



**UNIVERSITY OF TASMANIA**

---

**Desktop Computing Policy (Usage)**

**2004**

## Contents

Introduction.....	3
Purpose.....	3
Stakeholders and Responsibilities.....	3
Objectives .....	3
Scope.....	4
Definitions.....	4
Standards.....	4
1. Desktop Computing Service and Support Mechanisms.....	4
1.1. Central Support Services.....	5
1.2. Local Support Services .....	5
2. Desktop Computing End-Users Rights and Responsibilities.....	6
3. Desktop Computing Data and Information Management.....	7
Schedule 1 – Tiered Support Structure .....	8
Schedule 2 – ICT Responsibility Matrix	

## Introduction

The University is highly dependent on the efficient deployment and support of desktop computing technology and as such, seeks to maximise the value and usage of its technology investment across the organisation.

The University supports clear and consistent strategies and technologies, which lower the total cost of ownership (TCO) whilst increasing usability and consistency. This is achieved through timely and accurate end-user support through a structured support model. The model utilises the delivery and support of a Standard Operating Environment (SOE) based upon industry best practice models aimed at maximising efficiency and reliability whilst retaining the lowest possible TCO. The SOE is defined in the Desktop Computing Policy.

This policy supports the business imperatives as identified in University Strategic Plan strategies S34 and S38.

## Purpose

The purpose of this policy is to provide standards and guidelines for ensuring adequate and consistent support for all levels of end-user computing activity at the University. This includes the usage and security of desktop and portable computers and data, whether stored locally or on a fileserver.

## Stakeholders and Responsibilities

The following groups are stakeholders in the delivery of ICT systems and support:

- IT Resources (ITR)
- Flexible Education Unit (FEU)
- Library (Service Desk)
- Faculties and Divisions

Schedule 2 – ICT Responsibility Matrix contains a detailed breakdown of these groups and their respective responsibilities.

## Objectives

- That all end-users of University desktop computing resources are adequately supported in their day to day activities;
- That end-users of University desktop computing resources have an acceptable level of training in the use of such resources;
- That the University's productive effort is enhanced by the effective use of desktop computing technologies;
- That end-users have a clear guide to their rights and obligations in relation to provision of desktop computing services;
- That data correctly stored by end-users in accordance with relevant policies is secure and protected from non-authorised persons, misuse or theft; and
- That the software component of the University's computer systems meets statutory obligations with regard to usage and copyright.

## Scope

This policy applies to all users of University desktop computer equipment as part of their functions as staff or students of the University.

This policy should be read in conjunction with the Information Technology Facilities Use Guidelines, Desktop Computing Policy, Web Usage Policy and associated documents. Current versions of these documents 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/>.

## Definitions

For the purposes of this Policy, the following definitions are applied:

- **Desktop Computing** – all manner of end-user computing whether on a workstation, laptop, notebook, terminal or desktop computer, regardless of age, platform or operating system.
- **Licensed software** – software for which an unencumbered clear licence can be demonstrated, whether a University Site Licence, a University Licensing Agreement, departmental educational licence or an individual licence. Shareware licences must be paid within the period stipulated on the licence unless the licence is clearly stated to be free for educational purposes. Freeware licences are acceptable provided that they are installed in a manner that is in compliance with the licensing conditions. Every software installation must have a uniquely identifiable software licence.
- **Banned Software** – The University will publish a banned software list. This may be supplemented by Faculties, Schools and Sections (Organisational Units) banned software lists.
- **Central Storage Facility** – electronic data storage areas provided by IT Resources for use by students and/or staff, commonly referred to as “student home drives” or “eDirectory Group Drives”. Based on fault tolerant central servers with secure access from multiple locations based on end-users’ UTAS eDirectory credentials.

## Standards

This policy outlines three Standards. These Standards reflect the obligations and the expectations of end-users of University desktop computing facilities.

The three Standards are:

- Desktop Computing Service and Support Mechanisms
- Desktop Computing End-user Rights and Responsibilities
- Desktop Computing Data and Information Management

### 1. Desktop Computing Service and Support Mechanisms

University staff members require access to a high level of computer usage support for University activities in order to fulfil their duties as employees of the University. Students require access to a high level of computer usage support in order to facilitate their studies as clients of the University. Client support for desktop computing end-users is provided through local support personnel or via the central Service Desk.

The Service Desk, the Flexible Education Unit (FEU) and IT Resources provide Central Support. Central Support is comprised of three main elements, arranged in a tiered structure:

- Tier 1 support (entry point) - Telephone consulting and referral service according to respective Service Level Definitions via the Central Service Desk;
- Tier 2 support - Specialist support in the delivery of pedagogical services via flexible delivery, and high level support and training in associated technologies, such as Web usage via the Flexible Education Unit; and
- Tier 2/3 support - Remote support for specific central services such as network faults, central system support (eg FMIS, HRMS, email services etc), general access lab support, user authentication and desktop controls via IT Resources.

