POLICY: IT Asset and Acquisition	
Policy Number	TM14
Version	1
Functional Area	Technology Management
Policy Custodian	Executive: Technology Management
Approved by	The Board
Decision Number	B.03.2026.46
Approval Date	30/06/2026
Effective Date	30/06/2026
Review Cycle	Triennially
Next Review Date	2029
Review History	30/06/2026_v1

1. INTRODUCTION

The Da Vinci Institute (The Institute) recognises Information Technology (IT) assets as strategic resources essential for delivering academic programmes, research and administrative services and day-to-day operational duties.

This policy ensures that IT assets are acquired, managed, secured and disposed of in alignment with institutional governance, compliance and accountability frameworks. The Institute is committed to responsible asset lifecycle management to maintain financial accountability, system integrity and continuity of services

2. DEFINITIONS

IT Asset	Any item of value related to Information Technology that The Institute owns, licenses, or controls, including but not limited to hardware, software, and Development.
Hardware	Computers, Screens, TV's, Projectors, laptops, servers (Cloud, On-prem), mobile devices, network equipment peripherals and or other digital devices. All hardware assets labelled with an asset number.
Software	Licensed applications, operating systems, productivity suites, cybersecurity tools, databases and cloud-based and academic subscriptions or services (e.g., Microsoft 365, Zoom, Azure).
Development	Custom-developed systems, software code, digital platforms, mobile applications, integrations, or configurations commissioned or built for institutional use. These are recognised as intangible assets with intellectual property (IP) and operational value.
End-user	Any employee, faculty member, contractor, or student who has been formally allocated an official Da Vinci Institute (DVI) email address or granted access to Da Vinci systems including hardware, software, or development tools for the purpose of fulfilling their institutional role, assigned duties, or academic activities.
Theft	The unlawful removal of The Institute's IT assets while on the premises or in the possession of a staff member. All incidents of theft must be reported immediately to the Technology Management Department (IT), Business Operations, and Security/People Management, and accompanied by a case number from the

	South African Police Service (SAPS) or relevant authority and submitted to the allocated Insurance company within 24hours.
New Appointments	Refers to newly employed staff, contracted faculty/personnel, or interns requiring IT equipment to perform their roles effectively. Allocation is based on the individual's job function and aligned to standard device categories defined by The Institute.
Hardware Failure	The malfunction of an IT device or component that prevents it from performing its intended function. Hardware failure must be verified by the IT Department before replacement or repair is authorised.
End-of-Life (EOL)	The stage at which IT hardware including cloud infrastructure, or software which is no longer supported by the vendor, is incompatible with institutional systems, or is no longer cost-effective to maintain. End-of-life assets are retired (disposed of) and replaced according to lifecycle management standards.
Lifecycle	The period from the acquisition of an IT asset (hardware, software, or development) through its deployment, active use, maintenance, and eventual retirement or disposal. For hardware, the typical life cycle is 3–5 years, depending on warranty, performance, and business requirements. For software and licenses, the life cycle extends until the vendor ends support, security updates are discontinued, or renewal is required. For development assets (custom systems or applications), the life cycle is determined by continued maintainability, compatibility with institutional systems, and evolving business needs.

Delegation of Authority (DOA)	The Delegation of Authority (DOA) is a formal governance framework that defines the levels of decision-making power and financial approval limits within an organisation. It ensures that authority is exercised responsibly, transparently, and in alignment with institutional strategy and compliance requirements. Any deviation from this policy must be formally motivated and approved in accordance with the Delegation of Authority (DOA).
IT Asset Disposal	The controlled internal process of decommissioning, writing off, recycling, or removing IT equipment from operational and financial records following approval by Executive Technology Management and processing by Finance.

3. REGULATORY FRAMEWORK

This Policy is benchmarked against the following legislation and frameworks:

a. Institute of Directors in South Africa (IoDSA). 2024. *King V™ Report on Corporate Governance for South Africa*. Johannesburg: Institute of Directors in South Africa.
b. International Organization for Standardization (ISO). 2022. *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements*. Geneva: ISO.
c. Republic of South Africa. 1997. *Higher Education Act, No. 101 of 1997*. Pretoria: Government Printer.
d. Republic of South Africa. 2002. *Electronic Communications and Transactions Act, No. 25 of 2002*. Pretoria: Government Printer.
e. Republic of South Africa. 2013. *Protection of Personal Information Act, No. 4 of 2013*. Pretoria: Government Printer.

4. SCOPE

a. This Policy applies to all employees, students, faculty, contractors and stakeholders who are allocated IT assets by The Institute.
b. It governs acquisition, allocation, use, maintenance, transfer and disposal of all IT hardware and software.
c. IT assets allocated to users remain the property of The Institute and may not be transferred, sold, exchanged, or reassigned without approval from Executive Technology Management.

