ICT Access Control Policy

Responsible Officer  Chief Information Officer

Approved by  Council

Approved and commenced  August, 2014

Review by  August, 2017

Relevant Legislation, Ordinance, Rule and/or Governance Level Principle

Broadcasting Services Act 1992 (Cmth)
Copyright Act 1968
Crimes Act 1914 (Cmth)
Personal Information Protection Act 2004 (Tas)
Telecommunications Act 1997
Ordinance 9 – Student Discipline

Responsible Organisational Unit  Information Technology Services

CONTENTS

1 Objective .................................................................................................................... 2
2 Scope ......................................................................................................................... 2
3 Policy Provisions ........................................................................................................ 2
3.1 Access to University ICT Services, Facilities and Infrastructure .......................... 2
3.2 Account Creation ...................................................................................................... 3
3.3 Account Deactivation ............................................................................................ 3
3.4 Account Privileges ................................................................................................. 4
3.5 Account Auditing ................................................................................................... 4
3.6 Account Security .................................................................................................... 4
3.7 Administrator Access Requirements ...................................................................... 4
3.7.1 Administrator Account Security ......................................................................... 4
3.7.2 Separation of Duties ......................................................................................... 5
3.8 Generic Accounts ................................................................................................... 5
3.9 Privacy .................................................................................................................... 5
3.10 Breaches ............................................................................................................... 5
4 Responsibilities ........................................................................................................ 6
5 Definitions and Acronyms ........................................................................................ 6
6 Supporting Documentation ....................................................................................... 10
7 Versioning ................................................................................................................ 10
1 Objective

The purpose of this document is to define who may access the ICT Services, Facilities and Infrastructure provided by the University of Tasmania, and to describe the logical and physical access conditions to those ICT Services, Facilities and Infrastructure items.

The objectives of the Access Control Policy are:

- to communicate the need for access control.
- to establish specific requirements for protecting against unauthorised access.
- to create an ICT infrastructure that will foster data sharing without sacrificing security ICT Infrastructure resources.

2 Scope

This policy applies to all University of Tasmania staff, students, contractors and associates.

3 Policy Provisions

The University of Tasmania provides ICT Services, Facilities and Infrastructure in support of teaching, learning, research and operational activities.

The University provides either public services or private services, which are available to Authorised Users only.

Public services include, but are not limited to, the University’s publicly available web site and the information contained on it and services offered by the University Library.

All other services are private services and are provided by the University of Tasmania for use by Authorised Users only.

Authorised Users are only eligible to hold an active account while their relationship with the University is current. At the cessation of their relationship with the University, they are no longer considered Authorised Users and their Access will be revoked.

3.1 Access to University ICT Services, Facilities and Infrastructure

Persons having any of the following relationships with the University are automatically afforded Authorised User status:

- a current member of the governing body of the University;
- a currently employed officer or employee of the University;
- a currently-enrolled student of the University.

In addition, any person falling under the following categories may apply for non-University Member status and receive authorisation from the Chief Information Officer, to use the University’s ICT Services, Facilities and Infrastructure and become recognised as an Authorised User:

- 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.

Non-University personnel may request access to University ICT Services, Facilities and Infrastructure using the online form located at the following URL:
https://secure001.utas.edu.au/cgi-bin/non_uni_members.pl

Information about the Request for Access to University Services process and stakeholder roles may be found at the following URL:
https://secure001.utas.edu.au/cgi-bin/non_uni_members.pl?task=nota_bene

3.2 Account Creation

Account creation occurs when a person becomes an Authorised User. This process indicates a person has a current relationship with the University of Tasmania.

Account creation will only occur when a person has been registered:

• as a current student, through enrolment;
• as a current staff member, through Human Resources processes; or
• has completed the Request for Access to University Services process and registered as a non-University member.

Account creation will not occur before a person is recognised as an Authorised User. Upon completion of entry processes of the University of Tasmania the account will become registered and active.

3.3 Account Deactivation

Account deactivation shall occur upon termination of an Authorised User’s relationship with the University of Tasmania. This may occur via, but is not limited to, the following events:

• Student:
  o graduation from a course of study;
  o failure to re-enrol during a course of study;
  o expulsion from the University.

• Staff:
  o termination of employment;
  o resignation;
  o retirement.

• Associate:
  o conclusion of contract or consultant services;
  o conclusion of collaborative research project;
  o termination of associate staff/study arrangements.
3.4 Account Privileges

Assignment of account privileges is based on the principal of least privilege. An Authorised User will be provided with access sufficient for their role at the University of Tasmania, and will not be afforded greater levels of access.

If an Authorised User’s role within the University changes, their access rights may also change to reflect the requirements of their new role.

