Critical Finance Systems User Governance Procedure

Section 1 - Purpose

(1) This Procedure establishes the controls governing user access management for Critical Finance Systems across the University and its Controlled Entities ('the Group').

Background

(2) The University Computer and Network Security Procedure requires the University to establish controls for access to University information and systems. Section 4 of Computer and Network Security Procedure requires secure account management processes to be documented. This Procedure establishes requirements for allocation and review of user access rights to Critical Finance Systems across the Group.

Scope

(3) This Procedure applies to all staff who either manage user access rights or have been assigned user access rights to any Critical Finance System across the Group.

Section 2 - Policy

(4) Nil.

Section 3 - Procedure

User Governance Structure, Responsibilities and Required Actions for all Finance Critical Systems

(5) Critical Finance IT Systems are either (a) under IT Governance, or (b) not under IT Governance.

(6) For systems under IT Governance, the IT Support Leader and their team are accountable for key user access governance tasks.

(7) For systems not under IT Governance, the Business Owner is accountable for key user access governance tasks.

(8) This Procedure covers five key stages of the user life-cycle, each of which are detailed further below:

a. Initial Creation of New Users, and Ad Hoc Requests to Vary a User Profile Over;
b. Fortnightly Review of Access to Identify and Remove Terminated Staff;
c. Biannual Review of Ongoing User Access;
d. Monthly Review of Admin Users; and
e. Reporting of adherence to overall Procedure.

Initial Creation of New Users, and Ad Hoc Requests to Vary a User Profile Over Time

(9) Authority to approve a new user and vary a profile of an existing user:

a. Access rights to all Critical Finance Systems require the approval of the user's line manager / supervisor.
b. Access rights to Critical Finance System Restricted Functions require the additional approval of the Critical Finance Systems Business Owner, as detailed in Appendix A - Group Critical Finance Systems.
c. Admin User rights to Critical Finance System Restricted Functions require the approval of the Critical Finance Systems IT Support Leader, as detailed in Appendix A - Group Critical Finance Systems.

(10) Documentation required for user creation:

a. Evidence of approval of new users for each Critical Finance System will be retained by the Critical Finance Systems IT Support Team (or Critical Finance Systems Business Owner where the system is not under IT Governance), as detailed in Appendix A - Group Critical Finance Systems.

Fortnightly Review of Access to Identify and Remove Terminated Staff

(11) The process and frequency of access review:

a. Unless off-boarding of application users occurs automatically via the Active Directory, user access lists for all Critical Finance Systems will be reviewed at least fortnightly by the relevant Critical Finance Systems IT Support Team (or Critical Finance Systems Business Owner where the system is not under IT Governance) to identify and remove users who have ceased employment with the University Group.

(12) The identification of accounts of staff members that have separated from the employment of the University:

a. Separated Staff Reports will be circulated by the HR system IT Support Team to the relevant Critical Finance Systems IT Support Team (and Critical Finance Systems Business Owners where the system is not under IT Governance) each fortnight for those Critical Finance Systems without automatic off-boarding.

(13) The review and removal of accounts of staff members that have separated from the employment of the University:

a. User access lists for all Critical Finance Systems will be reviewed fortnightly against Separated Staff Reports by the relevant Critical Finance Systems IT Support Team (or Critical Finance Systems Business Owner where the system is not under IT Governance) to identify user profiles of employees who have ceased employment within the University Group.
b. Terminated staff will be removed from each Critical Finance System by the relevant Critical Finance Systems IT Support Team (or Critical Finance Systems Business Owner where the system is not under IT Governance) within two (2) business days of receipt of the Separated Staff Report.

(14) Reporting and documentation required to be generated and retained:

a. Evidence of completion of each review, as well as details of users deleted, will be retained by the relevant Critical Finance Systems IT Support Team (or Critical Finance Systems Business Owner where the system is not under IT Governance).

Biannual Review of Ongoing User Access

(15) Existing account access and permissions review requirement:

a. User access lists for all Critical Finance Systems will be reviewed bi-annually to ensure appropriate ongoing access.
b. The Chief Information Security Officer will liaise with each Critical Finance Systems IT Support Leader (or Critical Finance Systems Business Owner where the system is not under IT Governance) to compile a timetable for bi-annual reviews for all Finance Critical Systems.

(16) Review process for existing account access and permissions:

a. Critical Finance Systems IT Support Teams (or Critical Finance Systems Business Owner where the system is not under IT Governance) will:
    i. review the assigned privileges of all user accounts within the relevant Critical Finance System with the user's line manager;
    ii. reduce privileges where staff have changed roles and no longer need the same level of privileged within the relevant Critical Finance System; and
    iii. disable user access where staff have changed roles and no longer need to access the relevant Critical Finance System.
b. Users who have not accessed a particular Critical Finance System for 180 calendar days will have their user access rights removed from that Critical Finance System.

(17) Reporting and documentation required to be generated and retained:

a. Evidence of completion of each review, as well as details of users deleted or modified, will be retained by the Critical Finance Systems IT Support Team (or Critical Finance Systems Business Owner where the system is not under IT Governance).
b. A quarterly report will be prepared confirming the bi-annual reviews completed in that reporting period, and the schedule for upcoming biannual reviews, across all Critical Finance Systems, including a summary of user access changes made, and any issues arising. This report will be reviewed by the Chief Information Security Officer and the Deputy Group Chief Financial Officer.

