Griffith UNIVERSITY
Queensland, Australia

Policy

Software Asset Management Policy

1.0 Purpose

This policy aims to maintain a mature and centralised software asset management approach, to ensure a compliant and optimised licensing position is maintained, including the provision of appropriate governance and oversight.

2.0 Scope

This policy applies to any Griffith University acquisition of software licences and/or services from a source outside of the University, regardless of whether it is free, a once-off cost, or based on a subscription model.

An established exception to this policy is use by the Griffith community of university authorised social media platforms that allow user content to be uploaded or modified (e.g. YouTube) without compromising Griffith's copyright guidelines, IT Code of Practice and using University information computing resources.

3.0 Policy statement

The implementation of consistent and centralised software asset management practices at the university will facilitate improved control and management of ICT investments and reduce financial and legal risks associated with software utilised by the university community. This policy will ensure:

- Due diligence with the Queensland Government requirements of the university as a statutory body with respect to relevant legislation and policies
- An appropriate level of oversight is provided, to address the possibility of a higher level of risk, including licence compliance and data security
- Risks are identified, prioritised, and managed in a coordinated manner.
- Effort is not duplicated (existing internal and external options should be explored prior to acquiring a new service), nor ownership of the University's assets compromised
- The University's information assets remain protected and available
- The University derives maximum value from expenditure on IT services
- Savings achieved through licences only being purchased when needed and unused licences being tracked, pooled and transferred as required
- Cost reductions through linkages from metering reports to ICT planning to ensure maintenance agreements will be continued only for software that is currently in use
- Diminished exposure to financial and legal risks

- More efficient use of resources, with time not being wasted in attempting to locate media, supporting untested software or searching for licences
- More accurate and precise budgeting will be possible, since maintenance renewal dates will be captured, upgrades will be accurately calculated, and user base licence growth can be calculated

4.0 Roles, responsibilities and delegations

In accordance with the current university procurement guidelines, all software is to be purchased through Digital Solutions.

Digital Solutions are responsible for the Software lifecycle, including procurement, compliance, licence key management, deployment, licence transfer and optimisation and disposal.

The use of university credit cards to purchase software is not permitted, this includes Software-as-a-Service or other IT software subscription services.

Many software licence agreements require the execution of a contract. An IT Contract is considered a special contract subject to the Griffith University Delegations Framework. Only the Chief Digital Officer, Chief Operating Officer or Vice Chancellor can sign an IT contract.

Risk analysis and due diligence relating to compliance, financial and contractual risks are undertaken by Digital Solutions, Finance, and Legal Services prior to contract execution.

On an ongoing basis, operational and contractual risks are to be managed by the relevant Business Owner and Data Custodian for that service. Managers, at all levels, are required to ensure that staff and students are aware of their responsibilities under the Information Technology Code of Practice.

While providing benefits to the University, use of software can also introduce risks. As risks are identified, they must be managed via the Digital Solutions IT Risk Register. The Head of IT Governance, Risk, Compliance and Continuity is responsible for maintaining the Digital Solutions IT Risk Register and reporting monthly to the Chief Digital Officer.

Any significant IT risks associated with licenced software must be escalated immediately to the Chief Digital Officer.

ROLE	RESPONSIBILITY
Chief Operating Officer	Approval of Software licences and agreements including execution of IT contracts up to Financial Delegation
Chief Digital Officer	Approval of Software licences and agreements including execution of IT contracts up to Financial Delegation. Reviews and provides recommendations for licences and agreements for Chief Operating Officers approval and execution
IT Sourcing and Contracts Specialist	Review IT Contract documents and coordinate the IT Solution review process, including document management processing
IT Procurement Officer	Manage the university software asset lifecycle including procurement, licence key management and end of service life / disposal

5.0 Definitions

For the purposes of this policy and related policy documents, the following definitions apply:

Software as utilised in this document incorporates software applications, that are installed on university owned equipment, or accessed via cloud-based services. The use of software is governed by a licence agreement, which details the rights of usage for the software.

Software licence – the purchase of software provides the university a 'right to use' the software in accordance with the vendor's terms or End User Licence Agreement (EULA). The university does not own commercial software, it purchases a licence (a right to use). Software can be licenced perpetually or on a subscription basis, using a variety of metrics to determine costs and compliance.

INFORMATION	Printable version (PDF) Downloadable version (Word)
Title	Software Asset Management Policy
Document number	2023/0001015
Purpose	This policy aims to maintain a mature and centralised software asset management approach, to ensure a compliant and optimised licensing position is maintained, including the provision of appropriate governance and oversight.
Audience	Staff
Category	Operational
Subcategory	Staff
Approval date	3 April 2023
Effective date	3 April 2023
Review date	2025
Policy advisor	Chief Digital Officer
Approving authority	Chief Operating Officer

RELATED POLICY DOCUMENTS AND SUPPORTING DOCUMENTS	
Legislation	Queensland Government – Procurement and Disposal of ICT products and services policy (IS13) Queensland Government – Software Asset Management Policy
Policy	Procurement and Supply Policy Cloud Hosting Policy Asset Management Policy Enterprise Information Systems Policy Information Security Policy
Procedures	N/A