Information Security - User Access Management Procedure

Section 1 - Summary

(1) The purpose of the User Access Management Procedure is to support the Information Security Policy and provide a framework for the management of user access to Victoria University (VU) information systems, networks, and equipment.

(2) The User Access Management Procedure defines the procedures in place for granting, modifying, removing, and reviewing user access privileges to VU systems and applications in order to protect the privacy, security, and confidentiality of University information assets and systems.

Section 2 - Scope

(3) This Procedure applies to all users of VU information systems and services, including employees, students, contractors and third-party providers both on and offshore.

(4) This Procedure applies to persons responsible for the management of user accounts or access to University information assets and systems, including departmental accounts (Business Owner or Custodian) and centrally managed accounts (ITS).

(5) This Procedure applies to information systems and services owned and/or operated by VU or outsourced or hosted through external/third-party service providers.

(6) This Procedure does not include physical access to VU computing equipment and IT controlled areas. Please see the Information Security Policy.

Section 3 - Policy/Regulation

(7) Information Security Policy

Section 4 - Procedures

Part A - Summary of Roles and Responsibilities

Roles	Responsibility
Business Owner or Custodian	- Will comply with User Access Management procedures for their information system. - Are responsible for ensuring third-party service providers of services and systems comply with VU User Access Management procedure. - Are responsible for retaining a record of user access requests, approvals, terminations, and disabling for information systems for auditing purposes. - Are responsible for documenting and retaining a record of user access reviews for auditing purposes.

Roles	Responsibility
ITS	- Will maintain a record of Business Owner or custodian, Managers, and delegates who can approve user access privileges to information systems and services.
People and Culture	- Will notify ITS of employees who are leaving the University due to redundancy (targeted or voluntarily) or have been dismissed/employment terminated.
Employees, students, contractors, and third-party service providers	- Are responsible for the protection of their individual account and password, must not share their password with anyone, or allow others to use their account in accordance with the IT Appropriate Use Policy. - Will immediately change their password and/or notify ITS Service Desk if they believe their account details have been disclosed or used by an unauthorised user. - Will log out of their account or use screen locking on a device when not present to prevent unauthorised access to their account and underlying University systems.
System Administrator, Database Administrator, Application Administrator	- Are responsible for the protection of administrator account details and must not share administrator account details with unauthorised users. - Will immediately change the account password and notify the Business Owner or Custodian of the relevant information system if they believe an administrator account has been improperly disclosed or used by an unauthorised user. - Will only use administrator accounts for performing administration related activities.

Part B - Authentication Services

(8) All VU equipment, networks, and information systems must identify and authenticate VU users using approved authentication methods.

(9) Approval via the Chief Digital Officer and Executive Director Campus Services must be obtained to use alternate authentication models.

(10) The identification and authorisation of user access to VU systems and applications must meet the access controls defined in the Information Security Policy and IT Security Standards.

(11) Students, employees, contractors, and third-party service providers accessing VU information systems will be uniquely identified.

(12) The use of anonymous or 'guest' user accounts to access VU information systems is prohibited.

(13) User accounts that have been inactive for a period of 30 days or more will require the user's password to be reset through self-service or the ITS Service Desk before access is granted to VU information systems and services.

Part C - Granting User Access Privileges

(14) Access to information that is not publicly available will be provided on a need to know basis and disclosed to individuals who have a legitimate business need for the information.

(15) Access to VU information systems and services will be granted based on the individual's job duties, project responsibilities, and other business activities.

(16) Requests for access to VU information systems and services lodged via the ITS Service Desk will be referred to the relevant Business Owner or Custodian or ITS team for action.

(17) Business Owner or Custodian is responsible for approving new requests for user access to information systems.

(18) Departmental managers must provide approval for new user access requests to file permissions within their department's information assets.

(19) Third-party service providers must comply with the User Access Management Procedure and ensure that user access to information systems and data is granted only for individuals that have been authorised by the relevant Business Owner or Custodian.

