DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

Statewide Policy

OREGON ACCOUNTING MANUAL

Subject:	Accounting and Financial Reporting	**Number:**	10.70.00
Division:	Chief Financial Office	**Effective date:**	June 14, 2017
Chapter:	Internal Control		
Part:	Security Access to Central Financial Systems		
Approved:	George Naughton, Chief Financial Officer	Signature on file	

PURPOSE: This policy outlines the process and assigns responsibilities for requesting security access to the state's central financial systems.

AUTHORITY: **ORS 291.015**
ORS 293.595
Statewide IT Policy 107-004-050
Statewide IT Policy 107-004-052

APPLICABILITY: This policy applies to all entities that access the statewide financial systems.

FORMS: Systems Security Access Request Forms

POLICY:

101. Agency management must develop control procedures that ensure the systems access granted to each user is appropriate and consistent with the user's job duties.

102. The Chief Financial Office, Statewide Accounting and Reporting Services (SARS), Systems Security team manages security access for the following central financial systems:

    a. SFMA (Statewide Financial Management Application). This mainframe application includes:

    - R*STARS (Relational Statewide Accounting and Reporting System)
    - ADPICS (Advanced Purchasing and Inventory Control System)

    b. OSPA (Oregon State Payroll Application) – a mainframe application.

    c. The Datamart – a system that houses tables of data downloaded from:

    - SFMA (R*STARS, ADPICS)
    - OSPA
    - PPDB (Position and Personnel Database)
    - PICS (Position Information Control System)

    Access to PPDB and PICS is addressed in paragraphs 120 and 121 of this policy.

103. The SARS financial systems security officers (SSO) validate agencies' requests for systems access, provide training to ASOs, conduct semi-annual security reviews, and participate in the Secretary of State's annual audit of the financial systems.

104. Systems access must be set at the minimum level needed for the user to perform assigned job duties.

105. *At a minimum*, each agency should designate two Agency Security Officers (ASO) for each financial system the agency uses – one to serve as the primary security officer and one to serve as the backup. Each ASO is expected to understand how the financial system(s) operates, be familiar with the security access screens (including profiles), and have the ability to verify user access

106. To designate a new ASO, or change/revoke existing authority, the agency CFO (or designate) completes and submits the ***Agency Security Officer Notification Form*** to the Systems Security team within one business day of the change event.

107. ASOs must:

- Review, approve, and process all valid requests submitted by agency management to add, modify, or revoke a user's access to the central financial systems.
- Actively participate in the statewide semi-annual security reviews.
- Attend statewide security training provided every two years by the Systems Security team.
- ASOs may **not** submit security requests for their own access.

108. ASOs must document all requests received from agency management to add, modify, or revoke a user's access. Maintain all security documentation for audit purposes a minimum of three years.

109. Upon the complete fulfillment of a personnel action -- related to the departure or position change of an employee -- within PPDB, the employee's access to the systems covered by this OAM are automatically revoked in an overnight process. However, if the agency determines that an employee's access needs to be modified or revoked, and it will not result in the **immediate and complete** fulfillment of a personnel action as described above, the agency must notify the ASO within two weeks of that determination. In turn, the ASO will have one business day, starting from their notification by the agency, to notify the Systems Security team via email at security.systems@oregon.gov to modify or revoke the employee's access, as applicable.

Each agency is responsible for developing procedures to notify their ASO timely of a need to revoke a user's access that is not related to the immediate and complete fulfillment of a personnel action as described above.

110. All systems security request forms must be submitted electronically to the Systems Security team by the ASO authorizing the add/modify/revoke.

111. **Users must not allow other individuals to use their passwords or RACF ID.** The Systems Security team will immediately revoke access to all central financial systems for each person involved in a security violation. Agencies are responsible for taking corrective actions, including disciplinary measures, and must contact the Systems Security team via email at security.systems@oregon.gov for reinstatement requirements and instructions.

PROCEDURES

Requests for Standard Access to SFMA and OSPA

112. The ASO reviews each written request for user access received from management to ensure the request is consistent with the user's position and assigned job duties. The written request for access is the beginning of the security audit trail.

113. If the ASO has a security concern, the ASO notifies the user's manager and suspends processing until the concern is resolved.

114. Once the concern is resolved, the ASO continues processing the request. The ASO completes the ***SFMA and OSPA – Mainframe Access*** request form located on the SARS Systems Security website:

http://www.oregon.gov/das/Financial/Acctng/Pages/Syst-security.aspx

When completing the form, the ASO must provide the following information for each user:

- Full name of the individual as shown in the PPDB
- The user's RACF ID
- Agency number
- The user's active email address and phone number
- The desired action: Add, Modify, or Revoke
- The system(s) requested – by completing the applicable section(s) of the form
- A brief explanation of job duties that require the specific access requested for each system. (Example 'to process payments received from vendors')

115. The ASO signs the form electronically, enters the current date, and uses the 'submit by email' button provided to submit the form to Systems Security.

