ICT Security 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 (Cmth)
- Crimes Act 1914 (Cmth)
- Telecommunications Act 1997 (Cmth)
- Personal Information Protection Act 2004 (Tas)
- Ordinance 9 – Student Discipline

Responsible Organisational Unit: Information Technology Services

CONTENTS

1 Objective ................................................................................................................... 2
2 Scope ........................................................................................................................ 2
3 Policy Provisions ....................................................................................................... 2
  3.1 Access Control .......................................................................................................... 2
  3.1.1 Access to ICT Services and Facilities ........................................................................ 2
  3.1.2 Logical Access to ICT Services, Facilities and Infrastructure ..................................... 2
  3.1.3 Operating System Access Control ............................................................................. 3
  3.1.4 Application Systems .................................................................................................. 3
  3.1.5 Network Access ......................................................................................................... 3
  3.1.6 External Access to University Resources ................................................................... 4
  3.1.7 Physical Access to ICT Services, Facilities and Infrastructure ................................... 4
  3.1.8 Security of Information Assets ................................................................................... 4
  3.1.9 Data Archiving and Recovery .................................................................................... 4
  3.2 Monitoring of ICT Services, Facilities and Infrastructure ............................................ 4
  3.2.1 Usage of ICT Services, Facilities, and Infrastructure shall be Monitored .................... 5
  3.2.2 Monitoring of University Members .............................................................................. 5
  3.3 Development and Modification of Facilities and Services ......................................... 5
  3.3.1 Development of Services and Facilities ..................................................................... 5
  3.3.2 Modifications of ICT Services and Facilities and ICT Infrastructure ............................ 5
  3.4 Security Governance .................................................................................................  6
  3.4.1 Risk Management ...................................................................................................... 6
  3.4.2 Audit .......................................................................................................................... 6
  3.4.3 Business Continuity Planning .................................................................................... 7
  3.4.4 Disaster Recovery Planning........................................................................................ 7
  3.4.5 Incident Response Procedure .................................................................................... 7
  3.4.6 Security Incident Management Procedure ................................................................. 7
  3.5 Privacy....................................................................................................................... 8
  3.6 Breaches ................................................................................................................... 8
  4 Responsibilities ........................................................................................................ 8
  5 Definitions and Acronyms .......................................................................................... 8
  6 Supporting Documentation ...................................................................................... 13
  7 Versioning ............................................................................................................... 13
1 Objective

The purpose of this document is to set out the University of Tasmania's definition of, commitment to, and requirements for, ICT security. It specifies the security requirements of the University ICT Services and Facilities to ensure the availability and integrity of information assets and supporting infrastructure.

The objective of this Policy, and associated procedures are to:

- minimise the exposure of the University of Tasmania to risk
- ensure the security of ICT Services and Facilities, information assets and associated infrastructure
- provide direction and support for ICT security management.

2 Scope

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

3 Policy Provisions

It is University of Tasmania policy that the ICT Services, Facilities and Infrastructure it manages, inclusive of all electronic information, shall be appropriately secured against breaches of confidentiality and integrity of information or interruptions to the availability of the ICT Services, Facilities and Infrastructure.

3.1 Access Control

The University of Tasmania provides public and University ICT Services. Public ICT Services are considered to be those available to non-University personnel including, but not limited to, the University's publicly available web site and some services offered by the University Library.

University ICT Services include all ICT Services offered in support of learning, teaching and research, and operational business and all ICT Facilities and Infrastructure which support those ICT Services.

3.1.1 Access to ICT Services and Facilities

University ICT Services are considered to be those offered to University members in support of learning, teaching research and operational business. Access to these ICT Services, and supporting ICT Facilities and Infrastructure is restricted to Authorised Users only.

The conditions of access to University ICT Services for Authorised Users are defined in ICT Access Control Policy.

3.1.2 Logical Access to ICT Services, Facilities and Infrastructure

All access to University ICT Services and Facilities must incorporate appropriate authentication controls.
Authentication should, where possible, be provided using a unique username and password which is assigned to each Authorised User. Password details must be kept secret, and account details must not be shared.

All areas of the University of Tasmania will employ the account management processes described in the ICT Access Control Policy to manage user credentials for their full lifecycle.

Authentication methods must support minimum password standards, as defined in the User Password Procedure.

The use of generic accounts should be avoided wherever possible. Where generic access is necessary the use of such accounts must be in accordance with the provisions of the ICT Access Control Policy.

3.1.3 Operating System Access Control

Where technically feasible, password protected inactivity time-outs shall be implemented for terminals and workstations. The period of inactivity shall be no longer than twenty minutes in publicly accessible areas. Where a workstation is not publically accessible, inactivity time-outs may be extended beyond twenty minutes.

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

- identifying and verifying the identity and, if necessary, the terminal or location of each Authorised User
- recording successful and failed system accesses
- providing appropriate means for authentication. If a password management system is used, it shall enforce the use of strong passwords
- where appropriate, restricting the connection times of Users.