3.5 Account Auditing

Periodic auditing of accounts will be performed by the University to identify and revoke non-active, unused or non-authorised accounts; or to perform the reallocation or revocation of privileges.

3.6 Account Security

Account details must be made secure as per the requirements of the User Password Procedure, which forms part of the ICT Security Framework of the University of Tasmania.

3.7 Administrator Access Requirements

Administration of ICT Services, Facilities and Infrastructure may only be carried out by:

- ICT Officers authorised by a Senior Officer of the University, or by a senior ICT Officer in a Division, Faculty, School, Centre, Institute or Section; or
- A person who holds responsibility, via their current position description, for the maintenance and management of data, or an ICT Service.

Administrators must be current members of the University or approved third party support persons. Administration rights, access and group membership held by an individual shall be immediately revoked upon cessation or suspension of employment with the University, change in role, or termination of contractual support arrangements with the University.

3.7.1 Administrator Account Security

Administrator Account details must be made secure as per the requirements of the ICT Systems Administrative Password Procedure, which forms part of the ICT Security Framework of the University of Tasmania.
3.7.2 Separation of Duties

Administrators of ICT Services, Facilities and Infrastructure shall not hold rights greater than those required of their role.

Separation of duties and responsibilities will be used to ensure no one person has the ability to circumvent normal auditing processes.

The minimum implementation will be to separate the roles of Systems Administrator and Application Manager for all systems holding confidential or financial information, or any system identified as a corporate system.

3.8 Generic Accounts

The use of shared, guest, anonymous and other such generic user accounts shall be avoided where possible. If guest or anonymous accounts must be used to access University of Tasmania ICT Services and Facilities they must be supported by a process that identifies the user of the account, such as a record of account allocation.

Wherever possible, generic accounts must have the minimum rights and privileges required to perform their role, and must not be used to access any corporate systems or stores of confidential information.

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.

3.9 Privacy

Information related to the use of University of Tasmania ICT Services and Facilities is collected and may be consulted to ensure compliance with University Policies, Procedures and Guidelines; and relevant State and Federal legislation. This information may be accessed for purposes of investigating allegations of misuse.

Information may be provided to law enforcement agencies where necessary to investigate or report suspected unlawful activity, as per University of Tasmania Privacy Policy.

3.10 Breaches

Breach of this Policy may result in disciplinary action as provided for under the applicable Employment Agreements and Ordinances.

Staff, students and associates learning of any violation of this Policy are obligated to bring this matter to the attention of an appropriate staff member within the University without delay.
4 Responsibilities

Chief Information Officer is responsible for:
- Implementation
- Compliance

ICT Security Manager is responsible for:
- Monitoring and evaluation

Chief Information Officer and ICT Security Manager is responsible for:
- Development and/or review

ICT Security Manager, together with the Legal Office is responsible for:
- Interpretation and advice.

5 Definitions and Acronyms

Access
Connection of University, personal or third party owned Devices to ICT Infrastructure facilities via a direct or indirect connection method. Such connection methods could include but are not restricted to:
- LAN/MAN/WAN network connections (e.g. Ethernet);
- Wireless network connections;
- Remote access via a third party such as a contracted ISP with trusted access to the University network;
- Connection via VPN (Virtual Private Networking) technology; and
- Connection to any systems, services and applications.

Account
A combination of a username (identifier) and password allocated by an ICT Officer to an Authorised User (the account owner) to access ICT Services, Facilities and Infrastructure.

Algorithm
A cipher used to encrypt and decrypt information using a series of steps that can be followed as a procedure.

Anti-Virus Software
A software package designed to identify and remove known or potential computer viruses, and associated software including but not limited to virus definition files.

Authorised User
An individual who has been granted access to University ICT Services under one or more of the following categories:
- A current member of the governing body of the University;
- A currently employed officer or employee of the University;
- A currently-enrolled student of the University;
- Any person granted access to use University of Tasmania ICT Services including, but not limited to:
  - 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; or
  - A visiting lecturer, student or other associate who is undertaking similar activities in a recognised University,
as a registered associate.

Copyright  
A form of intellectual property which gives the creator of an original work exclusive rights in relation to that work; and control over its distribution, publication, and adaption.

Data Custodian  
A nominated trustee of University of Tasmania data. A data custodian holds responsibility for protecting the data as defined by University of Tasmania Policies and Procedures.

Data Custodians may be nominated by their role with the University of Tasmania, or by their role in relation to a ICT Service. A Data Custodian will typically have responsibility for the management of a location of shared information, a database, or an application referencing a database distinct from the role of a systems administrator.

Data Custodians may include but are not restricted to:

- Application Managers
- Data Managers
- Business Systems Owners

Device  
Any computer or electronic device capable of accessing, storing and communicating data.