Part D - Modifying User Access Privileges

(20) Managers will ensure that when an employee changes role within the organisation, their access will be amended so that it reflects the requirement of their new role. Any user access privileges to VU information systems or services that are no longer required for the employee’s new role will be removed.

(21) Requests for changes to an individual's user access privileges for a VU information system or service lodged via the ITS Service Desk will be referred to the relevant Business Owner or Custodian or ITS team for action.

(22) Business Owner or Custodian is responsible for approving changes to user access for information systems.

(23) Departmental managers must provide approval for user access changes to file permissions within their department's information assets.

Part E - Removal of User Access Privileges

Employee Account Termination

(24) Employees that are leaving the University, for any reason will have their user access privileges disabled at the end of their employment unless an exemption is granted by the Chief Digital Officer and Executive Director Campus Services.

(25) System Administrators will remove application specific access for the user account.

Student Account Termination

(26) Students will continue to have access to their student email accounts after the end of enrolment at VU.

(27) Student access to other VU systems and services will be terminated at the end of the enrolment.

Suspension of User Access Privileges

(28) VU reserves the right to revoke the system privileges of any user at any time.

(29) Suspension of user access for student accounts requires approval from the Chief Digital Officer and Executive Director Campus Services and must be conducted in accordance with Student Misconduct Regulations 2019.

Part F - Reviewing User Access

(30) Business Owner or Custodian will conduct a user access review every 12 months at a minimum to ensure that current access privileges to information systems and services are relevant and appropriate for each individual user.

(31) Departmental managers are responsible for conducting annual user access reviews of file permissions within their department's information assets.

(32) User access reviews should be documented and retained for auditing purposes.

(33) Changes to user access for an information system identified as part of user access reviews should be performed by following the relevant procedures for modifying or terminating user access privileges.

(34) Business Owner or Custodian can create their own specific procedures to review user access accounts for their VU information system.

Part G - Administrator Account Management

(35) Administrator account details will only be disclosed to individuals who require this type of access based on their role.

(36) Where possible, default administrator accounts for information systems should be disabled. If the account cannot be disabled, the account should be renamed and the default password should be changed immediately.

(37) Requests for access to an administrator account must be authorised by the Business Owner or Custodian or a relevant ITS manager.

(38) Administrator accounts must only be used for performing administration-related activities. All non-administrator activities must be performed under the employee's user account.

(39) Passwords for administrator accounts must be changed at least quarterly or immediately if a user with knowledge of the password leaves the University or no longer requires access to the account based on their role.

(40) Administrator account access is to be reviewed at least quarterly.

Part H - Contractor Account Management

(41) Contractors will be assigned a user account for temporary access to information systems that will be set to expire according to the expiry date obtained from the contract agreement.

(42) Contractor user accounts will be terminated within the specified timeframes under Employee Account Termination (clause 24).

(43) System Administrators are responsible for removing application specific access for the contractor account.

(44) Any contractor user account that has been inactive for a period of 30 days or more will be disabled.

Section 5 - HESF/ASQA/ESOS Alignment

(45) HESF: 2.1 Facilities and Infrastructure, 7.3 Information Management.

(46) Outcome Standards for NVR Registered Training Organisations 2025: Standard 1.8 Facilities, Equipment and Resources; 4.3 Risk Management.

Section 6 - Definitions

(47) Business Owner or Custodian: Individual with operational authority for a specified information asset and responsibility for establishing controls for its protection.

(48) Administrator Account: A user account with access to one or more systems that provide the user with system-level privileges including access to user acceptance testing, development, and production environments.

Status and Details

Status	Current
Effective Date	10th June 2021
Review Date	15th March 2026
Approval Authority	Executive Director, IT Services
Approval Date	9th June 2021
Expiry Date	Not Applicable
Accountable Officer	Lisa Line Deputy Vice-Chancellor Enterprise and Digital Lisa.Line@vu.edu.au
Responsible Officer	Stuart Hildyard Chief Digital Officer and Executive Director Campus Services +61 3 9919 5576
Enquiries Contact	James Munro Associate Director, VU Cyber 0437216020