



UNIVERSITY OF TASMANIA

**Desktop Computing
Procurement, Installation and Service Policy**

2004

Contents

Introduction.....	3
Purpose.....	3
Objectives	3
Scope.....	4
Standards.....	4
1. Hardware Provision (Purchasing & Leasing)	4
2. Software Provision (Purchasing & Leasing).....	5
3. Hardware Service and Desktop Management.....	5
4. Data Storage.....	6
5. Data Backup and Recovery.....	6
6. Hardware Security	7
7. Hardware Lifecycle and Disposal.....	7

Introduction

Information technology plays a vital role in the administrative and day to day function of the University in the 21st century. Desktop computing plays a vital part in this process by delivering functionality across the spectrum of available applications and services to the end user. To this end, it is imperative that all desktop computing hardware is procured, deployed and managed in a manner that is appropriate to the needs of the entire organisation.

In the information technology market of today there exists an extensive range of products to cater for a wide variety of needs. While technology influences purchasing choices and the software market rapidly expands to meet a constantly broadening scope, total cost of ownership (TCO) is increasingly recognised as the vital benchmark to be used in technology procurement decisions.

The University is a significant consumer of technology and as such, should seek to gain the best return on its technology investment for the organisation as a whole. This can be best achieved through reducing the total cost of ownership, in particular through centrally co-ordinated large-scale purchasing decisions, defining minimum standards and by ensuring an adequate and consistent standard operating environment for all levels of end-user computing activity.

IT Resources, through its Customer Service Charter, seeks to promote strategies and technologies which lower the TCO while increasing reliability and consistency. This is achieved through the provision of quality hardware at the best possible price, reliable internal operating systems and timely and accurate hardware support.

An up-to-date copy of this policy will be maintained on the University Web site at <http://www.utas.edu.au/policy/>

Purpose

The purpose of this policy is to establish the standards and guidelines for the procurement, installation and service of desktop and portable computers, and file servers.

Objectives

- That the hardware procured by the University is of high quality to maintain reliability and consistency, thus increasing productivity and lowering total cost of ownership (TCO¹).
- That the University achieves the best possible return on its significant investment in information technology.
- That the operating systems, applications and associated software are reliable and consistent, adhering wherever possible to a defined Standard Operating Environment (SOE).
- That data stored by end-users is secure and protected from tampering by non-authorised persons, misuse or theft.
- That the software component of the University's computer systems meets IT Resources statutory obligations with regard to usage and copyright.

¹ Total Cost of Ownership (TCO) is defined by Gartner Group Inc (USA) as follows: "TCO represents an holistic view of IT costs across the enterprise over time. The elements of cost used to achieve this holistic view are grouped into a series of direct and indirect cost elements".

- That IT Resources and other solution providers and purchasers have a clearly defined standard operating environment forming the basis for testing and certification of new and upgraded product releases.
- That the ongoing re-valuation of information technology assets are accurately reflected in the University's statement of accounts.

Scope

This policy covers all computer hardware, software and information that is stored in any form by or in electronic systems of the University.

This policy applies to all University desktop computer equipment² whether leased or purchased by IT Resources or by faculties, schools or departments.

This policy should be read in conjunction with the Desktop Computing Usage Policy, Web Usage Policy and associated documents, which can be found at <http://www.utas.edu.au/policy/>.

The current version of this policy will be maintained on the University Website under <http://www.utas.edu.au/policy/>.

Standards

This policy outlines seven Standards. The Standards reflect the base requirements and support levels for the provision of adequate client service for desktop computing for the University.

The seven Standards are:

- Hardware Provision (Purchasing & Leasing)
- Software Provision (Purchasing & Leasing)
- Hardware Service and Desktop Support
- Data Storage
- Data Backup and Recovery
- Hardware Security
- Hardware Lifecycle and Disposal

1. Hardware Provision (Purchasing & Leasing)

Hardware provision for the University should be of the highest order to ensure quality, consistency and reliability.