3.1.4 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:

- control user access to application system functions
- provide protection from unauthorised access by any software or device utility that is capable of overriding system or application access controls
- not compromise the security of other systems or applications.

3.1.5 Network Access

Access to the University’s ICT Services, Facilities and Infrastructure is limited to Authorised Users except where limited access is provided to the public.

Devices which are considered or known to send generally undesirable transmissions are to be blocked from access to the University of Tasmania network.
All interfaces between the University of Tasmania and third party networks shall be secured according to the requirements of the External Access Procedure.

All devices hosted on, or connected to, University of Tasmania ICT Services, Facilities, and Infrastructure must meet the minimum security requirements of this policy, and associated policies and procedures of the ICT Security Framework.

3.1.6 External Access to University Resources

The encryption of outbound communications must be commensurate with the level of classification of information that is being sent.

Inbound communications via the University of Tasmania’s website must be encrypted where those communications require user authentication.

Inbound connections to University of Tasmania internal ICT Services and Infrastructure (i.e. non-internet based resources) must be encrypted and use methods of communication approved by the Chief Information Officer.

3.1.7 Physical Access to ICT Services, Facilities and Infrastructure

Physical access to ICT Facilities is managed through the University’s security arrangements. Access to buildings and computing laboratories is at the discretion of the relevant Facility Administrator.

Hosting of ICT Facilities and Infrastructure on campus must be undertaken as per the provisions of the ICT Physical Security Procedure.

3.1.8 Security of Information Assets

Information assets within the University of Tasmania must have a nominated custodian. This Data Custodian will be responsible for implementing this policy in relation to the information assets for which they are accountable.

3.1.9 Data Archiving and Recovery

All University of Tasmania Corporate and Research data shall be archived as per the requirements of applicable State and Federal legislation and University of Tasmania policy.

3.2 Monitoring of ICT Services, Facilities and Infrastructure

The University of Tasmania provides members with access to ICT Services, Facilities and Infrastructure in support of teaching and learning, research activities, and in support of University business. These Services, Facilities and Infrastructure are provided on condition that members meet the requirements described in the ICT Security Framework.
In order to ensure compliance with University Policies, Procedures and Guidelines and relevant State and Federal legislation, the University of Tasmania may collect information related to the use of ICT Services, Facilities and Infrastructure.

3.2.1 Usage of ICT Services, Facilities, and Infrastructure shall be monitored

Information related to the usage of ICT Services, Facilities and Infrastructure may be consulted to investigate and ensure compliance with legislation and policies, or may be used for the purposes of: operations, maintenance, audit, quality of service, identifying inappropriate, excessive or unauthorised usage and for the purpose of litigation and criminal investigation.

System logs and audit trails from application systems, networks, and computer systems shall, where appropriate, be aggregated and filtered to assist in the identification of incidents.

To ensure the accuracy of and the ability to compare audit logs, procedures shall be in place to ensure all systems have synchronised clocks.

3.2.2 Monitoring of University Members

Monitoring of staff, students and associates shall be carried out only in accordance with appropriate legislation and Policies.

Organisational Units monitoring their own ICT communications shall do so within the requirements of University Policy, Federal and State Government legislation and regulations.

3.3 Development and Modification of Facilities and Services

ICT Services, Facilities and Infrastructure are controlled by the Senior Officer as defined in this policy. No changes may be made to any ICT Services, Facilities or Infrastructure without the approval of a Senior Officer or authorised ICT Officer.

Any authorised changes to ICT Services, Facilities and Infrastructure must meet the requirements set out in this policy and other relevant University of Tasmania policies.

3.3.1 Development of Services and Facilities

Development of new University of Tasmania ICT Services and Facilities must be approved by an appropriate Senior Officer.

3.3.2 Modifications of ICT Services and Facilities and ICT Infrastructure

Modifications to ICT Services and Facilities and ICT Infrastructure must be made by an authorised ICT Officer.

Infrastructure failing to meet these specifications may only be connected following approval from the Chief Information Officer.

The Division, College, Academic Unit or Section responsible for the development of, or modification to, any ICT Service, Facility or Infrastructure item should maintain
thorough documentation, including any changes made in modification to the ICT Service, Facility or Infrastructure item. The current status and configuration of any ICT Service, Facility or Infrastructure item should also be recorded.

3.4 Security Governance

The University of Tasmania ICT Security Framework provides guidance and control over ICT Services, Facilities and Infrastructure and defines the rights and responsibilities of University members in their use of ICT Services and Facilities.

The ICT Security Framework is subject to change, via a process of review and revision, to ensure ICT Security Risks are mitigated and that the Framework remains relevant to the strategic goals of the University.

Processes of Risk Assessment, Audit, and Incident Management and Response will provide input into the review and revision cycle, and the Framework will align with the Business Continuity processes of the University of Tasmania.

3.4.1 Risk Management

The University of Tasmania Risk Management Policy defines the processes adopted by the University in identifying, analysing, prioritising and treating risks.

