GELOS
ENTERPRISES

ICT Procurement and Installation Policy

GELOS ENTERPRISES

Contents

Introduction

This policy document describes the process for researching, procuring, evaluating and installing hardware and software for:

- an upgrade to an existing computer system
- a new computer system
- peripheral devices.

All associated forms are available from the Gelos Enterprises intranet site.

Allowing employees to install software on company computing devices opens the organisation up to unnecessary security risks and other issues. Some examples of the problems that can be introduced when employees install software on company equipment include conflicting file versions or a dynamic link library (DLL) that can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organisation's network.

1. Scope

This policy applies to all Gelos employees, contractors, vendors and agents with Gelos-owned mobile devices. This policy covers all computers, servers, smartphones, tablets and other computing devices operating within Gelos.

2. Process and responsibilities

The table outlines the key steps in procuring and installing hardware and software, along with the roles and responsibilities of those involved at each stage.

Table 1: ICT procurement and installation process and responsibilities

Step	Responsibility	Procedure
1.	End user or department	• Lodge request via email or service desk
2.	ICT Support Senior Manager	• Approve initial request • Assign task to appropriate ICT Technician or Specialist
3.	ICT Technician or Specialist	• Complete appropriate Hardware and Software Upgrade Request (docx) form, New Computer System Request, Peripheral Device Request). – One copy of the appropriate request form is to be completed for each ICT solution. If it includes multiple components, or will be completed on multiple machines, one form can be used. – Confirms request with end user. – Liaises with end user to determine specific needs. • For software requests, a pre-installation audit is performed. • Complete Quotation Request (docx) form . – Research and evaluate solutions. – Research costs of ICT solution from vendors. – Determines best solution, including costings. • Liaise with end user regarding proposed solution (if applicable). • Liaise with ICT Support Senior Manager regarding proposed solution.
4.	End user	• Signs approval to purchase section of completed Quotation Request form (from Step 3) (if applicable). – Confirm solution meets their needs.
5.	ICT Support Senior Manager	• Sign approval to purchase section of completed Quotation Request form (from Step 3). – Approve solution regarding costs, timeframes and effectiveness. • Organise or delegate the purchasing of hardware.

Step	Responsibility	Procedure
6.	ICT Technician or Specialist	• Complete Installation Plan (docx) • Complete Implementation Plan (docx)
7.	End User	• Sign approval of Installation Plan section of completed Installation Plan form (from Step 6) (if applicable) – Confirms installation plan meets their needs
8.	ICT Support Senior Manager	• Sign approval of Installation Plan section of completed Installation Plan form (from Step 6) – Approve solution regarding preparation, procedure, testing and timeframe
9.	ICT Technician or Specialist	• Organise the installation and configuration of hardware according to the installation plan. • Organise implementation of software according to implementation plan. • Test hardware or software. • Complete Completion of Installation (docx) form. • Train end user if needed. • Evaluate solution and support provided.

3. Procurement

3.1 Source and evaluate technology

3.1.1 Evaluation criteria

After determining detailed task requirements from the relevant end user or department, the following criteria must be considered:

- **Compare options**: Explore multiple tools or systems to understand their capabilities, useability and functionality.
- **Assess scalability**: Consider whether the solution can grow with your business.

- **Evaluate costs**: Include licensing, maintenance, and training expenses.
- **Test or demo**: Whenever possible, request a trial or demonstration to see how the technology performs in real-world scenarios.

3.1.2 Review vendor information

After shortlisting potential solutions, confirm their suitability by carefully reviewing vendor documentation, specifications, and support options. Key considerations include:

- **Technical fit**: Does the technology integrate with our current systems?
- **Compliance**: Does it meet legal, industry, or organisational standards? Will it contribute to environmental efficiency or consume significant energy?
- **Security**: How secure is the technology and can it be breached?
- **Support and training**: Does the vendor offer adequate support and resources?

3.2 Pre-installation audit (software)

Software must be selected from an **approved software list**, maintained by the ICT Systems Support team, unless no selection on the list meets the requester's need.

The ICT Systems Support team will test new software for conflicts and compatibility, as well as measure the level of interoperability (see below). Once the software pre-installation audit report is approved by Management, the ICT Systems Support team will obtain and track the licences and perform the installation.

