IT Procurement

and Installation Policy

Red Opal Innovations

Version 3

Table of Contents

Introduction

This policy document describes the process for researching, procuring 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 Red Opal Innovations 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 DLLs 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.

Scope

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

Process and responsibilities

The following table outlines the steps involved in procuring and installing hardware and software, and who is responsible.

Table 1: IT procurement and installation process and responsibilities

Step	Responsibility	Procedure
1	End User	• Lodges request via email or Service Desk
2	Network Manager	• Approves initial request • Assigns task to appropriate IT Technician
3	IT Technician	• Completes appropriate form (*Hardware/Software Upgrade Request, New Computer System Request, Peripheral Device Request*) o One copy of the appropriate request form is to be completed for each IT solution. If it includes multiple components, or will be completed on multiple machines, one form can be used. o Confirms request with end user o Liaises with end user to determine specific needs • For software requests, a pre-installation audit is performed. • Completes *Quotation Request* form o Researches solution o Researches costs of IT solution from vendors

		o Determines best solution, including costings • Liaises with End User regarding proposed solution (if applicable) • Liaises with Network Manager regarding proposed solution
4	End User	• Signs *Approval to Purchase* section of completed *Quotation Request* form (from Step 3) (if applicable) o Confirms solution meets their needs
5	Network Manager	• Signs *Approval to Purchase* section of completed *Quotation Request* form (from Step 3) o Approves solution in regards to costs, timeframes and effectiveness • Organises or delegates the purchasing of hardware
6	IT Technician	• Completes *Installation Plan*
7	End User	• Signs *Approval of Installation Plan* section of completed *Installation Plan* form (from Step 6) (if applicable) o Confirms installation plan meets their needs
8	Network Manager	• Signs *Approval of Installation Plan* section of completed *Installation Plan* form (from Step 6) o Approves solution in regards to preparation, procedure, testing and timeframe
9	IT Technician	• Organises the installation and configuration of hardware according to the installation plan • Tests hardware • Completes *Completion of Installation* form • Trains End User if needed • Evaluates solution and support provided

Pre-installation audit (software)

Software must be selected from an **approved software list**, maintained by the Information Technology department, unless no selection on the list meets the requester's need.

The Information Technology Department will test new software for conflicts, compatibility and measure the level of interoperability (see below). Once software pre-installation audit report is approved by Management, the Information Technology Department will obtain and track the licences and perform the installation.

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. 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. The type of information exchange that happens at each level is also described.

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 Department of Defense.

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 e.g. 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 (i.e. not eBay, Gumtree, etc.)
- Must be able to provide warranty.

The Network Manager and the End User (if applicable) must approve all purchases.

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.**

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.

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

Full system backups should only be scheduled during weekends (between Saturday 8:00PM Sunday 8:00PM) and incremental backups should be scheduled during working days (Monday to Friday) after hours between 9:00 PM – 3:00AM.

E-waste disposal and recycling

All e-waste must be disposed of in an environmentally considerate manner.

Environmental sustainability

Red Opal Innovations 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.

Guidelines for disposal:

- Lithium BIOS batteries must be sent to our contracted disposal company *ezyewaste.com.au*
- *Toner cartridges must be disposed of through our cartridge supplier recycling service ezyrecycling.com.au*
- Cathode Ray Tube (CRT) monitors, printed circuit boards, redundant hardware, must be disposed of by using the local council E-waste disposal facilities.
- Cardboard, paper, and polystyrene will be recycled through our agreed contactor's special bins.
- Any useable computer must have the hard drives removed and destroyed (by drilling) and disposed of via our contractor *computer4charity.com.au*

Guidelines for storage:

- The storage area for hardware and peripherals should be dry, not too hot or humid as well as ventilated.
- Hardware components awaiting repair should be well marked to show that they are in need of repair. They should be stored in a location where they can be easily accessed and not mistaken for other items.
- The hardware or peripheral should be wrapped to protect it from dust or damage and if possible stored in its original packaging.

Work health safety

It is the responsibility of the IT Technician to ensure that they follow the procedures listed in the IT WHS Compliance Checklist.

Completion of installation

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

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.

Evaluation

All installations must be evaluated by requesting the user to complete an online survey. ROI's preferred online survey provider is [SurveyMonkey](#).

Policy compliance

Compliance measurement

The IT Support team will verify compliance to 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.

Exceptions

Any exception to the policy must be approved in advance by IT Support Management.

Non-compliance

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