1.1. Hardware³ purchased or leased by a faculty, school or administrative office will meet or exceed the minimum system requirements as outlined in Schedule 1 – Hardware Benchmarks and Minimum Configuration. This schedule is maintained to reflect minimum benchmark hardware requirements as defined by Director IT and maintains IT Resources currency through changes in technology, system requirements or obsolescence. Up-to-date versions of Schedule 1 are maintained at <http://www.utas.edu.au/policy/>

1.2. In order to ensure adequate support for peripherals, standardisation wherever possible should be encouraged. Where additional or specialised hardware,

² Desktop Computer Equipment is defined as either

1. a personal computer (workstation, microcomputer, portable computer, notebook or laptop) or;
2. a file server used for storage of data directly related to desktop computing activities.

³ Hardware is defined as an item of computer equipment requiring an internal or external power source to operate. This includes desktop and laptop computers, RAM, monitors, scanners, CD-ROM and DVD-ROM drives, printers and related devices.

including external peripherals, is required on fully owned equipment the faculty, school or administrative office will endeavour to adhere to standards published by IT Resources except where there are reasonable operational or performance reasons to depart from such standards.

- 1.3. Where additional or specialised hardware, including external peripherals, is required on leased equipment the faculty, school or administrative office will provide the prescribed specifications to IT Resources for procurement and/or advice prior to purchase.

2. Software Provision (Purchasing & Leasing)

- 2.1. Audit requirements for full licensing of all software installed on local computers are necessary to ensure the University fulfils its statutory obligations in relation to copyright and software piracy laws. The organisational unit providing the equipment to end-users will take responsibility for all software installed on such equipment and will have auditable records of such software installations. Specifically, the OEM operating system licence must be present on each machine and cannot be transferred from another device.
- 2.2. Software⁴ installed on new computers either purchased by an individual faculty, school or administrative office or leased thereto through a lease agreement with IT Resources will endeavour to meet minimum requirements as outlined in Schedule 2 – Software Configurations. This schedule is maintained to reflect minimum benchmark system requirements at the discretion of Director IT, and will be regularly reviewed. Up-to-date versions of Schedule 2 are maintained at <http://www.utas.edu.au/policy/>
- 2.3. Where additional or specialised software is required on leased computer equipment, the faculty, school or administrative office will provide the specifications, including version number where appropriate to IT Resources for assessment of compatibility with current hardware and software prior to procurement to allow for testing of that package with the Standard Operating Environment (SOE).

3. Hardware Service and Desktop Management

Application software management of desktops is most efficiently managed through the deployment of specialist tools. All faculties, schools and administrative offices should endeavour to manage desktop software with such tools to ensure optimal efficiency and consistency. IT Resources employs such tools to monitor system performance and provides ongoing maintenance of on-line systems through software upgrades and diagnostics.

IT Resources maintains a Standard Operating Environment (SOE) which is specifically tailored to address the requirements of this Policy. The SOE is also designed to be flexible in order to encompass the varying needs of different organisational units. All faculties, schools and administrative offices should

⁴ Software is defined as magnetic or optically stored information utilised by a computer system for the interface between its hardware and other hardware or a human operator. This includes operating systems (UNIX, Windows 2000, NT etc) applications (MS Office, Netscape Navigator, FMIS etc) and 'drivers' for additional peripherals.

endeavour to adhere to the components of the SOE wherever feasible. The SOE is published in Schedule 3 – Standard Operating Environment and maintained on the web at <http://www.utas.edu.au/policy/>

4. Data Storage

- 4.1. IT Resources provides data storage facilities for the on-site preservation of data for central systems.
- 4.2. Organisational units are responsible for ensuring adequate data storage facilities are available for the storage of user data.
- 4.3. IT Resources stores additional data through lease-scheme and other contractual arrangements
- 4.4. End-users are responsible for storing data according to the instruction of the data storage facility's provider

5. Data Backup and Recovery

Data residing on University desktop computing systems represents a valuable resource for the University. It is therefore imperative this information is protected through appropriate backup procedures.