The ICT Security Framework adopts the University’s processes and regular Risk Management activities will be undertaken.

Where the Risk Management process requires changes to be made to the ICT Security Framework, these changes will be performed as part of the review and revision cycle of the ICT Security Framework.

Risk assessment activities will occur:

- annually
- after a serious ICT Security incident that highlights vulnerabilities
- when cumulative updates indicate that the risk assessment requires a review
- when an event, or series of events indicate(s) that a review is required (i.e. these could include incidents, events elsewhere, changes to business operations etc.)
- where Infrastructure changes, such as technology and/or software upgrades;
- following a change in business requirements
- following a change in University Ordinances, Rules or Policies
- following a change in State or Federal legislation.

3.4.2 Audit

Audit of ICT Security controls and the ICT Security Framework will occur in line with the requirements of the University of Tasmania Audit and Risk Committee.

The Chief Information Officer may also request a full or partial audit of the ICT Security Framework at any time.
The results of any audit of the ICT Security Framework, or part thereof, may be used for review and revision, or may be used to assess compliance with the ICT Security Framework.

3.4.3 Business Continuity Planning

The ICT Security Framework will align with the Business Continuity Plans of the University of Tasmania.

The ICT Security Framework will meet the Business Continuity requirements by ensuring the application of appropriate security and availability controls on ICT Services, Facilities and Infrastructure.

3.4.4 Disaster Recovery Planning

All critical ICT Services covered under the ICT Security Framework will be supported by disaster recovery plans.

Disaster recovery plans for ICT Facilities and Infrastructure that support critical ICT Services will also be required under the ICT Security Framework.

Disaster recovery planning will be performed in conjunction with the University of Tasmania Business Continuity Planning processes, however it is also mandatory for any critical ICT Service, Facility or Infrastructure item not covered under that process.

3.4.5 Incident Response Procedure

The ICT Security Framework will align with the Critical Incident Response Procedures of the University of Tasmania and of IT Services.

The Framework will meet the ICT Security requirements of those processes, and will compliment and facilitate the action plans of those documents.

3.4.6 Security Incident Management Procedure

Security Incident Management Procedures will cover any breach of the ICT Security Framework.

Procedures may vary depending on the severity of the incident, but can include:

- evaluation of an incident
- classification of an incident
- investigation procedures
- escalation processes
- notification of appropriate people regarding the incident
- immediate mitigation processes
- review procedures regarding the incident itself, the wider risks involved, and effect on the ICT Security Framework.
3.5 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 the University of Tasmania Privacy Policy.

3.6 Breaches

Breach of this policy may result in disciplinary actions, 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

Chief Information Officer and ICT Security Manager is responsible for:

- Monitoring and evaluation
- Development and/or review

ICT Security Manager, together with the Legal Office is responsible for:

- Interpretation and advice.

5 Definitions and Acronyms

**Academic Unit**

Means the secondary organisational unit in the academic structure of the University, reporting directly to the College Executive Deans, as per Ordinance 14 – Academic Structure.

**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.

College
Means
(a) the primary organisational unit in the academic structure of the University, as per Ordinance 14 – Academic Structure
(b) the University College

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 an 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
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.

Executive Dean
Means:
(a) the Executive Dean of the relevant College, or
(b) in relation to the University College, the Principal of the University College

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).

Head of Academic Unit
Means the head of the relevant Academic Unit

ICT
Information and Communication Technologies

ICT Facilities
All computers, terminals, telephones, end host devices, licences, centrally managed data, computing laboratories, video conference rooms, and software owned or leased by the University.
| ICT Infrastructure | All electronic communication devices, networks, data storage, hardware, and network connections to external resources such as AARNet and the Internet. |
| ICT Officer | The University of Tasmania staff authorised by the College, Academic Unit, and/or Chief Information Officer to maintain and/or administer ICT Services, Facilities, Infrastructure, user level accounts and passwords. |
| ICT Security Manager | The ITS appointed representative responsible for ICT security. |
| ICT Services | All systems supporting interaction, information provision, information storage, or communications provision and the ICT Facilities on which they operate. |
| Internet | 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. |
| ITS | Information Technology Services |
| Limited Personal Use | 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. |
| Modifications | The disconnection, repair, or connection of devices and the installation or configuration of software or hardware. |
| Network Modification | 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 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 Services 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)
• Executive Dean
• Head of Academic Unit
• 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
- Data Backup and Restoration Procedure
- ICT Physical Security Procedure
- ICT Systems Documentation Procedure
- Secure Disposal of ICT Equipment Procedure

7 Versioning

|                  | Version 2 - ICT Security Policy; minor amendments to update terms and references; approved by University Secretary, August, 2014.  
|                  | Version 3 - ICT Security Policy; approved May 2014, minor amendments to incorporate the final academic structure. |

| Current Version | Version 4 - ICT Security Policy (current document); approved May 2014, amended in December 2017 to reflect academic structures and nomenclature. |