IT Security - User Access Management Procedure

Section 1 - Purpose / Objectives

(1) The purpose of the User Access Management Procedure is to support the IT Security Policy and provide a framework for the management of user access to Victoria University business systems, networks and equipment through an ITS approved authentication service.

(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 / Application

(3) This procedure applies to all users of Victoria University information systems and services including staff, students and contractors.

(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 Owners) and centrally managed accounts (ITS).

(5) This procedure does not include physical user access to VU computing equipment and IT controlled areas. Please see the IT Security Policy and Security Access to Controlled IT Areas Procedure .

Section 3 - Definitions

(6) Nil

Section 4 - Policy Statement

(7) Nil

Section 5 - Procedures

Part A - Roles/Responsibilities

Roles	Responsibility
Business Owners	- Business Owners will comply with User Access Management procedures for their business system. - Business Owners are responsible for ensuring external providers of services and systems comply with VU User Access Management procedures. - Business Owners are responsible for retaining a record of user access requests for business systems for auditing purposes.
Information Technology Services	- ITS will maintain a record of Business Owners, Managers and delegates who can approve user access privileges to information systems and services.
People and Culture	- People and Culture will notify ITS of staff members who are leaving the University due to a redundancy (targeted or voluntarily) or have been dismissed/employment terminated.

Part B - Procedures

Approved Authentication Services

(8) In accordance with the IT Security Policy , all VU equipment, networks and business systems must identify and authenticate VU users by an Information Technology Services (ITS) approved authentication service.

(9) Approval via the Director of IT Operations must be obtained to use alternate authentication models.

(10) ITS approved authentication services include Active Directory and WebSSO.

(11) The use of anonymous or 'guest' user ID's and passwords to access VU information systems and services is prohibited. Exceptions apply to sites and systems where all users are intended to be anonymous.

(12) The identification and authorisation of user access to VU systems and applications must meet the User ID and password controls defined in the Information Security (Best Operational Practice) Procedure .

(13) User accounts that have been inactive for a period of 6 months 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 systems and services.

Granting User Access Privileges

(14) In accordance with the IT Security Policy , 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) Staff member 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 staff access to VU business systems and services lodged via the ITS Service Desk will be referred to the relevant business owner or ITS team for action.

(17) Business Owners are responsible for approving new requests for user access to business systems.

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

(19) External service providers will ensure that user access to information systems and data is granted only for individuals that have been authorised by the relevant Business Owner.

Modifying User Access Privileges

(20) Managers will ensure that when a staff member 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 business systems or services that are no longer required for the staff member'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 ITS team for action.

(22) Business owners are responsible for approving changes to user access for business systems.

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

Removal of User Access Privileges

Staff Account Termination

(24) Staff members that are leaving the University due to a redundancy (targeted or voluntary) or have been dismissed/employment terminated will have their user access privileges revoked within 1 business day of receiving notification from People and Culture.

(25) Other staff accounts to be terminated will continue to have user access privileges to staff email and AD accounts for 3 months after end of contract unless otherwise advised by the staff member's manager to allow access to payslips via HR Zone after employment has ceased. Access to other VU systems and services including Finance systems will be terminated at end of contract.

(26) ITS will terminate staff user accounts within the specified timeframes and contact Business System Administrators to remove application specific access for the staff account.

Student Account Termination

(27) Students will continue to have access to their student accounts for a period of 12 months after end of enrolment at Victoria University.

Suspension of User Access Privileges

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

(29) Suspension of user access for student accounts require approval from the Director of IT Operations and must be conducted in accordance with Student Misconduct Regulations .

Administrator Account Management

(30) Administrator account user ID's and passwords that provide the user with system-level privileges including access to user acceptance testing, development and production environments will only be disclosed to individuals who require this type of access based on their role.

(31) Requests for access to an administrator account must be authorised by the Business Owner or the relevant ITS Team Manager.

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

(33) Passwords for administrator accounts must be changed at least every 12 months 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.

(34) Administrator account access is to be reviewed every 12 months.

(35) Business Owners must ensure elevated access to systems using administrator accounts will only be granted after the staff member has logged on using their employee ID and password in the first instance.

Reviewing User Access

(36) Business Owners 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.

(37) Departmental managers are responsible for conducting annual user access reviews of file permissions within their department's shared network drive.

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

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

(40) Business Owners can create their own specific procedures for the review of user access accounts for their VU business system.

Contractor User Account Management

(41) Contractors authorised to use VU information systems and services will have an account created in the University Identity Management System (IDM) and allocated a unique 7000 series identification code with separate controls applied to access the VU network, email or VU applications.

(42) Contractors will be provided with temporary authorisation for system access with an expiry date applied that is obtained from the contract agreement.

(43) By default all contractor IDM accounts will expire from 12 months of creation.

(44) In the event a contractor account is to be extended beyond the applied expiry date or the default expiry date, the authorising manager is responsible for extending the account to continue access to VU information systems and services.

(45) To de-provision a contractor user account, the authorising manager must request the cancellation of all IT services for the contractor by contacting the ITS Service Desk.

(46) ITS will terminate user access for contractor accounts and notify other Business System Administrators to remove application specific access for the de-provisioned account.

(47) ITS and Business Owners will conduct a review of contractor user accounts every 12 months.

(48) Any contractor user account that has been inactive for a period of 6 months or more will be disabled.

Section 6 - Guidelines

(49) Nil

Status and Details

Status	Historic
Effective Date	1st September 2015
Review Date	1st May 2018
Approval Authority	Vice-Chancellor
Approval Date	25th August 2015
Expiry Date	5th February 2017
Responsible Officer	Stuart Hildyard Chief Digital Officer and Executive Director Campus Services 9919 5576
Enquiries Contact	Jessica Carter Coordinator Quality Assurance +61 3 99196292