



POLICY NUMBER: 3

ITS Software Compliance Policy

Prepared by	IT Services Division
Approving Authority:	FNU Council
Date Approved:	1 August 2025
Next Review:	1 August 2028
Version Number:	1.0

1.0 Purpose

The purpose of this Policy is to outline the acceptable use of software on the university owned devices at Fiji National University, to protect the University and its authorized users from legal action resulting from the use of unauthorized software, and to gain efficiencies from centralized software procurement.

2.0 Scope

This policy applies to all Fiji National University employees, contractors, consultants, temporary staff, students, and other workers at the University, including all personnel affiliated through third parties.

3.0 Policy Principles

- 3.1 Fiji National University will only use legally acquired software that is configured and used in accordance with the license terms and conditions.
- 3.2 To maintain the integrity, security, and compliance of the University's IT environment, all Fiji National University (FNU) issued computing devices shall be secured against the unauthorized installation of software.
 - 3.2.1 Access Restriction: The ability to install or modify software on FNU-owned computing devices will be strictly restricted. Only designated and authorized IT Services staff will be granted administrative privileges necessary for software installation.
 - 3.2.2 User Privileges: End users will operate under standard user accounts without administrative rights. This measure ensures that no unapproved software—whether intentional or accidental—is introduced into the university network environment.
 - 3.2.3 Monitoring and Enforcement: FNU will implement endpoint protection, application control, and system monitoring tools to enforce this policy. Any attempt to bypass these restrictions will be considered a breach of FNU's IT policies and may result in disciplinary action.
 - 3.2.4 Exceptions: Any requests for new software installation by staff must be submitted through the Service Desk, accompanied by a valid business case. Approval must be granted by the Director of IT Services or their delegate before installation is permitted.
- 3.3 Use of software which tests or attempts to compromise University systems or network security is prohibited unless the Director of IT Services has been notified and has given authorization for the use of testing systems.
- 3.4 When staff and students are issued with University-owned computer devices, it will be loaded with the software below at minimum by the IT Services:

Staff windows OS	Staff Mac OS	Student windows OS
Windows 10 Pro (64 bit) or above	MS365 Apps or any approved university Office Application	Windows 10 Pro (64 bit) or above
Microsoft365 Apps or any approved university Office applications		Supported Microsoft Office applications
ESET Endpoint Security (Staff) or University approved endpoint security software		ESET Endpoint Antivirus or University approved endpoint security software
Google Chrome, and Microsoft Edge Browser		Google Chrome, and Microsoft Edge Browser
WinRAR		WinRAR
Adobe Reader		Adobe Reader
VLC Player		VLC Player
OneDrive		
MS Teams		

3.5 Free Software(s) may only be used if the free license conditions explicitly allow for use in an enterprise (University) with the approval of the respective supervisor and Director of ITS.

3.6 When staff or students leave the University, their entitlement to use University-licensed software on personally owned devices ends. Some education software license terms allow for the installation on personal devices. Consequently, it becomes the responsibility of the user to have all such software promptly uninstalled from their personal computers.

3.7 Software Procurement and Installation

3.7.1 Information Technology Services is responsible for the purchasing, renewal, and disposal of all software to be used on university owned devices.

- 3.7.2 Any software renewal, increase in license, and new request must be submitted with proper justification, approval from Dean or Director and usage report where applicable.
- 3.7.3 Software which has been personally purchased will not be installed on Fiji National University owned computer devices.
- 3.7.4 The IT Services will not procure licenses for installation on staff and student's personal computers separately.
- 3.7.5 ITS is responsible for the installation of the software on university owned devices.

Under unique circumstances some staff may be provided administration privileges to install software on university owned devices in the pursuit of teaching, learning and research; these privileges are governed and regulated by the ITS Software Compliance Policy.

3.8 Software License Management

ITS is responsible for ensuring that all software used within the university has been legally acquired or purchased and is being used within the terms of the software license. For each item of software managed by ITS, adequate records are to be kept about the software, such as:

- a) The name, platform, and version number of the software.
- b) The number of licenses purchased and used.
- c) The date purchased and purchase order reference.
- d) The location of the software installed, installation media, installation codes and documentation
- e) Any restrictions on the licensed use of the software
- f) Date of renewal

4.0 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.