

OREGON ACCOUNTING MANUAL

Subject: Accounting and Financial Reporting	Number: 10.70.00.PR
Division: State Controller's Division	Effective date: March 8, 2007
Chapter: Internal Control	
Part: Security Access to Financial Systems	
Section:	
Approved: John Radford, State Controller	Original signature on file in SCD

Authority [ORS. 291.015](#)
[ORS 293.595](#)

Security Requests

- .101 All security requests, except for requests to reset or resume a password (see paragraph .114 and 115), need to be sent via e-mail to security.systems@state.or.us or faxed to the Department of Administrative Services (DAS), State Controller's Division (SCD), Statewide Accounting and Reporting Services (SARS), System Security Officer (SSO). Requests by e-mail should include all information in the text of the message, not in attachments. All requests must be from the designated agency security officer(s) (see OAM Policy, **10.70.00.PO**, .103 *Agency Security Officer(s)*) to ensure requests are properly authorized. Requests must include the information specified in this procedure.
- .102 Agency security officers must consider the job duties of each employee and authorize security access that supports the agency's internal controls. Access should be granted at the minimum level needed for an employee to perform his/her job duties.
- .103 The SSO is responsible for verifying the authenticity of each request. If there is not enough information or the information provided is incorrect, the SSO will request additional or corrected information before the request is processed.
- .104 When a security access change is needed for an agency security officer, the request must come from either his/her supervisor or another security officer in the agency.

Notification of Agency Security Officer(s)

- .105 When an agency appoints an agency security officer(s), the agency needs to provide to the SSO the name, mailing address, phone number, fax number, and e-mail address of the appointed individual(s). In addition, the notification needs to indicate the effective date of the assignment and the specific financial systems or databases for which the individual(s) will serve as the agency security officer(s). If an agency has more than one security officer, specify if the newly assigned security officer is to receive the semi-annual security review reports. When making an assignment change, the agency must send a notification to the SSO indicating that the individual is no longer the agency security officer within 24 hours of the change in duty assignment.

Security Reviews

- .106 The SSO will provide security reports to the agency security officer once every six months for agency review and analysis.

- .107 The agency security officer will review the security reports, mark any changes to security access, sign and date the report, and initial each page (even if there are no changes). Upon completion of the review, the agency security officer will return all of the reports to the SSO.

Security Training

- .108 Training is provided periodically by the SSO to all agency security officers. Agency security officers are responsible to attend training as needed.

New User Access

- .109 New user access requests need to state that the request is a new activation and include the following information:
- R*STARS: Indicate the request is for access to R*STARS. Include the full name of the individual as shown in the state's personnel system, agency number, **RACFID**, the individual's e-mail address, user class and any other applicable access information. A listing of user classes can be found in the R*STARS Security Manual, available from the SSO.
 - ADPICS: Indicate the request is for access to ADPICS. Include the full name of the individual as shown in the state's personnel system, agency number, RACFID, Standard User Classification and its associated User ID, the individual's e-mail address and phone number, User Department, User Level, and any other applicable access information. User Classification information can be found in the ADPICS Security Manual, available from the SSO.
 - Accounting Datamart: Indicate the request is for access to the Accounting Datamart. Include the full name of the individual as shown in the state's personnel system, agency number, agency name, User ID, agency billing or department billing number, as well as the user's phone number and e-mail address.
 - OSPA: Indicate the request is for access to OSPA. Include the full name of the individual as shown in the state's personnel system, agency number, the individual's e-mail address, and RACFID. Include appropriate access by payroll function as described in the OSPA security training, or through contacting the SSO.
 - Payroll Datamart: Indicate the request is for access to the Payroll Datamart. Include the full name of the individual as shown in the state's personnel system, agency number, agency name, User ID, agency billing or department billing number, as well as the user's phone number and e-mail address.

New Terminal Access – OSPA Only

- .110 Requests for new OSPA Terminal access must include the four digit terminal identification, agency number, type of access (such as D for display), printer terminal (if applicable), and a description of the terminal location.

Modifying User Access

- .111 Requests for modified access need to state that the request is a modification and include the following information:
- Full name of the individual as shown in the state's personnel system;
 - Agency number;
 - The system in which access is to be modified;
 - RACFID or User ID;
 - The modification requested; and
 - A brief explanation or reason for the request.

Inactivation

- .112 Requests for the inactivation of a user need to include the following: RACFID, agency number, and related system(s), and a brief explanation or reason for the inactivation. The SSO will send an e-mail to the DAS Enterprise Security Office (security.ggdc@state.or.us) to request that the RACF group connection be removed. For inactivation resulting from a change in job duties, notification must be made within 24 hours of the change in duties.
- .113 Other inactivation of users, usually as a result of state personnel action notices, will be e-mailed to the SSO from the DAS Enterprise Security Office.

Password Resume or Reset

- .114 For DAS mainframe: Requests to resume or reset a user password do not involve the SSO or the agency security officer. These requests are sent directly from user ID owners to the DAS Enterprise Security Office. If a user's RACF ID has been revoked, and the user remembers his or her password, the user will send an e-mail to the DAS Enterprise Security Office (security.ggdc@das.state.or.us) to request that his or her password be resumed. If a user's RACF ID has been revoked, but the user does not remember his or her password, the user will send an e-mail to the DAS Enterprise Security Office (security.ggdc@das.state.or.us) to request that his or her password be reset. The request must include the user's RACF ID and indicate the request is for the DAS mainframe. The Enterprise Security Office will verify that the request is from the owner of the RACF ID.
- .115 For SCD Accounting Datamart or Payroll Datamart: Requests to reset a user password for access to the Datamart do not involve the SSO or the agency security officer. These requests are sent directly from user ID owners to the DAS Enterprise Security Office. If a user does not remember his or her Datamart password, the user will send an e-mail to the DAS Enterprise Security Office (security.ggdc@das.state.or.us) to request that his or her password be reset. The request must include the user's RACF ID and indicate the request is for the Accounting or Payroll Datamart. The Enterprise Security Office will verify that the request is from the owner of the RACF ID. Datamart passwords cannot be "resumed" because these passwords are not "revoked" as mainframe passwords are revoked. Datamart passwords are reset, not resumed.

Mainframe Password Change

- .116 A password change is made by the individual mainframe user, not requested through the SSO or the DAS Enterprise Security Office. Mainframe users can utilize a CICS web site to change their password, which is located at: <https://columbia.das.state.or.us:3025/cics/wtst/daswpscp/>. This is especially helpful for agencies that have elected to use Zephyr Web-to-Host software to access the mainframe instead of software such as TN3270, Attachmate's Extra, or Passport. Zephyr Web-to-Host access users may want to use a calendar entry to remind them to change their password before it expires.

Datamart Password Change

- .117 A password change is made by the individual Datamart user, not requested through the SSO or the DAS Enterprise Security Office. If a user's Datamart password has expired, the user needs to change his or her Datamart password. This is done through the internet at <https://dasdm1.iservices.state.or.us/cgi-bin/login>. From this web page, the user will log in using his or her User ID in lower case and his or her expired password. Then, the user will select the option to change the password. After confirming the new password, a message will be displayed indicating the password change was successful.