- 5.1. Backup schedules for critical data implemented by faculties, schools and administrative offices must adhere to the University's overall backup retention schedule to ensure protection of data. The University backup schedule requires daily, weekly and monthly copies of data to backup devices, with monthly backup being retained for two years. Faculties, schools and administrative offices must ensure retention periods for critical backups are equal to or longer than those documented in the Central Backup Retention Standard.
- 5.2. Non-critical data, which is nevertheless operationally valuable, should be backed up for at least one month. For this purpose it is acceptable to provide staff with the facility to undertake this backup themselves. Suitable solutions include (but are not restricted to) the following options:
 - 5.2.1. No local data storage, data stored on central file servers which are backed up to tape, or
 - 5.2.2. Centralised client backup of locally stored data via tape, eg Retrospect, ARCserve, or
 - 5.2.3. Local backup to removable media, eg: CD-RW, ZIP, floppy disk or similar.
- 5.3. IT Resources provides adequate central on-site and off-site backup facilities for central systems to minimise information loss due to infrastructure, data or end-user corruption, fire, theft or other physical means;
- 5.4. Backups of critical data will be undertaken in line with the Central Backup Retention Standard and stored in an off-site facility in line with the Desktop Computing Usage Policy; and
- 5.5. The recovery of files from backup will be undertaken in a timely manner to ensure minimal loss of business activity.

6. Hardware Security

- 6.1. The security of central file servers and central data storage systems remains the province of IT Resources.
- 6.2. Leasehold and purchased computer equipment must be secured against theft, fire and vandalism in accordance with university policy;
- 6.3. The central server room in IT Resources is environmentally and humidity controlled, requiring security access by authorised staff;
- 6.4. Departmental server rooms are to be kept in a well ventilated environment with access limited to authorised staff, at the discretion of the individual department. Climate control is recommended.
- 6.5. Asset Management Services are to be notified of any damage to, or theft of, hardware. Additional notification is to be sent to the hardware owner, and lessee department as appropriate.

7. Hardware Lifecycle and Disposal

- 7.1. There are three defined levels of hardware deployment, with appropriate support and maintenance levels. In all cases, the hardware must remain compliant with the current level of central system security, anti-virus software of the current standard, and must comply with current authentication parameters.

7.1.1. Primary Deployment

Primary deployment hardware is that which has a “life” of up to three (3) years after which time it is replaced. Such equipment is utilised in high use areas such as staff offices and student and teaching laboratories. They are typically covered by lease arrangements, full on-site warranty and associated support levels. Where the machine is three (3) years of age and re-deployment into secondary or tertiary deployment is not considered viable it is considered “end of life” and will be disposed of accordingly.

7.1.2. Secondary Deployment

Equipment in this rank are redeployed Primary Deployment machines which may, although unsuitable for their previous role, still be utilised in areas of low traffic for general purposes such as shared casual usage or spare workstations. This rank of equipment does not attract a level of support under which repairs are undertaken and maintenance is limited to minimal upgrades of software where considered viable, at the discretion of the provisioning area. When the unit is no longer fit for this purpose, or other secondary equipment of a higher order becomes available, it is deemed “end of life”.

7.1.3. Tertiary Deployment

This rank is comprised of redeployed Primary Deployment machines that retain a high level of reliability. This equipment is not subject to any support and is deployed in low traffic, single use areas such as Windows Terminal Services client or to manage database client software. When the unit is no longer fit for this purpose, or other tertiary equipment of a higher order becomes available, it is deemed “end of life”.

- 7.2. Non-compliant hardware over three years of age is deemed “end of life” and will not be considered for re-deployment.

- 7.3. Hardware redeployed into a secondary or tertiary role will be identified by a sticker or similar marking as “redeployed” and will be subject to reduced support levels as defined above.
- 7.4. Redeployed hardware may continue to use the operating system version that was current when that equipment was new, as it is generally impractical and uneconomic to upgrade older hardware to run newer operating system versions.
- 7.5. All hardware greater than five years of age is deemed “end of life”.
- 7.6. At the “end of life” of computer equipment, hardware is to be disposed of in accordance with the Asset Disposal Policy.