Usage of University Support services will be in accordance with the tiered structure model, with all requests being channelled through the Tier 1 Service Centre in accordance with Schedule 1 – Tiered Support Structure.

## **1.1. Central Support Services**

- 1.1.1. The University, through IT Resources, is responsible in the first instance for provision of all ICT infrastructure, including LAN, WAN and Internet connections.
- 1.1.2. University central services are normally available on a 99% availability basis during business hours. Outside business hours availability is reduced to 80% in order to allow routine maintenance. Regular maintenance schedules and live system status reports will be published on the web at <http://monitor.utas.edu.au/>
- 1.1.3. The University will ensure access to the Central Service Desk within advertised hours for all users of desktop and laptop computers.
- 1.1.4. Application software management will be undertaken in an efficient and consistent manner by support staff whether locally or centrally based in order to facilitate and enhance cross-functional support.
- 1.1.5. Students and staff may be allocated central server storage capabilities, dependent on hierarchical or procedural changes, at the discretion of Director IT Resources, or by negotiation with faculties or schools. Use of the central supported storage facility (eg Student Home Drives) provides for a high level of data integrity and security through the use of fault tolerant servers, backups and uninterruptible power supplies. Data will be backed up on tape every 24 hours and may subsequently be recovered in accordance with the Central Backup Standard.

## **1.2. Local Support Services**

- 1.2.1. Organisational Units are responsible for the adequate provision of Local Support at Tier 1 and Tier 2:
  - 1.2.1.1. Personnel employed by a faculty, school or administrative office for that purpose provide local support. Such personnel may be either directly employed or provided via contractual or lease arrangements with IT Resources or

other approved body. The support provided at this level includes:

- General user application support;
  - Support of specialist applications in general or mandatory usage within the organisational unit;
  - Training;
  - Software installations;
  - Basic hardware maintenance including warranty management;
  - Liaison with IT Resources;
  - Replacement/loan equipment; and
  - Maintenance of data backups and information security.
- 1.2.2. The Organisational Unit will ensure access is available to adequate local support staff within business hours for all users of desktop and laptop computers within that organisational unit.
  - 1.2.3. Organisational units will adopt the University SOE (Standard Operating Environment) in accordance with the Desktop Computing Policy (Procurement Installation and Service) in order to maximise the effectiveness and interoperability of central and local support efforts.
  - 1.2.4. (Organisational Units will ensure that all staff members and students have reasonable access to an operational computer that is compliant with minimum standards as defined in the Desktop Computing Policy (Procurement, Installation and Service).
  - 1.2.5. Application software management will be undertaken in an operationally efficient and consistent manner by support staff whether locally or centrally based in order to facilitate and enhance cross-functional support.
  - 1.2.6. Whilst provision of Local Support is in the first instance the responsibility of individual organisational units, some or all of this support may be arranged through IT Resources via contractual or lease arrangements.

## **2. Desktop Computing End-Users Rights and Responsibilities**

- 2.1. End-users covered by this policy include any individuals who are provided with access to the University LAN, via a direct or indirect connection method. Such connection methods could include but are not restricted to: University LAN connections (eg Ethernet); wireless network connections; remote access via a third party such as a contracted ISP with trusted access to the University LAN; or connection via VPN (Virtual Private Networking) technology.
- 2.2. Only licensed software may be installed on University computer equipment. End users will only connect equipment that has licensed software only installed upon it to the University network, either directly or indirectly.
- 2.3. Students and staff may be allocated central server storage capabilities, dependent on hierarchal or procedural changes, at the discretion of Director IT Resources, or by negotiation with faculties or schools. All end-users are responsible for the security of their own data if stored outside the supported storage facility.

- 2.4. End-users will ensure that their non-critical operational data is stored on a backed-up storage device, be it locally or centrally located, in line with procedures outlined by Director IT Resources.
- 2.5. End-users will be responsible for the management of all their own data in accordance with University and Organisational Unit guidelines if not stored on IT Resources or Faculty servers.

### **3. Desktop Computing Data and Information Management**

The University operates a central authentication service allowing same sign-on across desktop computers for all users. This service provides standard access for users, reducing duplication, and providing individual access for staff and students. Use of the system also provides for the portability of client access between machines across multiple locations within the University.

