Information Security Policy

Account Management and Password Policy

1 Introduction

1.1 The University's Information and Technology [IT] systems should only be available to authorised users. Access controls must be appropriate for the sensitivity of the information processed and maintained in a way that guards against unauthorised use. Privileged access to sensitive data or systems must be granted and revoked through a formal process.

1.2 Passwords are the principal authentication method for University IT systems. They must be sufficiently complex that they are not easily guessed or susceptible to dictionary attack and may in certain cases have additional requirements regarding history and expiry. Passwords must not be misused in ways that compromises the security or availability of IT systems.

2 Purpose

2.1 This policy defines user management and password requirements.

3 Scope

3.1 This policy applies to those responsible for the management of IT systems owned by or operated on behalf of the University and all IT users (such as staff, students, contractors, consultants, visitors and guests).

4 Access Controls

4.1 Access to University IT systems must be mediated by an authentication system that will centralise access controls and enforce consistent password standards. Where such authentication is inappropriate or impractical, manual procedures must be invoked that implement the controls listed below.

4.2 Passwords should be transmitted through encrypted channels when authenticating to University IT systems.

4.3 Personal accounts that give access to PCs, email, file systems etc. must be created and closed in accord with the IT Services User Management Procedures. These accounts must not be shared.

4.4 Group accounts may only be issued where suitable controls can be demonstrated; these must be used only for the specific purpose for which they were created.

4.5 Privileged access (for example to system management software or to sensitive data such as human resources information) must be granted to specified users via a formal authorisation process and must be revoked when a user ceases to have entitlement.

4.6 Access privileges must be segregated and set to the minimum level necessary for a particular requirement.

4.7 The use of system management accounts should be auditable to individual members of staff.

4.8 Sensitive systems may be subject to additional physical and logical access controls.

4.9 Access to accounts should be logged.

5 Password Controls

5.1 Controls on passwords will include length, complexity, history, and expiry. Details will be published in an Annex A to this policy and updated from time to time.

5.1.1 Administrator accounts (root, administrator etc.):

5.1.1.1 all password controls apply (length, complexity, history, and expiry);

5.1.1.2 logical access controls must be used to restrict access to a defined range of IP addresses.

5.1.2 Sensitive accounts (those with access via the central database to financial, personnel and other corporate information):

5.1.2.1 Length, complexity and expiry controls apply;

5.1.2.2 Password expiry must be informed by risk analysis.

5.1.3 Privileged accounts (those created with elevated capabilities for use by system or application administrators) and service accounts:

5.1.3.1 Length and complexity and expiry controls apply;

5.1.3.2 Password expiry must be informed by risk analysis.

5.1.4 Hard coded script accounts:

5.1.4.1 Length and complexity controls apply;

5.1.4.2 Script password change must be informed by risk analysis.

5.1.5 General user accounts:

5.1.5.1 Length and complexity controls apply.

5.2 Passwords must be kept secret and not shared with other users.

5.3 Users must not use their IT Services password on other systems.

5.4 Administrator passwords must be stored in a secure and accessible location as a requirement of business continuity.

6 Other Authentication mechanisms

6.1 In some circumstances, security risk analysis may require that access controls use other mechanisms such as challenge-response authentication.

7 Review

7.1 Access and password control standards will be reviewed annually by the Information Service Assurance Manager.

ANNEX A

Password Controls

The current central authentication system limits passwords to a maximum of 8 characters. Development effort is underway to allow longer passwords.

1. General user accounts: Passwords must be between six and eight characters in length. They should include upper and lower case letters and must include at least one non alpha character, from

   ! £ $) (% ^ & * # @ ? { } [ ] = + > < _ - ; : . ? 0 1 2 3 4 5 6 7 8 9

   Further guidance is available via IT Services FAQs.

   It is recommended that these passwords be changed at least every six months, although expiry will not be enforced.

2. Sensitive accounts: password expiry is informed by risk analysis. Passwords that grant access to financial and HR information via the central database must be changed every six months.

3. Accounts holders that have access to sensitive data or system management rights via a single reusable password must change their passwords quarterly.

4. Administrator, privileged and system accounts:

   4.1. On Windows systems these passwords must be at least 15 characters in length to force the use of the NT hash.

   4.2. UNIX root and system passwords must be at least 10 characters long.

   4.3. Administrator and root passwords should be changed when necessary, as informed through risk assessment, e.g. staff change roles or leave employment. They must be changed in a manner that will not expose risk through denial of access.

   4.4. Passwords should not be re-used.

   4.5. Windows systems support staff should be issued with individual secondary accounts with appropriate privileges for their role and these must be used instead of the administrator account whenever possible.

   4.6. UNIX systems support staff should use su or sudo from their personal accounts to provide an audit trail. Login via the root account should be used only if essential.

Ownership:

Owner	Department/Team
Director ITS	ITS

Authors:

Author(s)	Department/Team
Jeremy Maris	Client Services

Contributors and Reviewers:

Contributor/Reviewer	Department/Team
Matthew Trump	Information Service Assurance Manager

Revision History:

Version Number	Status D/R/A/I[1]	Date Issued	Reason for Issue	Issued by
1.0	D			
1.1	I	14/05/09	Approved ISC	Jeremy Maris
1.2	I	05/04/13	Minor update	Jeremy Maris
1.3	I	01/06/15	Reformatted. Add policy control page and information.	SR
1.4	I	20 June 2017	Minor Amendments	MT

[1] D = Draft; R= Ready for approval; A = Approved for issue; I = Issued