5. PURPOSE

The purpose of this Policy is to:

a. Ensure transparent, cost-effective and compliant acquisition and disposal of IT assets.
b. Provide clear processes for handover and accountability.
c. Maintain a secure and accurate asset register.
d. Protect The Institute's technological investments and ensure sustainability.

6. ACQUISITION AND HANDOVER PROCEDURE

The following procedure governs acquisition and handover of IT assets (Refer to Annexure A: Purchase and Handover of IT Equipment Procedure):

a. **Request Initiation** – Requests are submitted by People Management, staff, line managers, or IT for new equipment or replacements (e.g., new appointments, theft, hardware failure, end-of-life).
b. **IT Review** – IT validates the request against institutional requirements and policies.
c. **Quotation Process** – IT sources quotations from three approved vendors, ensuring best value. Where three quotations cannot reasonably be obtained, written motivation and approval must be documented.
d. **Approval** – The Executive: Technology Management, Finance and Executive: Operations approve the acquisition in line with the DOA.
e. **Invoice & Finance Verification** – Finance verifies vendor, budget availability and approves vendor payment.
f. **Delivery & Verification** – IT department checks delivery against purchase order.
g. **Setup & Configuration** – IT department installs, configures, migrates data and trains or onboards the user.
h. **Asset Tagging** – IT department labels equipment with a unique asset number and updates Finance and related asset tracking systems.
i. **Handover & Acknowledgement** – Staff member or the relevant stakeholder signs handover form; IT countersigns; copies sent to Finance and HR are stored and captured with the related asset tracking system.
j. **Finance Confirmation** – Finance verifies receipt with the user.
k. **Asset Register Update** – Asset details are recorded in the central register.
l. **Resignation, retirement, dismissal** – Assets to be returned on their last day, as per the instruction and confirmation by the People Management department.

7. DISPOSAL OF IT ASSETS

a. The disposal of IT assets is managed as an internal operational process coordinated between Executive: Technology Management and the Finance Department.
b. Where an IT asset is identified for disposal, replacement, write-off, insurance claim, or decommissioning, approval must be obtained from the Executive responsible for Technology Management. Upon approval, the Executive: Technology Management will communicate the details and reason for disposal to the Finance Department via formal written communication (email or approved internal documentation).

c. The Finance Department will be responsible for removing the asset from the accounting asset register and financial systems in accordance with financial control procedures.
d. Following approval and financial processing, the IT asset may be:
    I. Collected by the insurance provider where an approved insurance claim exists
    II. Disposed of in accordance with the organisation's Environmental Policy and applicable environmental regulations
    III. Retained for spare parts or component recovery where appropriate and authorised.
e. All disposals must ensure that organisational data security, environmental compliance, and financial governance requirements are maintained.
f. Prior to disposal, reassignment, insurance collection, recycling, or component recovery, all institutional data must be securely removed or destroyed in accordance with information security and POPIA requirements.

8. HARDWARE ASSET COST CAP AND ALLOCATION

Hardware Asset Cap:

a. Standard office laptops and desktops are capped at R15,000 per unit in general and as per budget.
b. The Institute maintains a standard range of approved office devices priced between R10,000 – R15,000, suitable for academic, administrative, and general business use.
c. Any request for specialised hardware (e.g., high-performance devices for graphic design, data analysis, or video editing) that exceeds the R15,000 cap must be formally motivated by the requesting manager and approved by:
    I. The purchase order process is initiated by the requester.
    II. All purchase orders for IT equipment must be approved by the Executive: Technology Management prior to the placement of the order.
    III. The Executive: Operations, Executive: Finance, and the relevant Department Head / Line Manager may be included in the workflow as reviewers and acknowledgement stakeholders.
    IV. Final procurement may only proceed once the supplier invoice has been approved through the accounting system by the Executive: Technology Management.
    V. Executive: Technology Management – Approval required
    VI. Executive: Operations – Review and acknowledgement
    VII. Executive: Finance – Review and acknowledgement
    VIII. Department Head / Line Manager – Review and endorsement.

Purpose of Cap:

a. Ensure cost-effective procurement aligned with budget constraints.
b. Standardise hardware across the organisation to improve support, efficiency, and asset lifecycle management.

c. Allow flexibility for exceptions where business-critical specialised performance is required.