- 3.1. The University will provide staff and students with secure individual sign-on capabilities with minimal duplication for access to services used for teaching and learning, research and administrative activities. Organisational Units and administrative offices should ensure that staff and students use their secure individual sign-on capabilities to access desktop computers in accordance with approved procedures;
- 3.2. Users will not divulge their individual sign-on credentials to other staff, students or members of the public except for the purposes of problem resolution by authorised Organisational Unit or IT support personnel;
- 3.3. Users will comply with the Information Technology Facilities Use Guidelines; and with any succeeding guidelines;
- 3.4. The University will implement systems to ensure that systems and data are only accessed by those entitled and authorised to do so in order to protect copyright, intellectual property and privacy;
- 3.5. In order to ensure compliance with the Web Usage Policy, desktop systems will be required to implement appropriate access control. Furthermore, and apart from any other legal obligations, the University has a legal obligation under the Policy on Allowed Access to AARNET (Provision and Carriage Services) to ensure that AARNET is only accessed by AARNET members as defined in Clauses 1 and 2 of the abovementioned policy;
- 3.6. All desktop computers will have installed an approved anti-virus product, centrally supported and automatically updated from central mirror sites;
- 3.7. Desktop computers will be managed in such a way that security patches can be automatically and routinely applied, to hardware, operating system and standard applications. This will minimise disruption to end-users whilst ensuring that the University network protected from attack by malicious code, worms and viruses,
- 3.8. Users will, by default, have defined and restricted local access privileges. This limitation is required due to the risks inherent in granting full local access privileges which could enable malicious code, worms and viruses the ability to operate under the user's privileges and therefore compromise system and network security. Elevated local access privileges must only be granted for essential and specific purposes;
- 3.9. IT Resources provides adequate security of staff information through limiting of access to information by non-authorised users.

## Schedule 1 – Tiered Support Structure

In all cases, End-Users will initiate an incident call by first contacting the Central Service Desk.

The Service Desk is available by telephone on extension 1818 (03 6226 1818) or by email at: [helpdesk@postoffice.utas.edu.au](mailto:helpdesk@postoffice.utas.edu.au)

Up to date contact information will be published on the Web at <http://www.utas.edu.au/itr/help/>

### Tier One – Entry Point

Tier One is on-the-spot resolution of problems, or referral to an appropriate publication or other resource, or logging of a call for Tier Two or Tier Three handling.

As a guideline, Tier One matters are resolved by reference to standard published guides on IT and Library matters. Some explanation of the published guide may be necessary, particularly for students with low confidence in computing matters. Most queries should be resolved in a few minutes or less; few if any should take more than ten minutes. It must be recognized that it can be difficult at the outset for staff to estimate the time involved in dealing with a problem. Indeed, depending on circumstances, staff should be encouraged to exercise some discretion.

At Tier One, there will also be requests for services which are more complex, require professional skills, or which are likely to take more time. Such requests must first be qualified: is this a service which is available to this person, and if so is it available at Tier Two or Tier Three. If the request is qualified in those terms, then staff must obtain appropriate information to pass on. In the case of an on-the-spot referral, little or no information is required.

Where the referral is to be for Tier Three, then at the very least full client contact information is required, and beyond that, every reasonable effort should be made to enable Tier Three to take action. The client should not have to explain the problem all over again.

Basic Tier One tasks include:

- Monitoring Helpdesk and telephones, generating Service Requests via logging of incidents to the Service Desk system.
- PUPS account top-up, with payment by EFTPOS only. Limited account queries may also be possible.
- Password reset for student and staff email accounts - for cases where the account holder has forgotten the password. It is usual to require the account holder to be present in person with staff or student card to obtain this service.
- Provision of paper for printers in the libraries.

The role of the Tier One and Tier Two services provided under Library management is:-

- Understand/diagnose the incident or request. Allocate to Tier Two or Tier Three according to the level of complexity of the problem. Assign a priority to the incident.

- Qualify the incident/request: is it a matter that can be referred to another group as a Tier Three issue and if so which?
- Qualify the caller: is the person entitled under university policy to the service sought.
- Log all relevant details to the appropriate group.

## **Tier Two**

Tier Two deals with more complex or extended queries, requiring professional expertise.

Tier Two matters which are unlikely to be resolved within about ten minutes may be deferred, with an appointment or arrangement made to resolve the matter at an appropriate time when staff can schedule sufficient time.

At Tier Two, one of four things should happen within about ten minutes:

1. The customer's problem might be resolved, and that's the happiest ending.
2. The customer may be politely advised that no help is available, either because the problem is beyond the range of services provided by the university or because of the customer's entitlement or otherwise to the service. This will particularly arise in considering problems with computers other than those under the lease scheme.
3. The service can and will be provided at Tier Two, but the timeframe required is such that resolution must be deferred. In most such cases, there will be a resolution, but not an immediate one. Tier Two deferred resolution for student problems poses special difficulties. Students don't have offices or telephone extensions, and if a follow-up phone call is required that may not be practicable. Email may or may not suffice. The nature of student IT problems is such that Tier Two (deferred) should be relatively unusual, and there are grounds for generous interpretation of the ten-minute guideline with student customers.
4. The matter is referred to Tier Three.

## **Tier Three**

Tier Three problems or incidents are those which are provided by the university and in a centralised way, but not by the Library Service Desk.

Tier Three includes services provided by Computing and Distributed Systems, Communication Technologies and the Flexible Education Unit.

All problems handled by Tier Three should have been appropriately logged and escalated from Tier One, possibly via Tier Two.