FIJI NATIONAL UNIVERSITY

POLICY NUMBER: 4

ITS USER ACCOUNT AND PASSWORD POLICY

Prepared by	IT Services Division
Approving Authority:	FNU Council
Date Approved:	1 August 2025
Next Review:	1 August 2028
Version Number:	1

1.0 Purpose

The purpose of this User Accounts and Password Policy is to establish guidelines for the creation, management, and deactivation of user, service and generic IT accounts in the University’s IT systems. This includes establishing password requirements to ensure that only authorised individuals have access to systems and data, and that these accounts are maintained securely. This policy is not intended to supersede or replace other University policies but should be read in conjunction with them, especially the Acceptable Use of FNU ICT Resources Policy.

2.0 Scope

This policy applies to all staff, students and others who are authorized to have access to the University's systems, networks, and data.

3.0 Policy Principles

3.1 User Account Creation

3.1.1 Staff and Guest Accounts

3.1.1.1 Accounts for new staff members will be created by the division of IT Services upon receiving the complete and approved User Email/Internet Application Form from the division of Human Resources (HR).

3.1.1.2 Guest accounts will be created after the approval from appropriate managers in the division of Human Resources or Division of IT Services as deemed appropriate.

3.1.2 Student Accounts

3.1.2.1 Accounts for new students will be created automatically by the Student Management System (Banner) upon their admission.

3.1.2.2 The accounts, with the correct authentication, will provide access to necessary academic resources and systems like internet, learning management system and login to computers.

3.1.2.3 Accounts will remain active throughout the program duration and an additional 4 weeks after the exams to allow students to view their official results.

3.1.3 Generic and Service Accounts

Generic and service accounts will be created upon approval from the Deans or Directors as applicable. Final approval will be granted by IT Services.

3.1.3.1 These accounts are needed for various reasons such as integrating multiple systems and applications, email notifications, during projects and for temporary access to systems. Service account is a special type of account used by applications, services, or automated processes, rather than by a human user

3.1.3.2 Generic accounts must have an expiry date and be assigned to a risk owner as approved by the supervisor/manager - this is the individual nominated as being operationally responsible for the account(s) on a day-to-day basis.

3.1.3.3 IT Services will periodically disable generic accounts after the account expires, or at the request of the risk owner.

3.1.3.4 Risk owners are responsible for the assessment of business risks arising from the use of generic accounts and ensure safe keeping of the login credentials.

3.1.4 Official Accounts

These accounts will be created for positions such as OA, EO, Projects, Research, Managers, and higher positions to ensure email access continuity. These accounts will have the same expiry date as the associated staff account.

3.2 Password Requirements

3.2.1 Password Composition

3.2.1.1 Passwords for all accounts must be at least 8 characters long.
3.2.1.2 Passwords must be complex and include a combination of uppercase letters, lowercase letters, numbers, and special characters.

3.2.2 Password Management

3.2.2.1 Passwords must be changed every 90 to 120 days or as deemed appropriate considering industry's best practices, excluding Service accounts and the domain administrator account password, which must be changed after the system administrator's departure or, whichever occurs first. This ensures enhanced security, protects sensitive information, and maintains system integrity by ensuring only authorised personnel have access.
3.2.2.2 Service account password will be changed annually.
3.2.2.3 Users cannot reuse the last 5 passwords.

3.2.3 Account Lockout:

3.2.3.1 Accounts will lock after 5 failed login attempts and remain locked for at least 15 minutes.
3.2.3.2 Passwords must not be easily guessable and must not contain easily guessable information such as the user's name, position, or common words.
3.2.3.3 Staff will be prompted to change their password upon first login to the computers on the FNU network.

3.2.4 Password Protection

3.2.4.1 Passwords must not be shared with anyone.
3.2.4.2 Measures such as multi-factor authentication (MFA) will be enabled for services as available to provide an additional layer of security to prevent cyber-attacks.

3.3 Dormant Accounts

Dormant accounts are defined as accounts that do not have any login activity for a period of 365 days, excluding Domain administrator, Official, Service, and accounts of staff on leave.

3.4. Disabling and Deleting Accounts

3.4.1 Disabling Accounts

3.4.1.1 User accounts for exiting staff shall be disabled by the Division of IT Services upon receipt of a completed and authorized Staff Exit Form from the Division of Human Resources.

3.4.1.2 Student accounts inactive in the University's Learning Management System (LMS) for 90 days will be disabled but not deleted, allowing easy reactivation for returning students.

3.4.1.3 Accounts will be disabled temporarily in the event of any suspicious activity or a security breach.

3.4.1.4 Accounts will also be disabled on ad-hoc basis upon written advise from appropriate HR department and Registrar's office for staff and student accounts respectively.

3.4.2 Deleting Accounts

Staff accounts need to be deleted in a timely fashion to reduce security risks, free up storage space (e.g. One Drive) and licenses.

3.4.2.1 Staff accounts will be deleted 90 days after being disabled, unless there is a legal or operational requirement to retain the account.

3.4.2.2 It is the responsibility of the supervisor/manager of the departing staff to ensure important information is retained and that relevant data and files have been handed over before the user exits from the department/University to prevent data loss.

3.4.2.3 Only staff emails will be archived by IT Services before deleting the account.

3.4.2.4 Student accounts will be deleted after they become dormant.

3.5 Remote Access

3.5.1 Remote desktop access is provided to support flexible working arrangements and ensure continuity of operations at Fiji National University (FNU).

3.5.2 Remote desktop access must be endorsed by the relevant Division or college head and approved by IT Services. Only authorized users with a legitimate need for remote access will be granted remote desktop privileges.

3.6 Active Directory Access Rights Review

3.6.1 User Access rights review will be conducted quarterly to ensure no user accounts remain active after their exit from the University and that no users with excessive access exist in the Active Directory.

4.0 Responsibilities

4.1 IT Services

4.1.1 Responsible for the creation, management, and deletion of user accounts. IT Services may use its judgement or seek clarifications and approval from Director HR to address ambiguous situations.

4.1.2 To ensure compliance with this policy and conduct quarterly audits of user accounts.

4.2 Human Resources

4.2.1 Responsible for promptly notifying the IT Services of new hires, terminations, and changes in staff employment status.

4.3 Account Holders

4.3.1 Users are responsible for maintaining the security of their passwords and for complying with this policy.

5.0 Misuse and Abuse

All users must comply with the conditions set out in this policy. If any user breaches the Policy, the University may take disciplinary action.