Financial Systems Security Procedures

OVERVIEW

The University manages its financial operations through PeopleSoft Financials (the "Finance System") which enables the processing of financial transactions and the recording and extraction of financial data. These procedures, which form part of the Financial Management Policy and Procedures sets out the principles and processes to manage access to, and the use of, financial data within the Finance System and other financial systems.

SCOPE AND APPLICATION

These procedures apply 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
- IT specialists and technical support.

PRINCIPLES

- All data and information stored on the Finance System is considered confidential and must be handled in accordance with the IT Acceptable Use and Security Policy
- Users must take all reasonable steps to protect their account from unauthorised use and never share passwords or login credentials with others, especially if they hold an approval authority
- Requests for specific roles within the system must be requested via the Finance System Access Request eForm and approved by the Role Group Owner
- Access is only granted where a role is required for the person to perform their duties, and in accordance with the Segregation of Duties (SOD) Matrix.

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 enabling the user to raise and submit eForms. Access to

specific roles in the Finance System are requested by submitting a Finance System Access Request eForm (with the exception of the Purchasing Approver role).

Responsibility: ***Requestor****

a) Access the Finance System and click on eForms > Finance System Access
b) Use the following guides for instructions on how to complete the eForm -
   - 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.

* Students, casual staff, titleholders, and visitors requesting the role of "ePro Requestor" also require the approval of their immediate Supervisor or Line Manager and this must be attached to the eForm.

Procurement Approval Roles
To enable online approval of financial transactions, positions formally approved by the Vice-Chancellor and President to hold a financial expenditure authority are given approval roles.

a) Upon receipt of an approved financial delegation request to finprosupport@adelaide.edu.au, the Service Support Officer will add the position (number) to the relevant Finance User List in the HR System
b) An overnight feed dynamically applies the approval role with the applicable value limit, to the user profile in the Finance System
c) In the event the position becomes vacant or there is a change in staff member, the system will automatically remove or apply the roles to the new incumbent.

Payables System (Kofax)
Current staff and students are granted access to the Payables System to facilitate the submission of online Reimbursement / Other Payment requests and approvals. Administrator and AP Specialist Roles must be requested and approved by the Manager, Procure to Pay.

Kofax also hosts the Delegations of Authority (DoA) matrix, a control document that records expenditure workflow approvals by cost centre. Amendments to the DoA matrix must be submitted to finprosupport@adelaide.edu.au.

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
ePro Requestor	Relevant Finance Manager
Enquiry Only, Purchasing and Accounts Payable (specialised roles)	Manager, Procure to Pay
Inventory	Technical Support Operations Manager (SET)
Query Viewer, Accounting / Reporting, Projects, Grants / Contract Management, AR/Billing	Manager, Management Accounting & Reporting
Administration / Miscellaneous, System, Dynamic and Approver Roles	Director, Finance Strategy & Governance

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 as self-service or face to face with the Service Support Officers upon request.

3. Reporting access and approval

Users with reporting access are able to run financial reports in the Finance System and also through Cognos. This application is governed outside of Finance, however access to financial data must be approved by the following positions:

Type	Level	Approver (only one is required)
Finance data	Faculty / Division	Manager, Management Accounting & Reporting Team Leader, Management Accounting
Finance data	All of University	Manager, Management Accounting & Reporting Director, Finance Strategy& Governance Director, Finance & Accounting Services
Contracts and Billing	All Research Contracts	Manager, Management Accounting & Reporting Team Leader, Management Accounting

4. Monthly user access review

Role Group Owners 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) File evidence of review under Finance shared (S) drive > Finance System Access Audit
c) To request removal of system access email finprosupport@adelaide.edu.au

Responsibility: ***Service Support Officer***

d) Upon receipt of request, remove user and/or role assigned to them
e) File confirmation under Finance shared (S) drive > Finance System Access Audit for audit purposes.

5. Database access

A request to access any finance database is initiated by the ITDS Technical Lead (PeopleSoft) via ServiceNow and approved by Finance. Once approved, it is assigned to the Enterprise Systems Lead (ITDS) for action.

Direct write-access (update/insert/delete) to the production databases is not permitted. Database access is highly restricted, and a limited number of system administrators have read/write access due to their role as database administrators. Access to critical data within the database is also audited. Audit logs (and other security logs) are ingested by monitoring software and alerts generated if any unauthorised behaviour is noted.

6. Quarterly database security review

To ensure duties are segregated, user access audits and approvals are conducted by Director, Finance Strategy & Governance with any access changes executed by ITDS. A security review of staff who have access to the Finance System database is conducted on a quarterly basis and any changes/removal of system access submitted and actioned via ServiceNow. In addition there is an external audit process to ensure compliance with these procedures.

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 the HR System.

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 roles required for new position and / or reapply for roles when returning to a previous position. The user is notified by an automated email.
Financial Delegation	Positions holding a financial delegation (permanently or temporarily*) listed on the Finance User List are dynamically assigned the purchasing approver role and corresponding limit in the Finance System.

*Financial Delegations temporarily transferred via the Temporary Delegation Transfer eForm (in the HR System) 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 through the Change Request process.

Responsibility: ***Role Group Owner***

a) Submit a Change Request through ServiceNow

Responsibility: ***ITDS (Core Platforms)***

b) Complete an impact assessment for the requested role, or permission change
c) Provide findings and recommendations back to the Role Group Owner

Responsibility: ***Role Group Owner***

d) Assess findings and if no conflicts or security risks are found, approve the change
e) If this change impacts the SOD Matrix, raise a ServiceNow request to ITDS to reflect the change in the matrix.

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 section 8.

Responsibilities

Finance are custodians of the SOD Matrix and responsible for initiating any reviews, Change Requests or raising a ServiceNow request on behalf of the business.

The Role Group Owners (as per section 2) are responsible for:

- Annual review of the SOD Matrix as of 30th June, reporting to ITDS any potential conflicting roles for investigation (by raising a ServiceNow request).
- Requests and approval of changes to SOD Matrix for roles within their role group.

ITDS (Core Platforms) 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 eForm

System Administrator Role	
UOA_MONITOR_APPROVALS	Elevated access to amend approval workflow for purchase orders / vouchers.
UOA_SYSTEM_ACCESS	Limited access to amend user profiles e.g. change permissions, manual role assignment or unlocking user accounts

Non-standard system administrator access (i.e. for the UOA_Systems_Administrator role and other development related roles) are managed by ITDS via a ServiceNow request.

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 eForm. This report is reviewed by the Director, Finance Strategy & Governance who does not have system administrator access.

Responsibility: ***Director, Finance Strategy & Governance***

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 will be determined 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 Use and Security Policy.

11. Third party systems & controls

A number of third party systems e.g. Kofax, are managed within Finance. A register of these systems and the access security controls in place, is managed and maintained by the process owners within Finance.

DEFINITIONS

Finance System: PeopleSoft Financials and Supply Chain Management.

HR System: PeopleSoft Human Capital Management.

Finance User List: Lists of positions (by dollar limit) with financial expenditure delegation hosted within the HR System, changes to these lists are dynamically updated in the Finance System.

SOD Matrix: the Segregation of Duties Matrix is a formal document controlled by Finance (and held by Information Technology & Digital Services (ITDS) for audit purposes), which details the role name and description, and identifies incompatible roles for internal control purposes.

Role Group Owner: the approval authority appropriate to roles within their area of responsibility.

ITDS (Core Platforms): responsible for the technical support / maintenance of the Finance System within Information Technology & Digital Services (ITDS).

ServiceNow: a cloud-based IT Service Management platform.