Encryption  
The process of transforming information using an algorithm to render it unreadable to those without special knowledge (access to a key).

End Host Device  
An electronic device which can be connected to a network via the allocation of a network address to that device’s MAC address such that this forms the only active network connection on that device. End Host Devices include, but are not limited to:

- Desktop computers;
- Notebook computers;
- Workstations;
- Servers;
- Network Printers;
- Telecommunications equipment;
- Wireless Devices; and
- Other network aware devices.

Facility Manager  
Staff member authorised and responsible for managing access to and use of an ICT Facility.

Gateways  
Gateways are ICT Services where Device connection has been authorised by the Chief Information Officer. Gateways are provided for the purpose of connecting privately owned Devices, and include:

- Uconnect wireless; and
- Wired connectivity in some study areas (e.g. Learning Hubs).
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>ICT Facilities</td>
<td>All computers, terminals, telephones, end host devices, licences, centrally managed data, computing laboratories, video conference rooms, and software owned or leased by the University.</td>
</tr>
<tr>
<td>ICT Infrastructure</td>
<td>All electronic communication devices, networks, data storage, hardware, and network connections to external resources such as AARNet and the Internet.</td>
</tr>
<tr>
<td>ICT Officer</td>
<td>The University of Tasmania staff authorised by the Faculty, School and/or Chief Information Officer to maintain and/or administer ICT Services, Facilities, Infrastructure, user level accounts and passwords.</td>
</tr>
<tr>
<td>ICT Security Manager</td>
<td>The ITS appointed representative responsible for ICT security.</td>
</tr>
<tr>
<td>ICT Services</td>
<td>All systems supporting interaction, information provision, information storage, or communications provision and the ICT Facilities on which they operate.</td>
</tr>
<tr>
<td>Internet</td>
<td>A term for the global computer network used to share information along multiple channels, and over multiple protocols. This definition of Internet is inclusive of protocol driven networks such as the World Wide Web, and all peer-to-peer networks.</td>
</tr>
<tr>
<td>ITS</td>
<td>Information Technology Services</td>
</tr>
<tr>
<td>Limited Personal Use</td>
<td>Infrequent, brief and legal use of ICT Facilities for personal, non-commercial purposes during personal time. Personal use activities must not cause offence to other users, or be reasonably considered to cause offence. Personal usage must not disrupt other users or prevent any person undertaking University related work from using ICT Services and Facilities.</td>
</tr>
<tr>
<td>Modifications</td>
<td>The disconnection, repair, or connection of devices and the installation or configuration of software or hardware.</td>
</tr>
<tr>
<td>Network Modification</td>
<td>Any change to the topology of the University of Tasmania network other than the addition of End Host Devices. Changes include, but are not limited to, the addition, reconfiguration or</td>
</tr>
</tbody>
</table>
removal of:

- Network Switches;
- HUBS;
- Routers;
- Any network aware device with more than 1 active network connection.

**Network Port**

Any individual switch port, wall outlet or wireless access port that provides connectivity to the University of Tasmania network.

**Port Splitter**

Any device attached to a network port that allows simultaneous access through that port. Devices include, but are not limited to:

- Switches;
- HUBS;
- Routers;
- Wireless Access Points;
- Active Multi-homed computers/devices;
- Modems; and
- Any network aware device with more than 1 active network connection.

**Request for Access to University Services**

A process provided by IT Resources to handle requests for access to University ICT Services, Facilities and Infrastructure by non-University personnel.

**Senior Officer**

- Vice-Chancellor
- Provost
- Deputy Vice-Chancellor (Research)
- Deputy Vice-Chancellor (Students and Education)
- Chief Operating Officer
- Senior Executive Director Business Development
- Pro Vice-Chancellor (Regional Development)
- Pro Vice-Chancellor (Global Engagement)
- Dean including the Dean of Graduate Research
- Director/Principal of University Institute
- Chair of Academic Senate
- Chief Financial Officer
- Chief Information Officer
- Executive Director
- Vice-Chancellor’s Chief of Staff

**Simultaneous Access**

Access through one port or wall outlet by more than one End Host Device

**University**

The University of Tasmania
6 Supporting Documentation

- Privacy Policy
- User Password Procedure
- ICT Systems Administrative Password Procedure
- External Access Procedure

7 Versioning

<table>
<thead>
<tr>
<th>Former Version(s)</th>
<th>ICT Access Control Policy; approved by Council May, 2010; reviewed May, 2014.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Version</td>
<td>ICT Access Control Policy (current document); minor amendments to update terms and references; approved by University Secretary, August, 2014.</td>
</tr>
</tbody>
</table>