Financial Systems Security Procedure

OVERVIEW

The University manages its financial operations through PeopleSoft Financials which enables the processing of financial transactions and the recording and extraction of financial data. This procedure covers the process for access and approval, profile and role changes and security controls.

SCOPE AND APPLICATION

This procedure applies to all staff, students, titleholders and any person engaged by The University of Adelaide (e.g. contractors, agency staff) involved in the processing of financial transactions, including the use of financial data. All data and information stored on the Finance System is considered confidential and must be handled in accordance with the IT Acceptable and Security Policy.

DEFINITIONS

Finance System: PeopleSoft Financial Management system.
SOD Matrix: the Segregation of Duties Matrix is a formal document controlled by ITDS, which details the role name and description, and identifies where conflicts exist between roles.
Role Group Owner: Role owners are the approval authority appropriate to roles within their area of responsibility.
Continuous Delivery, University Operations: responsible for the technical support / maintenance of the Finance System within Information Technology & Digital Services (ITDS).
Jira: a project management tool used to manage and track technical issues.
Cherwell: a service request management tool.

PROCEDURES

1. Access to the Finance System

Upon commencement at the University, the HR system creates an employee profile that integrates into the Finance System creating a shell user account. The shell account enables the user to raise and submit e-Forms. Access to other roles in the Finance System are requested by submitting a Finance System Access Request Form. Access is only granted where a role is required for business purposes and in accordance with the SOD Matrix.

Responsibility: ***Requestor (see note for students & titleholders)***

a) Log into the Finance System and navigate to eForms > Finance System Access
b) Use the following guides for instructions on how to complete the form -
   - ePro Requestor
   - all other roles
c) If you have existing roles, the system will flag any role conflicts as per the SOD Matrix
d) Agree to the Access & Usage Declaration and submit for approval.

Note: Students, titleholders and visitors requesting the role of "ePro Requestor" also require the approval of their immediate Supervisor or Line Manager. This must be attached to the Finance System Access Request Form.

2. Approval of Finance System Access Requests

New user access and/or changes to current access, are approved by the Role Group Owner.

Role Group	Role Group Owner
General (includes ePro Requestor)	Relevant Faculty / Division Finance Manager
Purchasing	Manager, Procure to Pay
AR/Billing	Manager, Revenue Accounting
Accounts Payable	Manager, Procure to Pay
Accounting / Reporting	Manager, Research & Management Accounting
Projects	Manager, Research & Management Accounting
Grants / Contract Management	Manager, Research & Management Accounting
Administration / Miscellaneous	Manager, Financial Initiatives & Projects
System Roles	Manager, Financial Initiatives & Projects
Dynamic Roles	Manager, Financial Initiatives & Projects
Approver Roles	Manager, Financial Initiatives & Projects

Responsibility: ***Role Group Owner***

a) Assess the request based on justification and business need
b) If satisfied, approve request (email is generated to user; access is immediate)
c) Ensure appropriate training is provided (handover or on the job training must be provided with the exception of ePro Requestor which is available online).

3. Reporting access and approval

Users with reporting access are able to run financial reports in the Finance System and also through reporting tools such as ORBIT and Cognos BI. These tools are governed outside of Finance & Procurement Services, however access to financial data in these systems must be approved by the following positions:

Type	Level	Approver (only one is required)
Finance data	Faculty / school	Faculty Finance & Planning Manager
Finance data	Division / branch	Division Management Accountant Manager, Division Finance Manager, Research & Management Accounting Manager, Financial Initiatives & Projects
Finance data	All of University	Chief Financial Officer Director, Finance Strategy Director, Accounting Services
Contracts and Billing	All University contracts	Faculty Finance & Planning Manager Division Management Accountant Manager, Division Finance Manager, Research & Management Accounting Manager, Financial Initiatives & Projects Director, Research & Business Partnerships Director, Research Grants

4. Monthly user access review

Role Group Owners (with the exception of general roles which are considered low risk) receive a monthly auto generated Finance Security Audit Report to enable periodic review of roles and users assigned to them.

Responsibility: ***Role Group Owner***

a) Review report and confirm the assigned users still require access
b) To request removal of system access email finprosupport@adelaide.edu.au

Responsibility: ***Service Support Officer***

c) Upon receipt of request, remove user and/or role assigned to them
d) Close Cherwell.

5. Database Access

A request to access any finance database must be made and approved by the Manager, Finance Initiatives & Projects via a Jira request. Once the Jira is approved, it will be assigned to the Enterprise Systems Lead (ITDS) for action.

Database access will be granted according to database roles:

a) Application Administrator (read/write access to production and non-production),
b) Application Developer (read/write access to non-production),
c) Interface Developer (read-only access to production and non-production),
d) Functional Analyst (read-only access to production and non-production), or
e) External Contractor (restricted read-only access to non-production).

