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

Responsibilities and Required Actions

User Governance Responsibilities and Required Actions for all Finance Critical Systems

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

(5) 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 Restricted Functions Access Approver, as detailed in Appendix B - Critical Finance Systems Restricted Functions Access Approver.

(6) Documentation:

a. Evidence of approval of new users for Critical Finance Systems will be recorded by the Critical Finance Systems IT Support Team or the Critical Finance Systems Business Owner.

Fortnightly Review of Access to Identify and Remove Terminated Staff

(7) Review requirement:

a. Unless off-boarding of application users occurs automatically, 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 to identify and remove users who have ceased employment with the University Group.

(8) Identification:

a. Separated Staff Reports will be circulated by the HR system IT Support Team to the relevant Critical Finance Systems IT Support Teams or Critical Finance Systems Business Owners each fortnight for those Critical Finance Systems without automatic off-boarding.

(9) Review process:

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 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 within two (2) business days of receipt of the Separated Staff Report.

(10) Reporting and Documentation:

a. Confirmation of completion of each review, as well as details of users deleted, will be documented by the relevant Critical Finance Systems IT Support Team or Critical Finance Systems Business Owner.

Biannual Review of Ongoing User Access

(11) Review requirement:

a. User access lists for all Critical Finance Systems will be reviewed bi-annually to ensure appropriate ongoing access.

(12) Review process:

a. Critical Finance Systems IT Support Teams or the Critical Finance Systems Business Owner will:
    i. review the assigned privileges of all user accounts within the relevant Critical Finance System;
    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.

(13) Reporting and documentation:

a. Confirmation of completion of each review, as well as details of users deleted or modified, will be documented by the Critical Finance Systems IT Support Team or the relevant Critical Finance Systems Business Owner.

Monthly Review of Admin Users

(14) Review 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.

(15) Review process:

a. The review will be conducted each month by the relevant or Critical Finance System Business Owner (as listed in Appendix A – Group Critical Finance Systems).

(16) Reporting and documentation:

a. Confirmation of completion of each review, as well as details of any unusual activity, any concerns, and any remediation action required will be documented by the relevant Critical Finance Systems IT Support Leader or the Critical Finance Systems Business Owner 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.

Section 4 - Guidelines

(17) Nil.

Section 5 - Definitions

(18) Commonly defined terms are located in the University Glossary. 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.
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. [Materiality is defined as a system that generates or processes financial transactions with a cumulative impact of 0.5% of full year expenses for the relevant entity. For the University this is $5m per annum.]
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. They will perform reviews of Admin User activity logs as per Clauses 14 to 16.
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. Refer to Appendix B - Critical Finance Systems Restricted Functions Access Approver for details of Restricted Functions by Critical Finance System.

h. Critical Finance Systems Restricted Functions Access Approver means system custodian with responsibility for granting access to and monitoring ongoing access over Restricted Functions of a Critical Finance System. Refer to Appendix B - Critical Finance Systems Restricted Functions Access Approver for custodians by Critical Finance System and by Restricted Function.

i. 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.

j. Unusual activity means activity occurring at unusual times of day, or activity that is not core to the Admin User's normal assigned tasks.

k. 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	Historic
Effective Date	22nd February 2021
Review Date	22nd February 2023
Approval Authority	Vice-President, People and Services
Approval Date	11th September 2020
Expiry Date	5th May 2022
Responsible Executive	Eric Knight Deputy Vice-Chancellor (People and Operations)
Responsible Officer	Andrew Karvinen Chief Information Security Officer
Enquiries Contact	Andrew Karvinen Chief Information Security Officer