116. The Systems Security team will deny access if any required information is missing or not active. Requests are processed when received; early submissions and incomplete forms will be returned to the ASO for correction and resubmission.

Requests for Special View Access to SFMA (R*STARS only)

117. Access requests for statewide user classes (UC) require additional security documentation. Scan and email completed request forms to the Systems Security team at security.systems@oregon.gov. The original hardcopy is to be maintained by the agency.

- Statewide user classes 01-10, 36, 38, 39, 46, 50, 59, 65, 70, and 79-81 are restricted to SFMA analysts, SARS analysts and Secretary of State Auditors. The requesting agency's Division Administrator must authorize the access request. These user classes may not be active if the employee is in telework status. Email the Systems Security team to obtain the ***Statewide User Class Access*** request form. This form is not available on the SARS website.
- UC 78 allows the user to view all agencies' transaction records, including data classified as restricted and critical. Senior fiscal officers and ASOs must ensure that UC 78 requests are based on valid needs and that the level of access is consistent with each user's job duties. Completion of the ***User Class 78 - All Agency View Access*** form is required.

Requests for Datamart Access

118. **Datamart Standard Access**: The ASO completes and submits the required ***Datamart Standard View Access - SFMA and OSPA Tables*** request form for access. Upon activation, SFMA Datamart information is accessible even if OSPA Datamart is the only table requested.

119. **Datamart Special View Access:** Security level 3 (restricted) and level 4 (critical) data are not included in the standard Datamart view. The ASO must work with the agency's senior fiscal officer to ensure that each request to view sensitive data is consistent with the user's position and assigned job duties.

Datamart Standard View access must be activated before a special view is requested. Completion of the ***Datamart Special View Access*** form is required.

120. **PPDB Standard View Access:** The Department of Administrative Services (DAS), Chief Human Resources Office, HR Systems Section manages access to the PPDB system and the related tables in the Datamart.

Contact PPDB Security at Group.PPDB@oregon.gov for assistance.

121. **ORBITS/PICS Standard View access:** The DAS, Chief Financial Office, Statewide Audit and Budget Reporting Section (SABRS) manages access to ORBITS and PICS and the related tables in the Datamart.

Contact the SABRS unit at ORBITS.Help@oregon.gov for assistance.

OSPA Only – Terminal Access and Web Reports

122. ASOs must specifically identify the computer terminals used for OSPA mainframe access and the level of access allowed.

123. ASOs submit email requests to add or delete OSPA terminals not linked to a specific employee's activation to security.systems@oregon.gov. The notification must include:

- Four-digit terminal identification number
- Agency number
- Type of access: 'U' for update, 'D' for display
- Report printer identification (if applicable)
- Description of the terminal location

124. The DAS, Oregon State Payroll Services (OSPS) unit manages access to the OSPA web reports.

Contact the OSPS Help Desk at OSPS.Help@oregon.gov for assistance.

Requests to Change or Reset Mainframe Passwords

125. When a RACF ID revokes for password issues, only the user can request reactivation. The RACF ID user emails DAS Enterprise Technology Services directly at DAS.RacfUserAdm@oregon.gov.

The request must include the following information:

- Full name of the individual as shown in the PPDB
- The user’s RACF ID
- Indication that the request applies to the mainframe system
- Request a “resume” when the password is known but was entered incorrectly
- Request a “reset” when the password was forgotten or has expired

126. DAS Enterprise Technology Services verifies ownership of the RACF ID and sends a temporary password directly to the user.

127. Web-to-Host mainframe users manage their passwords by accessing the Customer Information Control System (CICS) website:

https://columbia.das.state.or.us:3025/cics/wtst/daswpscp/ .

Requests to Change or Reset Datamart Passwords

128. Datamart users may change passwords or request a password reset. Follow the instructions located on the Datamart User Maintenance Site:

https://dasapp.state.or.us/DatamartApp .

Security Reviews and Training

129. Semi-annual statewide security reviews are conducted electronically beginning in February and August of each year. The SSO first verifies ASO assignments with each agency’s CFO or designate.

The assigned ASO receives system-specific reports for review and analysis along with verification forms. The ASO verifies the correctness of the access granted to the agency’s users and checks with the users’ managers to determine if the level of access is still appropriate.

The ASO completes the verification form for each report by signing, dating, and recording any security changes to existing access. The ASO must return all verification forms to the SSO by the specified due date. Agencies should retain copies of the access reports for reference purposes.