3.2.1 Measuring the level of information systems interoperability (LISI)

The following table presents a general overview of the major elements that comprise LISI. This provides an assessment process for determining the **interoperability maturity level** or 'measure' of a given system or system pair.

The following table describes the interoperability maturity levels defined by LISI.

- **Information exchange:** The type of information exchange that happens at each level.
- **Level:** Each level is identified by a number from 0 to 4 and by the general nature of the interoperability i.e. Isolated, Connected, Functional, Domain and Enterprise.

Table 2: LISI interoperability maturity model

Information exchange	Level
• Cross-domain information and applications sharing • Advanced collaboration • (Interactive COP update, event-triggered global database update)	**4 – Enterprise** • Interactive manipulation • Shared data and applications
• Shared databases • Sophisticated collaboration • (Common Operational Picture)	**3 – Domain** • Shared data • Separate applications
• Heterogeneous product exchange • Basic collaboration • (Annotated imagery, maps with overlays)	**2 – Functional** • Minimal common functions • Separate data and applications
• Homogeneous product exchange • (FM voice, tactical data links, text files, messages, email)	**1 – Connected** • Electronic connection • Separate data and applications
• Manual gateway • (Diskette, tape, hard copy exchange)	**0 – Isolated** • Non-connected

For more information related to the LISI model, refer to Levels of Information Systems Interoperability (LISI) by the US Department of Defence.

3.3 Quotation requirements

Two quotes from approved vendors must be obtained before a purchase can be made. These quotes may be for the same item from different vendors, or comparable items, for example if there is only one vendor for a product. If multiple pieces of hardware are needed (such as a motherboard and CPU), these can appear on the same quote, if they are from the same vendor.

Hardware must be sourced from an appropriate vendor as per the following requirements:

- must be located within Australia, preferably within Sydney
- preferably with a bricks and mortar store
- must be able to deliver parts
- must be a registered business with an ABN (that is, not private sellers on eBay, Gumtree or similar)
- must be able to provide warranty.

The ICT Support Senior Manager and the End User (if applicable) must approve all purchases.

3.4 Environmental sustainability

Gelos will, when evaluating quotations or tenders, take into consideration the anticipated impact on the environment and show such consideration in their evaluation documentation. This may be achieved by procuring goods and services that will minimise their impact on the environment, including goods constructed from recycled or re-used products.

4. Installation

4.1 Installation plan

An installation plan, which includes a list of steps or tasks that need to be followed as part of the upgrade, must be completed. All steps should be in the correct order and follow the manufacturer's setup, safety and storage/transportation requirements.

The installation plan must also ensure minimal disruption to the daily work of the end user. Where possible, the installation should be scheduled during periods when the end user doesn't need to use their PC. **In situations where this cannot be done, or if the installation will take longer than four hours, an alternative PC must be supplied**.

4.1.1 Backup requirements

If critical data is stored on, or upgrades need to be made to, the machine's hard drive(s), a data backup must be made prior to the upgrade. This backup should be included in the task list of the installation plan. Refer to the Data Backup Policy (pdf) for more details.

The installation plan needs to be approved by both the End User and ICT Support Senior Manager before being implemented.

4.2 Completion of installation

After installation, any changes made must be documented using the Completion of installation form.

4.3 Work health safety

It is the responsibility of the ICT Technician to ensure that they follow the procedures listed in the ICT WHS Compliance Checklist (docx).

4.4 User training

Training must be provided to the end user or other relevant staff members in any new hardware or software installed, if needed or requested. This may include providing links to online documentation, user manuals, one-to-one training or group training where appropriate.

4.5 Evaluation

All installations must be evaluated by requesting the user to complete an online survey. Gelos' preferred online survey provider is SurveyMonkey.

5. Policy compliance

5.1 Compliance measurement

The ICT Systems Support team will verify compliance with this policy through various methods, including, but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved in advance by ICT Systems Support management.

5.3 Non-compliance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related documents

Refer to the following related documents, where required:

- Data Backup Policy (pdf)
- ICT Disposal and Storage Procedure (pdf)
- ICT WHS Compliance Checklist (docx)
- ICT Governance Policy (pdf)
- Standard Operating Environment Policy (pdf)

7. Version control

No	Effective	Approved by	Updates
1	20 August 20XX	Darren Cooper, Chief Technical Officer	Initial release