Information Security - User Authentication Procedure

Section 1 - Summary

(1) This Procedure establishes guidelines for user authentication within the university's information security practices. It aims to protect sensitive data and resources from unauthorized access, ensuring the confidentiality, integrity, and availability of information.

Section 2 - Scope

(2) This Procedure applies to:

a. Victoria University (VU) students and staff; controlled entities of VU, contractors and third-party service providers who have access to University Information Assets.
b. Other user accounts including unprivileged accounts, privileged accounts, break glass accounts, service accounts, system accounts, local accounts, generic accounts and other accounts that provide access to the university’s information assets, applications, devices and systems.

(3) This Procedure does not include the processes and practises for managing access to Information assets. See Information Security - User Access Management Procedure.

Section 3 - Policy/Regulation

(4) Information Security Policy

Section 4 - Procedures

Part A - Summary of Roles and Responsibilities

Roles	Responsibilities
Digital and Campus Services	Enforce authentication controls and password policies for VU information assets in line with this procedure. Adequately identify and verify the account owner as a pre-requisite to fulfilling a password reset request. Create user accounts or assign new account requests to the designated system administrator. Reset a user account password and inform the account owner if the account has been compromised or is at risk of being compromised in order to protect VU information assets from unauthorised access.

Roles	Responsibilities
Users	Authenticate using their user account (ID and password) credentials to access information assets including university systems, applications, and networks. Enable and use MFA on their user account in line with University guidelines. Ensure user account credentials are secure and not shared with others in line with this procedure. Report lost or stolen mobile devices used to access VU information assets to IT Customer Support Desk in order for appropriate account security actions to be taken. Inform IT Customer Support Desk immediately if they believe their account or password has been compromised.
Business Owners	Ensure their information system complies with this Procedure.

Part B - Procedures

Authentication Services

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

(6) A University approved password authentication system will be used as the preferred form of authentication for user accounts, privileged accounts, service accounts and system accounts. The use of alternate authentication models and methods must be approved by the Chief Digital Officer and Executive Director Campus Services.

(7) The authorisation of user access to VU information assets must meet the access controls defined in the Information Security Policy and Information Security - User Access Management Procedure.

User Authentication

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

(9) Users must authenticate using their credentials to access VU information assets including University systems, applications and networks.

(10) Authentication credentials (e.g. passphrase, keying materials or certificates) must be protected while in transit and at rest in line with University approved cryptography standards.

Multi-Factor Authentication (MFA)

(11) MFA should be enabled for all users of VU information assets.

(12) Users will register for MFA through VU's dedicated authentication portal and follow University guidelines for configuring and using MFA.

(13) Users unable to use/access any of their registered verification methods should contact IT Customer Support Desk for assistance.

(14) Requests for exemptions from enabling MFA on a user account must be supported by justification and approved in line with the exemption process in the Information Security Policy.

(15) VU reserves the right to reject a request to grant an MFA exemption based on feasibility and potential risks posed to the University.

User Account Creation

(16) User accounts for accessing VU information systems will be created by authorised VU staff or designated system administrators.

(17) Each user account will have a unique identifier, such as a username or email address, and a strong passphrase.

(18) User accounts (ID and password) will be assigned to an individual. The use of shared accounts are not permitted unless no alternative is available and approved by the Business Owner.

(19) On creation of a user account (ID and password), a temporary password will be provided to the account owner after adequately verifying the account owner's identity and transmitted through a secure method to prevent interception.

(20) 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.

(21) The creation of local privileged/administration accounts will be restricted and require approval from the Chief Digital Officer and Executive Director Campus Services.

User Account Lockout

(22) A user account lockout policy will be enforced to protect VU information assets against brute-force attacks.

(23) User account passwords can be manually reset by contacting the IT Customer Support Desk or the system administrator.

(24) User accounts will be regularly audited and reviewed for inactivity. User accounts that have been inactive for a defined period may be disabled.

Password Requirements

(25) A University approved password policy will be enforced on all user accounts and privileged accounts used to access VU information assets.

(26) User account passwords must not be shared with others or stored in an insecure manner that may result in unauthorised access to VU information assets.

(27) Strong passphrases will be used in line with the following standards:

a. User account passphrases are recommend to be a minimum of 14 characters in length.
b. Privileged account passphrases are recommend to be a minimum of 20 characters in length.
c. Passphrases must contain a mix of lowercase and uppercase characters, numbers and special characters.
d. Passphrases should not consist of the user account name (ID) or based on any identifiable factors such as the account owners name or date of birth.
e. Passphrases should not be made up of easy to guess dictionary words.

(28) If a user account or password is suspected to have been compromised, the IT Customer Support Desk should be notified immediately to reset the account password.

(29) All temporary passwords must be changed to a new strong password on first log in. Temporary passwords are recommended to be a random passphrase and a minimum of 14 characters in length.

(30) Temporary passwords should be set to expire after 3 days.

(31) Privileged account passwords will be managed to ensure recommended password strength and complexity are enforced and changed on rotation to ensure security of VU information assets.

(32) Default passwords configured in information assets are to be changed immediately to enhance security.

(33) Account owners will be adequately identified and verified prior to fulfilling a password reset or password change request.

(34) User account passwords that are changed/reset should comply with passphrase strength recommendations and should not be a previous password.

Section 5 - HESF/ASQA/ESOS Alignment

(35) HESF: 2.1 Facilities and Infrastructure; 3.3 Learning Resources and Support; 7.3 Information Management.

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

Section 6 - Definitions

(37) Authentication – The security practice of verifying the identify of a user, process or device prior to granting access to University information assets.

(38) Break Glass Account – A local account protected with robust security controls that are used in emergency situations when normal access to the resource is unavailable.

(39) Generic account – Account that is interactive that identifies and authenticates an individual, group or function to a system. By default, generic accounts do not maintain accountability unless specific controls are implemented.

(40) Information Asset – Any information that is of value to the organisation. This term also includes the underlying supporting infrastructure such as business processes, hardware, networks, storage, applications, removable media, third-party providers and storage amongst others.

(41) Local Accounts – An account that is created on a device, system, application, platform, etc that provides local, restricted access to that resource without using Victoria University's central authentication controls.

(42) Multi-factor authentication (MFA) – Multi-factor authentication (MFA) is an electronic authentication method in which a user is granted access after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is).

(43) Passphrase – a longer, stronger and more secure form of password that is typically made up of four or more random words and include upper case letters, numbers and special characters.

(44) Privileged user account – Account that is interactive (i.e., held by an individual) that identifies and authenticates an individual to a system. This user account has privileged access to one or more systems which includes the ability to perform significant configuration changes to an operating system/application.

(45) Service/System Account – Account that is systematic (i.e., utilised by a system/application) that identifies and authenticates a system/application to a system. This service/system account can be used for functions such as to authenticate systems to systems (e.g. SQL SA account, database connection accounts, etc.); to execute operating system services; to support application function calls (e.g. SQL Server, Linux cron jobs, etc.).

(46) Temporary Password – An initial or temporary one-time password generated on creation of a user account or resetting an existing account password.

(47) User account – Account that is interactive (i.e., held by an individual) that identifies and authenticates an individual to a system (albeit not having privileged access to any system) contains an Account ID and Password.

Status and Details

Status	Current
Effective Date	1st February 2024
Review Date	1st February 2027
Approval Authority	Vice-Chancellor
Approval Date	31st January 2024
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