1. Introduction

1.1. This information security policy document contains high-level descriptions of expectations and principles relating to how computer and application user accounts and privileges should be managed. This is a sub-document of Information Security Policy (ISP-S1).

1.1. User accounts and privileges must be managed correctly to ensure authorised user access to information systems is possible whilst preventing unauthorised access.

1.2. This document includes statements on:

- Scope
- Authorisation to manage user accounts and privileges
- Eligibility for accounts to use University IT facilities
- Management of user accounts and privileges
- Password management
- Expiry and deletion of user accounts on leaving

2. Scope

2.1. Login accounts and privileges must be managed in accordance with this policy for all computer systems and software applications used for University business or connected to University networks.

3. Authorisation to manage user accounts and privileges

3.1. Management of accounts and privileges on University computers and applications is to be restricted to authorised and suitably trained members of staff. Authorisation may be given, through line management, by the head of the department responsible for the management of the computer or application concerned.

3.2. Connection of privately owned computers to the wired network is only permitted in special circumstances with approval beforehand by both the Head of Department and a Network Authoriser. A condition of connecting a device to the wired network is that IT Services will be permitted to inspect its configuration. Where connection is permitted the designated system administrator of the device is responsible for ensuring that configuration and usage is in accordance with University Information Security Policy. This includes the management and usage of all login accounts and privileges on the device.

3.3. Specific staff are authorised to control login accounts and permissions for systems that IT Services manages. IT Services may delegate specific limited responsibilities for managing accounts and permissions to staff in other departments.

3.4. See also:

- Network Management Policy (ISP-S12)
4. Eligibility for accounts to use University IT facilities

4.1. Use of login accounts and privileges on University IT facilities, including permission to use University networks, may be authorised only for:

- Current University staff and students
- Students awaiting graduation
- Emeritus staff and those holding recognised honorary positions
- Those working closely with University staff on approved research or administrative projects.
- Staff in other organisations with which the University has a relevant formal agreement, e.g. for provision of computer system support.
- Visitors to the University, who may be granted temporary wireless access to the network by a member of staff with a CFS account

5. Management of user accounts and privileges

5.1. Those with responsibility for creating user accounts on University IT facilities must ensure that accounts are only created for individuals who are eligible to have an account and whose identity has been validated.

5.2. Before being provided with accounts, all users must be informed that compliance with University information security policy is a condition of using any University information system or handling University data.

5.3. Access to University IT resources must be authorised and a record maintained of such authorisations. For any computer, application or network account, it must be possible to determine:

- The identity of the person responsible for the account i.e. the user, or primary user in the case of shared accounts.
- The identity of the person responsible for managing the account and configuring its privileges. (This would typically be the administrator of the system, application or service to which the account provides access.)

5.4. Provision of privileged access to other organisations must be authorised by management and is subject to special controls. For further details see:

- Outsourcing and Third Party Access Policy (ISP-S4)

5.5. Computer user’s access to computer resources must be controlled and revised by system managers when circumstances change. This is to ensure that security risks are minimised and to allow University business to be carried out without undue hindrance. Specifically:

- Users’ access rights must be adjusted in a timely manner to provide only that access which is authorised and necessary. This should take place whenever there is a change in business need, staff change their role, or staff or students leave the University.
- The purpose and membership of all privileged groups and roles should be periodically reviewed.
- A periodic general review of login accounts should lead to removal of access to those accounts which are no longer eligible or required.
• Accounts to which authorised temporary access has been granted, e.g. by a password change, should be locked as soon as access is no longer needed.

5.6. Management of user privileges should wherever possible be based on group membership or role assignment, rather than by individual account. Except for systems or applications with a simple and self-documenting access control model, the purpose of each user group or role should be clearly defined and documented.

5.7. “Privileged accounts” are those with special computer system privileges that are needed by system administrators and which ordinary users do not need to use. System administrators must:

• Not provide ordinary users with privileges which could jeopardise the security of any other system users or their data.

• Not use privileged accounts themselves except when undertaking specific system administration tasks that require such privileges, i.e. they must use a normal account at other times.

5.8. See also “Accounts” section in:

• Use of Computers Policy (ISP-S9)

6. Password management

6.1. Once access to a system or application is authorised, the user is to be informed of their temporary password in a secure way. This temporary password must be changed immediately; this should be enforced automatically by the system where possible.

6.2. See also “Passwords” section in:

• Use of Computers Policy (ISP-S9)

7. Expiry and deletion of user accounts on leaving

7.1. University computer users will be notified by email that their University IT account will expire when they are due to leave the University.

7.2. Ninety days after the IT account has expired the IT account will be deleted. This includes all files associated with the account including emails.

7.3. Exceptionally and provided there is good reason for so doing, the ninety days period may be extended subject to approval by the relevant Head of Department or Head of Corporate Service, or by a member of the University Executive Board as appropriate.