9. MAINTENANCE AND REPLACEMENT

a. Only IT staff or approved suppliers may perform maintenance or repairs.
b. Replacement or disposal will be considered if the repairs exceed the actual acquisition price of the hardware device
c. Maintenance and repairs must be logged with IT and approved before execution.
d. Replacement or disposal of hardware requires Executive: Technology Management and relevant department head acknowledgement authorisation and user sign-off.
e. All changes: Asset transfers, replacements or disposals must be recorded in the asset register.
f. Software assets must be monitored for updates, security patches, and version control.
g. Licence renewals must be tracked and renewed in time to ensure compliance.
h. Unsupported or end-of-life software must be decommissioned (Disposed) responsibly, with data migrated or archived accordingly.
i. Renewal or replacement of software licenses will be considered when existing licenses expire, when software reaches end-of-support/Life from the vendor, or when system performance or security requirements necessitate an upgrade. All license renewals must align with approved budget allocations and comply with the Delegation of Authority (DOA) and this Policy. The renewal or replacement request must be formally initiated and approved by the Executive: Technology Management, Head of Department (HOD) and relevant stakeholders.
j. Replacement or redevelopment will be considered when platforms are no longer maintainable, do not meet business requirements, or when new technologies offer significant efficiency or compliance benefits.
k. Software and development assets depending on vendor support, system performance, and evolving institutional needs.
l. Renewal or replacement actions will be undertaken in accordance with available budgets and must be approved by the Executive: Technology Management and Executive: Operations and in accordance with the DOA.

10. INVENTORY AND RECORD-KEEPING

a. The IT department maintains the central asset register with the head of operations and the Finance department, updated with all acquisitions, changes, transfers and disposals within the allocated accounting system.
b. Quarterly stock takes are conducted jointly by Technology Management, Finance and Head of Operations.
c. Records (Capex forms, repair forms, handover documents, invoices) are retained for a minimum of 7 years.

11. RESPONSIBILITIES

a. Executive: Operations, Executive: Technology Management – Oversees compliance with procurement governance.
b. Executive: Technology Management – Validates requests, approves quotes, ensures policy compliance.
c. IT Staff – Configure, install, label, maintain, and update asset records.
d. Finance – Verify budgets, process payments, confirm receipt, and maintain records.
e. People Management (HR) – Record IT asset allocation in personnel files.
f. End User – Use equipment responsibly, safeguard assets, report issues, and return assets upon exit.

12. COMPLIANCE AND DISCIPLINARY ACTION

a. Non-compliance with this policy, including unauthorised purchases, negligence, or misuse of IT assets, may result in disciplinary action. This may include cancellation of access privileges, repayment of costs, warnings, suspension, or termination of employment.
b. Legal action may also be taken in cases of fraud or wilful misconduct.

13. REVIEW OF THIS POLICY

a. This policy shall be reviewed annually by the Executive: Technology Management and Executive Head: Business Operations, in consultation with the Executive: Registrar.
b. All amendments must be submitted for Board approval after FAIIR committee review.

14. ANNEXURE A: PURCHASE AND HANDOVER OF IT EQUIPMENT PROCEDURE

All purchases of new systems hardware or new components for existing systems must be made in accordance with The Institute's information security, finance and other relevant policies, as well as the required technical standards. Such requests to purchase must be based upon user requirement specifications considering longer term business needs.

All equipment must be fully and comprehensively tested and formally accepted by users before being transferred to the live environment, taking into consideration applicable policy requirements.

Step	Description	Notes
1	Request is received from the staff member, line manager or IT staff for IT equipment due to various reasons such as new appointments, theft, hardware failure, performance or end-of-life issues.	Requests are submitted through designated channels, such as a ticketing system or specific electronic forms provided by the IT department.
2	IT department reviews the request to ensure compliance with organisational policies and	In some cases, only an upgrade will be required before new, or

	requirements, and to confirm the validity of the request.	replacement devices are considered.
3	IT department requests quotes from approved vendors or suppliers, alternatively three quotations must be obtained from three different vendors.	Evaluate all quotes to determine the best fit for the required specification within the budget constraints.
4	The quotes are forwarded to the relevant authority for approval or notification thereof, which may include the staff member's manager and IT manager.	The IT Manager to provide a reason for recommending a specific quote.
5	Once a quote is approved, the IT department informs the vendor to forward the invoice to Finance@davinci.ac.za	The finance department verifies the order against the allocated budget and comments by the line manager or IT Manager and approves payment to the vendor.
6	Upon delivery, the IT department verifies the contents of the delivery against the purchase order.	The IT department closely monitors the status to ensure timely delivery and provides regular updates to the staff member.
7	The IT department assists the staff member with setting up and configuring the new equipment according to organisational standards.	This may include data migration, software installation, and user training.
8	Staff member to acknowledge receipt of the equipment by signing the handover document and the IT manager or designated staff member countersigns to confirm the successful handover.	Digital or physical document sent to the Finance Department and HR department for record keeping.
9	Finance department to verify with the recipient that they received the equipment.	Phone call or email and document date and time of call on asset register.
10	Asset will be allocated in the asset management system, and an asset number will be assigned to the device, which must be displayed on the equipment.	