

OREGON ACCOUNTING MANUAL

SUBJECT: Accounting and Financial Reporting

Number: 10.70.00

DIVISION: State Controller's Division

Effective date: August 1, 2009

Chapter: Internal Control

Part: Security Access to Central Financial Systems

APPROVED: John Radford, State Controller

Signature on file at SCD

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 Policies 107-004-050 and 107-004-052

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

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. Systems access must be set at the minimum level needed for the user to perform assigned job duties.
103. Agency Security Officers (ASO) must document all requests received from agency management to add, change or revoke a user's access, and maintain the documentation for audit purposes.
104. Agencies must notify the State Controller's Division, Systems Security unit to modify or revoke a user's access within 24 hours of a position change.
105. ASOs must participate in the semi-annual statewide security reviews and attend statewide security training provided every two years by the Systems Security unit.
106. **Users must not allow other individuals to use their passwords or RACF ID.** The Systems Security unit 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 unit for reinstatement requirements and instructions.

PROCEDURES

Central Security Officers

107. The State Controller's Division, Statewide Accounting and Reporting Services (SARS), Systems Security unit manages security access for the following central financial systems:
- a. SFMA (Statewide Financial Management Application). This application includes:
 - R*STARS (Relational Statewide Accounting and Reporting System)
 - ADPICS (Advanced Purchasing and Inventory Control System)
 - b. OSPA (Oregon State Payroll Application)
 - c. The Datamart – a system that houses tables of data downloaded from:
 - SFMA
 - OSPA
 - PPDB (Position and Personnel Database)
 - PICS (Position Information Control System)
- NOTE: R*STARS, ADPICS and OSPA are mainframe systems.*
108. The SARS financial systems security officers (SSO) validate agencies' requests for systems access, provide training to agency security officers, and conduct semi-annual security reviews.

Agency Security Officers

109. *At a minimum*, each agency should designate two ASOs 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.
110. To designate a new ASO, the ASO's supervisor completes and submits the **Agency Security Officer Notification Form** to the Systems Security unit. The form appears in the Security Access Request section at:
http://www.oregon.gov/DAS/SCD/SARS/systems_security.shtml
111. To change or revoke an existing ASO's system authority, agencies must submit requests to the Systems Security unit using the **Agency Security Officer Notification Form** within 24 hours of the change event. The new request will replace all previous designations for that particular ASO.
112. ASOs must:
- Review, approve, and process all requests submitted by agency management to add, change or revoke a user's access to the central financial systems.
 - Actively participate in the statewide semi-annual security reviews.
 - Attend statewide security training.

Requests for Standard Access to SFMA and OSPA

113. The ASO reviews each management request for user access to ensure the request is consistent with the user's position and assigned job duties.
114. If the ASO has a security concern, the ASO notifies the user's manager and suspends processing until the concern is resolved.
115. Once the concern is resolved, the ASO continues processing the request. The ASO completes the ***Financial Systems Security SFMA and OSPA Request Form*** located in the Security Access Request section at:
http://www.oregon.gov/DAS/SCD/SARS/systems_security.shtml.
116. When completing the *SFMA and OSPA Request 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 e-mail 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. (Ex. 'to process payments received from vendors')
117. If the ASO indicates the intent is to mirror another user's profile, the ASO still must specify the exact access for the new user by completing the section of the form applicable to each system requested.
118. The Systems Security unit will deny access if any required information is missing and return incomplete forms to the ASO.
119. The ASO signs the form electronically, enters the current date, and e-mails the form to:
security.systems@das.state.or.us

NOTE: The Financial Systems Security Request Form must be e-mailed by the same ASO who electronically signs and dates the form.

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

120. Access requests for statewide user classes (UC) require additional security documentation. Either scan or mail completed request forms to the Systems Security unit.
 - 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. Contact the Systems Security unit to obtain the ***Central Staff Statewide User Class Access Request Form***.

- 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. The **UC78 All Agency View Access Request Form** is located in the Security Access Request section at:

http://www.oregon.gov/DAS/SCD/SARS/systems_security.shtml

Requests for Datamart Access

121. **SFMA and OSPA Standard View Access:** The ASO completes and submits the **Datamart Standard View Access SFMA and OSPA Tables Request Form** found in the Security Access Request section at:

http://www.oregon.gov/DAS/SCD/SARS/systems_security.shtml

122. **SFMA 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. For special view access, please e-mail the Systems Security unit at security.systems@das.state.or.us, attention Datamart Business Analyst.

123. **PPDB Standard View Access:** The Department of Administrative Services (DAS), Human Resource Services Division, HR Systems Section manages access to the PPDB system and the related tables in the Datamart. The **PPDB Security Access Request Form** appears at the following link under HR Systems Forms:

<http://www.oregon.gov/DAS/HR/forms.shtml>

Contact PPDB Security at group.ppdb@das.state.or.us for assistance.

124. **ORBITS/PICS Standard View access:** The DAS, Budget and Management, Statewide Audit and Budget Reporting Section (SABRS) manages access to ORBITS and PICS and the related tables in the Datamart. The **ORBITS/PICS Security Form** appears at the following link under SABRS Operations:

<http://www.oregon.gov/DAS/BAM/forms.shtml>

Contact orbits.help@das.state.or.us for assistance.

Terminal Access – OSPA Only

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

126. Agencies submit e-mail requests to add or delete OSPA terminals not linked to a specific employee's activation to security.systems@das.state.or.us. 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

Requests to Change or Reset Mainframe Passwords

127. When DAS revokes a RACF ID for password issues, only the owner can request reactivation. The RACF ID owner e-mails DAS Operations directly at DAS.RacfUserAdm@das.state.or.us.

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
128. DAS Operations verifies ownership of the RACF ID and sends a temporary password directly to the user.
129. Zephyr Web-to-Host mainframe users manage their passwords by accessing the CICS Web site at <https://columbia.das.state.or.us:3025/cics/wtst/daswpscp/>.

Requests to Change or Reset Datamart Passwords

130. Datamart users may change passwords or request a password reset by following the instructions found at the Enterprise Systems Unix Web page:
<https://datamart.sdc.state.or.us/cgi-bin/login>

Security Reviews and Training

131. Statewide security reviews occur semi-annually in May and November. The SSO sends system-specific reports to the primary ASO for review and analysis. 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.
132. The ASO must sign and date each page of each report and record any security changes on the face of the report. The ASO must return all reports to the SSO by the specified due date. Agencies should retain copies of the reports for reference purposes.
133. The State Controller's Division, Systems Security unit provides statewide security training every two years. Each ASO is required to attend.