



POLICY– No. 5
ICT ACCESS CONTROL POLICY

Relevant UTas Ordinance and/or Rule Reference No.	Ordinance 9. – Student Discipline. General Staff Agreement Academic Staff Agreement
Relevant State/Federal Govt. Legislation	Nil
Commencement Date	14/03/2006
Review Date	14/03/2008

Policy Statement

1 Intent

This document defines the policy, standards and responsibilities related to the security of the University of Tasmania's ICT facilities.

2 Scope

All Staff, Students and Associates of the University of Tasmania.

3 Objective(s)

The objectives of the ICT Access Control Policy are:

- a) To establish specific requirements for protecting the University of Tasmania's ICT Facilities against unauthorised access.
- b) To create an ICT infrastructure that will foster data sharing without sacrificing the security of the University's ICT facilities.

4 Definitions and Acronyms

Authorised ICT Staff	University of Tasmania staff authorised by the Faculty, Department, School, or Director of Information Technology Resources (ITR) to maintain and/or administer user level accounts and passwords on ICT Infrastructure facilities.
Authorised User(s)	An authorised user is an individual who has been granted access to ICT Infrastructure facilities under one or more of the following categories: <ul style="list-style-type: none">• A current member of the governing body of the

	<p>University</p> <ul style="list-style-type: none"> • A currently employed officer or employee of the University • A currently-enrolled student of the University • A contractor undertaking work for the University under the provisions of a legal contract • A member of a collaborative venture in which the University is a partner • A visiting lecturer, student or other associate who is undertaking similar activities in a recognised University, at the discretion of the Director IT Resources.
ICT Infrastructure	All information technology hardware, software, data, information, processes, systems, services, devices, procedures, environmental, and support facilities provided by the University of Tasmania.
ITR	Information Technology Resources
ITR ICT Security Officer	The ITR appointed representative responsible for security.
Staff, Student, or Associate	An Authorised User.
University	The University of Tasmania
University of Tasmania Network	Any University of Tasmania ICT network

5 Policy Maker

Director, Information Technology Resources

6. Policy Provisions

6.1. Location of ICT Infrastructure

ICT Infrastructure on campus must be located in lockable and/or appropriately monitored locations. Consideration must be given to the reliability of the electrical power supply, the need for air conditioning, potential contamination (e.g. from dust particles) and the likelihood of flooding and fire.

6.2. Cabling

Cabling must be kept secure by:

- a) concealing major cable routes; and
- b) keyed access to cabling locations except where devices such as workstations are designed to connect to the cabling systems.

6.3. Network Access

- a) Access to the University's ICT Facilities is limited to Authorised Users except where limited access is provided to the public. and must be secure at all times.
- b) Certain external addresses, namely those which are considered or known to send generally undesirable transmissions, are to be blocked from access to the University of Tasmania network.
- c) Where technically feasible, password protected inactivity time-outs shall be implemented, for terminals and workstations.
- d) The period of inactivity shall be no longer than 20 minutes in publicly accessible areas.
- e) All interfaces between the University of Tasmania and third party networks shall be secured according to the requirements of the Director, IT Resources.

6.4. Generic Accounts

- a) The use of shared, guest, anonymous and other such generic user accounts shall be avoided. Where used any guest or anonymous accounts must have minimum rights and privileges and be restricted to services containing unrestricted data, and not residing within a zone protected by a firewall or similar barrier.
- b) Generic access to information stored in databases is allowed only for non-interactive tasks. A non-interactive task is one that is scheduled to run automatically or one that is triggered by a series of events. A User does not directly initiate the task, nor is a User the direct recipient of the information. This includes automatic downloads and other linkages for data transfer.

6.5. Authentication

- a) Access to the University of Tasmania ICT infrastructure shall only be through authorised accounts which include a logon process that conforms to the ICT Facilities Password Policy.
- b) Authentication mechanisms that verify the identity of individual users or system interfaces must be implemented at all network, operating system and application software entry points.
- c) Authentication protocols and standards employed must meet the requirements of the Director, ITR or his nominees as determined from time to time.

6.6. Operating System Access Control

Security mechanisms at the operating system level shall be used to restrict access to computer resources. The mechanisms must be capable of:

- a) Identifying and verifying the identity and, if necessary, the terminal or location of each authorised user.
- b) Recording successful and failed system accesses.
- c) Providing appropriate means for authentication. If a password management system is used, it shall enforce the use of strong passwords.
- d) Where appropriate, restricting the connection times of users.

6.7. Application Systems

Security facilities shall be used to restrict access within application systems.

Logical access to software and information shall be restricted to Authorised Users. Application systems shall:

- a) Control user access to application system functions.
- b) Provide protection from unauthorised access by any software or device utility that is capable of overriding system or application access controls.
- c) Not compromise the security of other systems or applications.

6.8. Audit Logs

All applications and operating systems with a logging capability must generate audit logs capable of verifying application operation and the activities of users. Audit logs must only be made available to those individuals with the authority to view them.

7. Breaches

Breach of this policy will result in disciplinary action that may include sanctions, suspension, expulsion, termination of employment, legal action, or other disciplinary action.

Staff, Students and Associates learning of any violation of this policy must bring this matter to the attention of an appropriate staff member within the University without delay.

8. Supporting/Related Documents

ICT Facilities Use Policy.

9. Key Words

- Security
- Access
- Control

- Account

10. Supporting Procedures/ Guidelines

Nil.

Responsibilities

Implementation	Director, ITR.
Compliance	Director, ITR and ICT Staff.
Monitoring and Evaluation	ICT Security Officer and ICT Staff
Development and/or Review	Director, ITR and ICT Security Officer
Interpretation and Advice	ICT Security Officer

Who Needs to Know this Policy?

All Staff, Students and Associates of the University.

Effectiveness of this Policy

The effectiveness of this policy shall be established through regular audit.

Policy History

Policy No.	5, version 3
Approved / Rescinded	Approved by John Parry, Director, ITR
Date	14/03/2006
Endorsement	Pending
Committee / Board	
Resolution Number	