User Management Policy

1. Introduction

1.1. This Policy governs:
- 1.1.1. The creation, management and deletion of user accounts.
- 1.1.2. The granting and revocation of authorised privileges associated with a user-account.
- 1.1.3. The authentication (usually a secret password) by which the user establishes their right to use the account.

2. Scope

2.1. This policy applies to all accounts on computer systems directly connected to networks which are managed by the university. This includes operating system (Windows, Linux etc), and application software (Blackboard, database etc) accounts.

2.2. This document includes statements on:
- 2.2.1. Access Control
- 2.2.2. Managing Privileges
- 2.2.3. Authentication/Password Management

3. Access Control

3.1. The creation, deletion and changes of user accounts and privileges must be carried out by trained and authorised staff.

3.2. The person enacting any change in a user account must be different from the one authorising/requesting the change.

3.3. An unalterable log will be kept of all account creation/deletion/changes.

3.4. Account details will only be divulged to the user after proof of identity has been established.

3.5. A review period will be established, at an appropriate level for each system, which minimises information security risks yet allow the university's business activities to be carried out.

4. Managing Privileges

4.1. A user account should have the least privilege which is sufficient for the user to perform their role within the university.

4.2. Changes in the privilege of an account must be authorised by a nominated "owner" of the system to which the account affects.

4.3. Procedures shall be established to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the university.

4.4. Users' privilege rights will be periodically reviewed.

5. Authentication/Password Management

5.1. All users will have a unique identifier for any university system.

5.2. The user responsible for their account will keep the accounts authentication details secret and will not divulge it to any other person for any reason.

5.3. The account must not be used by the user where there is a possibility that the account details may be revealed.
5.4. Passwords can only be changed by the user or suitably trained and authorised staff.
5.5. If a user suspects their password is no longer secret it must be changed immediately and the system "owner" notified.

6. Document Approval

Approved by: Kathryn Arnold CIO
Approved Date: October 5th 2012
Review Date: October 5th 2013
Reviewer: IT Governance Manager

7. Document History

7.1. 9th September 2010 – Draft 1 Neil Faver
7.2. 15th September 2010 – Draft 2 Neil Faver
7.3. 3rd November 2010 – Draft 3 Document re-formatted Neil Faver
7.4. 21st February 2011 – Draft 4 Neil Faver
7.5. 4th April 2011 – Draft 5 Neil Faver
7.6. 4th April 2011 – Draft 6 Neil Faver
7.7. 13th June 2011 – Draft 7 Neil Faver
7.8. 5th October 2012 – Version 1 Neil Faver