# Digital Software Asset Management Procedures

**Table of Contents**



## 1. Governing Policy

Digital Assets Policy

## 2. Purpose

To outline the process for managing software assets for Flinders University.

## 3. Definitions

| | |
|---|---|
| **Bring Your Own Device (BYOD)** | A computing device or other hardware asset owned by an individual and utilised in the course of university business, educational or research activities. |
| **Digital hardware asset** | A type of digital asset with physical or tangible components that make up or contribute to an organisation's information technology infrastructure. It includes those components currently in use, those in storage, and support equipment. |
| **Digital software asset** | A type of digital asset containing the digital or intangible components of an organisation's information technology infrastructure. It encompasses software applications, programs, licenses and related resources that are utilised for various purposes within an organisation. |
| **Freeware** | Software that is available to the user free of charge with no imposition of rights restriction on the user, and cannot be manipulated by the user |
| **Mobile communications device** | A portable hardware device primarily utilised for communications purposes, including (but not limited to) mobile or smartphones, pads or tablets. |
| **Open-source software** | Software that is designed to be manipulated by end users, whereas freeware is typically not so designed and is provided without access to source code. |
| **Shareware** | Software that is often initially free of charge or for evaluation, after which a fee or some other monetary/financial exchange may be requested for continued use. This may include accepting advertisements or restricting access. |

| | |
|---|---|
| **Software catalogue** | A database/listing of software and/or applications which are approved and licensed for use within the University's digital environment. |

## 4. Procedures

### 4.1. Acquisition and installation

a. A list of licenses and software approved by the CIO (or delegate) will be provided periodically as a software catalogue, available for download/installation through the channels outlined in the catalogue.

b. Flinders University community members seeking to access software not contained in the software catalogue or to use privately owned software on University owned hardware assets must consult IDS for advice and assistance. This includes the use of freeware, shareware and open-source software.

c. New software installations are subject to approval and security clearance by IDS. Installation of approved new software will be managed according to the nature of request and the source of funding (if applicable). If a request is not approved, a suitable substitute may be suggested/recommended.

d. Approved new software will be owned by the requesting business area or individual who will be responsible for any ongoing expenditure requirements.

e. Where a license agreement allows University owned software to be installed on a BYOD, it is the responsibility of the user to install the software on that device. Flinders University accepts no liability for any issue arising from the installation of University owned or managed software onto BYOD.

f. Any software or cloud platform utilised on Flinders University owned/managed digital hardware assets for University business, education or research purposes should be registered in the University's name where possible.

### 4.2. Management

a. All software utilised on University owned/managed digital hardware assets must comply with relevant Australian legislative requirements or restrictions, as well as any usage/access restrictions imposed by Flinders University, and be used in accordance with the terms and conditions associated with relevant license/s.

b. It is the responsibility of the assigned owner of any software to ensure that it is maintained and updated regularly.

c. Software owned and/or managed by IDS and identified as providing University-wide business capability and/or function will be supported via IDS and/or a third-party representative.

### 4.3. Decommissioning and removal

a. Software may be secured or removed from the University digital environment by an authorised delegate (in coordination with the owner and/or user) under the following conditions:

   i. software not in the approved software catalogue that has been installed onto Flinders University digital hardware assets without prior IDS engagement and/or clearance

   ii. software that has been prohibited by Federal, State and/or Territory legislation

   iii. software that is found to present material risk to the University and/or its systems/structures/community

   iv. a responsible owner for a software package or application cannot be identified or established

   v. purchase and/or license documentation for software cannot be presented when requested

   vi. any software that is not in normal use for its expected purpose.

b. All University owned software must be deleted from any BYOD owned/used by a Flinders University community member should that individual cease their relationship with the University.

c. Where a University digital hardware asset is being transferred or reallocated to a new individual or purpose, all previous software will be removed by IDS and new profiles/applicable software will be installed (where required) before the asset is transferred or reallocated.

## 5. Authorities

These authorities may be sub-delegated, provided the sub-delegation is made in accordance with the Delegations Policy.

| Delegate | Authority |
|---|---|
| **Chief Information Officer** | a. Approve the list of licenses and software to be provided as the software catalogue, available for download/installation through the channels outlined in the catalogue. |
| **Chief Information Officer**<br>**Chief Information Security Officer** | b. Approve the securing or removal of any software or application from the University's digital environment in the conditions set out in Procedure 3.4.a. |

## 6. Related documents

Digital Security Policy

Digital Hardware Asset Management Procedures

| | |
|---|---|
| **Approval Authority** | Vice-President (Corporate Services) |
| **Responsible Officer** | Chief Information Officer |
| **Approval Date** | 31 July 2024 |
| **Effective Date** | 31 July 2024 |
| **Review Date*** | 2027 |
| **Last amended** | |
| **CM file number** | CF24/511 |

* Unless otherwise indicated, this policy or procedures still apply beyond the review date.

Printed versions of this document are not controlled. Please refer to the Flinders Policy Library for the latest version.