Monthly Review of Admin Users

(18) Review of privileged activity requirement:

a. User activity logs for all Admin Users of all Critical Finance Systems will be reviewed at least monthly. Any activity identified as unusual will be investigated.

(19) Review process for privileged activity:

a. The review will be conducted each month by the relevant Critical Finance System IT Support Leader, or Critical Finance Systems Business Owner where the system is not under IT Governance.

(20) Reporting and documentation required to be generated and retained:

a. Confirmation of completion of each review will be documented by the relevant Critical Finance Systems IT Support Leader (or Critical Finance Systems Business Owner where the system is not under IT Governance) at least each month.
b. Reviews that have led to the identification of unusual activity, concerns or remediation action, will be reported to the Chief Information Security Officer for investigation. Where an investigation leads to a suspected breach of University policy, the Chief Information Security Officer will report investigation findings to the Chief Information and Digital Officer and the Deputy Group Chief Financial Officer.

Reporting of adherence to overall Procedure

(21) Reporting and documentation required to be generated and retained:

a. The Chief Information Security Officer, the Deputy Group Chief Financial Officer and IT System Leads will meet annually to review adherence or exceptions to this Procedure. Evidence of that meeting will be retained on file.

Summary of accountabilities

(22) For systems under formal IT Governance (as noted in Appendix A) the IT Systems Lead is accountable for the following tasks:

a. Initial Creation of New Users, and Ad Hoc Requests to Vary a User Profile Over Time is facilitated and controlled via One-help.
b. Fortnightly Review of Access to Identify and Remove Terminated Staff where automated offboarding via the Active Directory is not in place.
c. Ensuring biannual review of ongoing user access is scheduled, tracked and facilitated via One-help.
d. Ensuring monthly review of admin users is scheduled and tracked via One-help and referring any unusual activity to the Chief Information Security Officer for further investigation.

(23) For systems not under formal IT Governance (as noted in Appendix A) the Business Owner is accountable for the following tasks:

a. Retaining evidence of approval of new users and Ad Hoc Requests to Vary a User Profile.
b. Conducting and retaining evidence of a fortnightly review of access to identify and remove terminated staff based on a separated staff reports circulated by the HR system IT Support Team.
c. Conducting and retaining evidence of a biannual review of ongoing user access to identify and remove staff who no longer require access, based on input from their line manager.
d. Conducting and retaining evidence of a monthly review of admin user activity logs and referring any unusual activity to the Chief Information Security Officer for further investigation.

Section 4 - Guidelines

(24) Nil.

Section 5 - Definitions

(25) The following definitions apply for the purpose of this Procedure:

a. Admin User means a privileged level of user access rights that usually includes the ability to perform specialised, technical, or ‘back-end’ functions in a Critical Finance System and may allow the user to override system prevention or segregation controls that exist for standard users. (This type of role may have a different system-specific title but will be in substance as defined here).
b. Automatic Off-boarding means an automated process built into an application where a notification of an end of employment from HR systems results in the removal of all access to the application. This may be via removal at the system level, or via removal at the active directory level.
c. Critical Finance Systems means core Finance systems in use across the University Group, including all general ledger, banking, billing, supplier invoice approval, payroll, and other operational systems that materially impact data in the General Ledger, as listed in Appendix A - Group Critical Finance Systems. The Deputy Group Chief

Financial Officer, in consultation with the Chief Information Security Officer, may add and remove systems from this list based on their assessment of business risk.

d. Critical Finance Systems IT Support Leader means a specific role with oversight of a Critical Finance Systems IT Support Team. This role has accountability for execution of all tasks allocated to their Critical Finance Systems IT Support Team in this Procedure. Specific role titles in the Group who perform this leadership activity, as well as the specific systems over which they have accountability, are detailed in Appendix A - Group Critical Finance Systems.
e. Critical Finance Systems IT Support Team means the IT team accountable for the provision of administrative and back-end IT support functions for a Critical Finance System, as detailed in Appendix A - Group Critical Finance Systems. Led by a Critical Finance Systems IT Support Leader.
f. Critical Finance Systems Business Owner means the 'front-end' operational custodian of a Critical Finance System, as detailed in Appendix A - Group Critical Finance Systems.
g. Critical Finance Systems Restricted Functions means functions or access areas within a Critical Finance System that are deemed by the Critical Finance Systems Business Owner to be of higher risk due to ability to edit important information. Separated Staff Report means a report obtained from the Payroll System detailing fixed term and permanent staff who have ceased to be employed by an entity within the University Group in the period specified in the report.
h. Unusual activity means activity occurring at unusual times of day, or activity that is not core to the Admin User's normal assigned tasks.
i. User access rights means the permissions an individual user or a computer application holds to read, write, modify, delete or otherwise access a computer file; change configurations or settings, or add or remove applications. An organisation's network or information technology administrator can define permissions for files, servers, folders or specific applications on the computer.

Status and Details

Status	Current
Effective Date	6th May 2022
Review Date	6th May 2025
Approval Authority	Vice-President, Professional Services
Approval Date	12th April 2022
Expiry Date	Not Applicable
Responsible Executive	Eric Knight Deputy Vice-Chancellor (People and Operations)
Responsible Officer	Andrew Wan Chief Information Security Officer
Enquiries Contact	Andrew Wan Chief Information Security Officer