Flinders University

# Digital Hardware Asset Management Procedures

**Table of Contents**

## 1. Governing Policy

Digital Assets Policy

## 2. Purpose

To outline the process for managing digital hardware assets for Flinders University.

## 3. Definitions

| | |
|---|---|
| **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. |
| **End-of-life** | The pre-determined end of usable or acceptable lifespan for a digital asset. |
| **Profile (Staff, Learning & Teaching, Specialist)** | The standard operating environment (SOE) on a hardware asset as determined by the usage of that asset (i.e., Staff, Learning & Teaching or Specialist). The SOE is determined and configured prior to the deployment of the asset. |
| **Non-standard computer package** | A package of digital hardware assets for use in University research, education or business activities containing elements which are not pre-determined or approved and/or which deviate from standard hardware requirements. |
| **Owner** | An individual, or a Division or College, who has acquired the digital asset for the use of their staff / customers / students. This includes digital hardware assets located at temporary workstations and spaces (hot desks), student labs / study spaces and shared staff machines. |
| **User** | An individual determined as the primary/sole user of a digital hardware asset. The user will be required to account for the digital hardware asset throughout its lifespan. |
| **Shared hardware asset** | A digital hardware asset available to or intended for the use of more than one person. |

| | |
|---|---|
| **Standard Computer Package** | A pre-determined grouping of digital hardware assets available for purchase and use in University research, education or business activities, as approved by IDS. |

## 4. Procedures

### 4.1. Acquisition

a. Flinders University staff will be allocated or have access to one (1) Standard Computer Package to carry out their general work duties.

b. Staff in newly created positions may be allocated/have access to existing digital hardware assets still within its scheduled lifespan. New digital hardware assets will be acquired where existing digital hardware assets are not available or where an existing digital hardware asset is deemed not fit for the newly created position by both the employing College/Division and IDS.

c. Staff who are moving into an existing role with a standard computer package already available are expected to utilise the existing package allocated to that role unless an existing digital hardware asset is deemed not fit for the purpose by IDS.

d. Non-Standard Computer Package requests will be assessed by IDS on a case-by-case basis and will require justification and approval from both the relevant Division Director or Director, College Services and the Chief Information Security Officer (or delegate).

### 4.2. Management

a. IDS will record details of digital hardware assets.

b. Digital hardware assets for individual use will be allocated to the individual who will be the User of the digital hardware asset.

c. Shared digital hardware assets will be allocated to the relevant Manager/Supervisor, Division or College as the Owner.

d. The User or Owner will be liable for the asset throughout its lifecycle and will be required to make the asset available to IDS upon request.

e. Users or Owners must notify IDS at the earliest opportunity if a digital hardware asset in their possession or use is lost, stolen or damaged.

f. Digital hardware assets may be reallocated to another individual/group or re-provisioned/re-purposed through prior consultation with IDS.

g. Flinders University owned and managed digital hardware assets will be supported, maintained and repaired by IDS either directly or via a third-party. Any digital hardware assets that have not been pre-approved and/or purchased in accordance with the University's Procurement Policy will not be supported or maintained by IDS.

h. All digital hardware assets operating within the University's digital environment must comply to the University's security and configuration requirements.

i. In order to comply with the University's security and configuration requirements, all Flinders University owned and managed digital hardware assets will be deployed with a profile, applications and security management software pre-installed by IDS. These must not be removed without prior written approval from IDS.

j. Any digital hardware asset found to not comply with the University's security and configuration requirements or found to present any form of risk to the University's digital environment may be removed from the environment by an authorised delegate.

### 4.3. Replacement and disposal

a. Replacement and disposal of digital hardware assets will be coordinated with the relevant owner and users in accordance with the following schedule:

| ASSET | SCHEDULE |
|---|---|
| Staff computers | Every four (4) years commencing from the start of the device warranty period. |
| Learning and Teaching computers or computers for student use | Every five (5) years commencing from the start of the device warranty period |
| Specialist computers (e.g., for research purposes) | Every five (5) years commencing from the start of the device warranty period. |
| Peripheral items (e.g., monitors, docking stations, keyboards) | As determined by IDS on a needs and performance basis. |

b. Where a digital hardware asset has reached or exceeded its end-of-life, it may need to be relinquished to IDS and removed from service if it is creating risk. End-of-life or high risk hardware assets removed from service will not be redeployed, reimaged or reused in the University's digital environment. This would be done in coordination with users and others.

c. Digital hardware assets no longer in use must be relinquished to IDS for reimaging, retirement or redeployment. All relinquished assets will be securely wiped of all data related to its previous deployment (where applicable) by IDS before they are redeployed, repurposed or disposed of.

d. All digital hardware asset disposals will be carried out in a manner compliant with the relevant legislation and University policy.

## 5. Authorities

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

| **Delegate** | **Authority** |
|---|---|
| **Chief Information Security Officer** | a. Approve Non-Standard Computer Package requests, if also approved by the relevant Division Director or Director, College Services. |
| **Chief Information Officer**<br>**Chief Information Security Officer** | b. Approve removal of any digital hardware asset from the University's digital environment found to not comply with the University's security and configuration requirements or found to present any form of risk to the University's digital environment. |

## 6. Related documents

Digital Security Policy

Digital Software 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** | CF24/510 |

* 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.