ICT Systems Administrative Password Procedure

CONTENTS

1 Objective ............................................................................................................................................. 2
2 Scope ................................................................................................................................................ 2
3 Procedure .......................................................................................................................................... 2
4 Definitions and Acronyms .................................................................................................................. 3
5 Supporting Documentation .................................................................................................................. 4
6 Versioning ......................................................................................................................................... 4
ICT Systems Administrative Password Procedure

1 Objective

This document details the minimum standards for system administrative passwords required to maintain the ICT Services, Facilities and Infrastructure of the University of Tasmania.

2 Scope

All staff, students and associates of the University of Tasmania.

3 Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Administrative Passwords for University of Tasmania ICT Services and Facilities are to be generated and managed by the ICT Officers responsible for ICT Service, Facility or Infrastructure management.</td>
<td>ICT Officers</td>
</tr>
<tr>
<td>2.</td>
<td>Administrative Passwords must be kept secret from any person who is not responsible for the management of an ICT Service, Facility or Infrastructure item.</td>
<td>ICT Officers</td>
</tr>
<tr>
<td>3.</td>
<td>All administrative passwords must meet the following minimum standard in construction:</td>
<td>ICT Officers</td>
</tr>
<tr>
<td></td>
<td>• Contain eight (8) characters or more; and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Contain characters from the following character classes:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o Alphabetic (that is: a-z, A-Z)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o Mixture of capitalised and lower case alphabetic characters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o Numeric (that is: 0-9)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o Special characters (characters such as: ?, %, $, *, @, #)</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Administrative passwords will have a maximum age of six (6) months and will be changed during the closest administrative windows each system has to January 10th and July 10th of every year.</td>
<td>ICT Officers</td>
</tr>
<tr>
<td>5.</td>
<td>Administrative passwords must not be used on multiple occasions, and where possible systems should monitor password history.</td>
<td>ICT Officers</td>
</tr>
<tr>
<td></td>
<td>Upon change of the administrative password, a new random password should be generated following the rules defined in this Procedure.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Administrative passwords must be kept in a secure, locked space, accessible only by members of the University who have been appointed to a systems administration role.</td>
<td>ICT Officers</td>
</tr>
</tbody>
</table>
Administrative passwords must not be stored, or left, in non-secure spaces.

7. Administrative passwords must be changed if the following events occur:
   - Breach of system, or administrative account, through external/internal attack, or compromised external connection;
   - Member of the systems administrator team leaves the University, or transfers to another Division or Section;
   - Unauthorised access to password storage space;
   - Improper storage, or handling, of administrative passwords;
   - Password ageing window is met.

4 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 (eg 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.

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
 ICT Systems Administrative Password Procedure

- A visiting lecturer, student or other associate who is undertaking similar activities in a recognised University, as a registered associate.

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 a College, Faculty, Institute, School 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.

ITS
- Information Technology Services

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

Username
- Name used to identify an account. Normally associated with a password.

5 Supporting Documentation
- ICT Security Policy
- ICT Services and Facilities Use Policy
- ICT Access Control Policy

6 Versioning

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Version</td>
<td>ICT Physical Security Procedure; minor amendments to update terms/references; approved by Responsible Officer,</td>
</tr>
<tr>
<td>Chief Information Officer, August, 2014. Amended in December 2016 to incorporate Colleges.</td>
<td></td>
</tr>
</tbody>
</table>