6. Quarterly database security review

A security review of staff who have access to the Finance System database is conducted on a quarterly basis. A report is sent through Jira from ITDS to the Finance & Initiatives Project Team for review.

Responsibility: ***Finance Initiatives & Projects Team***

a) Review quarterly report and confirm the assigned users still require access
b) To request removal of system access, add to Jira

Responsibility: ***Enterprise Systems***

c) Upon receipt of request, remove user and/or role assign to them
d) Close Jira.

7. HR position changes to user profiles

A number of automated processes are triggered in the Finance System as a result of position changes in PeopleSoft HR.

Process	Action
Account Lock	User accounts are locked based on contract termination or suspension. The user is notified by an automated email. Roles are retained for 30 days before automatically being removed by the system.
Change in position	Changes in position number (permanently or temporarily) will result in roles being removed. The user must apply for access required for new position and / or reapply for access when returning to a previous position. The user is notified by an automated email.
Financial Delegation	Positions holding a financial delegation (permanently or temporarily*) in the Finance User List (hosted in PeopleSoft HR) are dynamically assigned the approver role and corresponding limit in the Finance System.

*Financial Delegations temporarily transferred via the Temporary Delegation Transfer e-Form (in PeopleSoft HR) are date effective and the role is automatically removed after the end date. Delegations (approver roles) are reviewed as part of the monthly user security review.

8. Permanent changes to roles and/or permissions

Permanent changes to roles or permissions are requested by the business and approved by the Role Group Owner before proceeding through the Change Request process.

Responsibility: ***Finance, Initiatives & Projects Team (on behalf of Role Owner)***

a) Based on business need, submit a Change Request through Jira

Responsibility: ***Continuous Delivery, University Operations***

b) Complete an impact assessment for the requested role, or permission change
c) Provide findings and recommendations to the Finance, Initiatives & Projects Team

Responsibility: ***Finance, Initiatives & Projects Team***

d) Assess findings and if no conflicts or security risks are found, approve the change
e) If this change impacts the SOD Matrix initiate a review in collaboration with the Role Group Owner
f) If a permanent change to the SOD matrix is approved, raise a Jira to ITDS to make the change.

9. Impacts to SOD Matrix

The SOD Matrix is a formal document, any changes or potential impacts as a result of role or permission changes must go through a review and approval process as per 7. f.

Responsibilities

Finance, Initiatives & Projects Team are custodians of the SOD Matrix and responsible for initiating any reviews, Change Requests or raising Jiras on behalf of the business.

Role Owners are responsible for:

- Annual review of the SOD Matrix for appropriateness, noting any conflicts. The review is initiated by FI&P Team as at 30th June.
- Request and approval of changes to SOD Matrix for roles within their role group.

Business Systems Support are responsible for:

- Update of the SOD Matrix following approval by the Role Owner
- Update system configuration and provide query listing conflicts.

10. System administrator roles

A limited number of staff hold system admin roles, giving them elevated access to modules within the Finance System. The level of access is based on business requirements.

Standard system administrator access roles (below) can be requested via the Finance System Access Request e-Form.

System Administrator Role	
Finance, Initiatives & Projects Team, Business Systems Support	Elevated access to change permissions, apply role changes to other System Administrators, amend approval workflow for purchase orders / vouchers.
Service Support Officers	Limited access to amend user profiles e.g. change permissions, manual role assignment or unlocking user accounts (as a result of an approved Finance System Access Request Form).

Staff (e.g. Functional Analysts) requiring non-standard system administrator access must complete the Finance System Administrator Access Form and summit to the Finance Initiatives & Projects Team for action.

The following roles **Sys_Admin_Tech** / **PeopleSoft Administrator** / **PeopleTools** require additional approval by the Enterprise Systems Lead (ITDS).

Monthly security exception report

The monthly security exception report tracks manual user profile, user permission and role assignment changes undertaken outside of the Finance System Access Request Form. This report is reviewed by the Manager, Finance Initiatives & Projects who does not have system admin access.

Responsibility: ***Manager, Finance Initiatives & Projects Team***

a) Review report and activities undertaken
b) If the change is authorised and appropriate then no further action is required (note and file report on the shared drive)
c) If the change is unauthorised and / or a serious breach is detected, escalate to the ITDS Information Security Team for a detailed investigation
   An investigable incident includes, but is not limited to;
   - manually resetting a user's password
   - high risk, unauthorised permission changes (such as granting approval access)
   - high risk, unauthorised role changes (such as granting a delegation role, approval role or modifying own access)

   The severity of a breach and the need for investigation is determined by the FI&P Team in consideration of all the facts and circumstances of the incident.
d) Should the outcome of the investigation determine inappropriate activities have taken place, proceed in accordance with the IT Acceptable User and Security Policy.

11. Third party systems & controls

A number of third party systems are managed within Finance & Procurement Services. A register of these systems, the process owner and access security controls in place, is maintained by the Finance, Initiatives & Projects Team.