



POLICY– No. 2
User Level Password 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 details the minimum standards for user passwords required to support the continued confidentiality, integrity and availability of the University of Tasmania Information and Communications Technology (ICT) facilities.

2 Scope

This policy applies to all users of the University of Tasmania ICT Infrastructure who have or are responsible for an account (or any form of access that supports or requires a password) on any University ICT facility or any system that resides at any University of Tasmania location or stores any sensitive and/or non-public University of Tasmania information.

3 Objective(s)

The objectives of the Access Control Policy are:

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

4 Definitions and Acronyms

| | |
|--------|--|
| Access | Connection to ICT Facilities via a direct or indirect connection method. Such connection methods include, but are not limited to: <ul style="list-style-type: none">• LAN\MAN\WAN connections (For example Ethernet) |
|--------|--|

| | |
|--------------------------|--|
| | <ul style="list-style-type: none"> • Wireless network connections • Remote access via a third party such as a contracted ISP with trusted access to any University of Tasmania network • Connection via VPN (Virtual Private Network) • Connection to systems, services, and applications. |
| Account | A combination of a username and password used to access ICT Facilities. |
| Device | <p>Any electronic or electrical instrument which can be utilised to access, store or communicate data. Devices include, but are not limited to:</p> <ul style="list-style-type: none"> • Desktop computers • Notebook computers • Workstations • File servers • Video conferencing equipment • Telecommunications equipment • Removable storage devices (For example, ZIP, compact discs, USB devices) • Cameras • Mobile phones with 3G, WAP, Infrared, Bluetooth, or other such technologies • Personal Digital Assistants (PDAs) such as Palm Pilot and iPod. |
| Authorised IT 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 IT Infrastructure facilities. |
| ITR | Information Technology Resources. |
| ITR ICT Security Officer | The ITR appointed representative responsible for security. |
| IT Infrastructure | All information technology hardware, software, data, information, processes, systems, services, devices, procedures, environmental, and support facilities provided by the University of Tasmania. |
| Password | A secret series of characters that enables an Authorised User to access any IT Infrastructure facility. Normally paired with a Username and associated with an Account. |
| University | The University of Tasmania. |

| | |
|----------|---|
| User | <p>An individual who has been granted access to IT Infrastructure facilities under one or more of the following categories:</p> <ul style="list-style-type: none">• 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• 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. |
| Username | <p>Name used to identify an account. Normally associated with a password.</p> |

5 Policy Maker

Director, Information Technology Resources

6. Policy Provisions

6.1 All passwords are to be treated as sensitive and confidential and must not be divulged to any party other than the account user.

6.2 All passwords must be changed every 6 months. It is recommended that passwords be changed on a more frequent basis.

6.3 Where possible all user passwords must:

- Contain eight characters or more; and
- Contain characters from the following character classes:
 - Alphabetic (That is: a-z, A-Z)
 - Numeric (That is: 0-9)

User passwords must not be:

- Blank. That is no password;
- A derivative of the username;
- A derivative of the word password; or
- A derivative of any of the five previously used passwords.

6.4 Where an ICT Facility, system or service is unable to support the minimum password complexity requirements detailed in section 6.3, the strongest password that can be used within the restrictions of that particular facility, system or service shall be used.

- 6.5 The minimum password standards as detailed in section 6.3 must be automatically enforced by systems and applications where possible.

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. | 2, version 4 |
| Approved / Rescinded | Approved by John Parry, Director, ITR |
| Date | 14/03/2006 |
| Endorsement | Pending |
| Committee / Board | |
| Resolution Number | |