONTRACTORS ON BEHALF OF STATE AGENCIES AND PUBLIC AUTHORITIES

When accessing and using the Statewide Financial System, I certify that:

1. I have been authorized by the head of a state agency or public authority to execute these transactions, which may include, but are not limited to: Billings, Travel Authorizations, Expense Reports, Budget Journals, Budget Transfers, General Ledger Journal Entries, Purchase Requisitions, and Purchase Orders;

2. I am familiar with the terms and conditions of the contract under which I have been assigned to work for a state agency and my conduct in the use of the SFS Program Online Services are in accordance with such contract and consistent with the requirements imposed upon state employees and public authority employees under the Act. Any false transactions may subject me to civil and/or criminal liability.

3. I am familiar with and agree to comply with the Comptroller's policies on Confidential, Personal and Private Information, as described in the Office of the State Comptroller's *Guide to Financial Operations, Section III.8*.

4. Accounts Payable Vouchers certified/approved by me and submitted to the Office of the State Comptroller are for claims that are just, true and correct and, therefore, appropriate to pay; and the goods or services rendered or furnished are for use in the performance of the official functions and duties of this agency.

5. Employee Expense Voucher certified/approved by me and submitted to the Office of the State Comptroller are for claims that are just, true and correct and, therefore, appropriate to pay; and the employee's supervisor certified that the expenses have been examined and to the best of the supervisor's knowledge and belief, the amounts claimed therein were necessary for the performance of the employee's authorized official duties.

FOR STATE EMPLOYEES ON BEHALF OF THEIR OWN TRAVEL-RELATED TRANSACTIONS AND NON-TRAVEL EXPENSE REIMBURSEMENTS

When accessing and using the SFS, I certify that:

1. The transactions executed and the attachments associated with the transactions are just, true, and correct, that no part thereof has been paid (except as stated therein), and that the balance therein stated is actually due and owing;

2. I understand that in processing employee-generated travel and expense transactions, SFS and Office of the State Comptroller (OSC) will use information from the OSC payroll system, including banking information relating to the direct deposit of my salary. If I use direct deposit for the processing of my payroll payments, I authorize SFS and OSC to use my banking information for the direct deposit of travel and expense payments.

3. I understand that I may opt out of receiving my travel and expense payments electronically by contacting my payroll office.

4. Imaged records accurately, legibly and completely reflect all the information in the original records except where personal or sensitive business information has been redacted. In cases where sensitive business information is redacted, I have submitted the original document containing the sensitive business information to my agency for retention.

Statewide Financial System (Internal Use Only).
Contents subject to change.

Any questions from our topics today?

Thank you for attending!

Contents subject to change.

Reference Section

Security Policy

Security Policy

- [Reference and Resources > Access to SFS (Security and Roles) > SFS Security Policy](#)

SFS Agency Security Maintenance Procedure

Security Maintenance Procedure on SFS*Secure*

- Reference and Resources > Access to SFS (Security and Roles) > SFS Agency Security Maintenance Procedure

STATEWIDE FINANCIAL SYSTEM

Maintenance Procedure Resource Considerations

- Effective communication among supervisors, Human Resources (HR) and agency SFS administrators
  - Supervisors provide the first line of insight on employee movement, extended leave, retirement, employee death, and termination
- As SFS Compliance Reviewers you should be the champion
  - Engage your management and SFS administrators in conversations for process improvement

STATEWIDE FINANCIAL SYSTEM

SFS Administration Observations

- User provisioning
  - Separated employees and non-employees who have access to SFS are not locked and removed timely.
    - Risk - the separated SFS users retain access to your agencies data.

- Separate process for contractors
  - Contractors are not in state payroll systems
    - How are you getting notified of contractor movement?

Contents subject to change.

SFS User Provisioning Request Form

- [SFS User Provisioning Request Form](#) or your internal SFS access form are the methods for timely notification of provisioning changes to the ASA
  - Documentation should be retained in case your agency is required to produce it upon audit request.

- *Authorization and justification of changes being made to users in SFS must be retained for traceability to the ASA Self-Service Request reference number*

Internal Control Compliance Review

Internal Control Compliance Review

- [SFS Internal Control Compliance Review](#) document

- SFS recommends each agency Internal Controls Officer (ICO)/Compliance Reviewer consider the checklist when completing an internal controls compliance review of access to SFS.

- This checklist supports the published Office of the State Comptroller (OSC) Guide to Financial Operations (GFO) '*Certification of Internal Controls over the Payment Process.*'

Compliance Review

- Internal Control Officers/Compliance Reviewers are asked to ensure:
    - An inventory is created of any lack of controls or weaknesses in established Agency provisioning processes.
    - A corrective action plan or compensating controls are established for any weaknesses identified in security processes.
    - Monitor SFS access by utilizing tools provided via the Internal Control Officer Information Center in SFS*Secure* under Reference and Resources.

STATEWIDE FINANCIAL SYSTEM

How to assess compliance?

- Ensure your agency has established policies over user access and SFS role assignment.
- Engage your administrators and list out any obstacles you face in these internal processes as currently implemented.
- Review your list with management for solution support.
- Escalate any road blocks.

Offboarding in SFS

- When an SFS user leaves state service, the User Account should be locked immediately and removed timely.

  - Many agencies listed outstanding travel or credit card transactions as a reason they are not locking or removing SFS access timely.

  - Outstanding travel or credit card transactions are NOT a reason to leave SFS access open to a separated state employee or contractor.

  - RISK: Leaving SFS access in place for a user who left state service

Account Security

SFS Audit Process runs on the first of every month:

- Account Locking:
  - Lock agency user accounts that are more than 90 days old and have never been used
  - Lock agency user accounts that have not been used in 180 days or more

- Removal of accounts:
  - Accounts that are locked by the audit process and not reactivated within 180 days are removed from the SFS system.
  - User accounts that hold travel only roles will not be removed as part of this process.

Any questions from our Reference Section?
Contact the SFS Help Desk!

Thank you for attending!

Contents subject to change.

STATEWIDE
FINANCIAL
SYSTEM