Password Usage and Management Policy

Version Control

Version	Date
Draft 0.1	20/09/2017
1.0	01/11/2017

Related Polices

- Information Services Acceptable Use Policy
- Associate Accounts Policy
- Data Storage and Remote Working Policy
- IT Security for 3rd Parties, Suppliers and Support Organisations Policy
- Access Control Policy

1. Introduction

1.1. Background

Although technical and procedural controls are applied throughout the University's IT infrastructure to protect facilities and data from unauthorised access, provision has to be made for legitimate users to access data relevant to their normal University activities where and when they need it.

Before a user can access University systems and data, a process of authentication is carried out which validates the access that a user is requesting against the permissions that individual has been granted. Key to this process is the User ID and password, which effectively presents their 'electronic identity'.

In order to provide accountability and to prevent misuse and abuse of their 'electronic identity' by others, it is crucial that passwords are both strong and managed diligently. The importance of this requirement cannot be overstated as the University moves towards 'Single Sign-On' (SSO) where the authentication process of user names and passwords will provide access to multiple systems and data to which account holders have been granted privileges.

This document which forms the University's *Password Usage and Management Policy*, defines the password controls that are designed to protect users, systems and data.

Applicability

This policy applies to the following:

- All full-time, part-time and temporary staff employed by, or working for or on behalf of the University;
- Registered students of the University;
- Contractors and consultants working for or on behalf of the University;
- All other individuals and groups who have been granted access to the University's IT facilities, including visitors.

It is the personal responsibility of each person to whom this Policy applies to adhere fully with its requirements. However, line managers are responsible for implementing this Policy within their respective department and for overseeing compliance by those under their direction or supervision.

Related Policies

- Information Services Acceptable Usage Policy
- Access Control Policy

1.3. Scope

This Policy concerns all computer systems operated by the University, regardless of location, where responsibility for user management and control resides with members of the University.

2. Password Usage and Management

2.1. Secrecy & Divulgence of Passwords

Individuals are personally responsible for maintaining the secrecy of their passwords and for controlling access to their user accounts through password security.

Passwords are not to be divulged by users to anyone including IT Services support personnel, secretaries or PAs.

2.2. Password Complexity and Choice

2.2.1 Password Complexity

The University will configure its systems to enforce password complexity and users are required to choose strong passwords.

2.2.2 Password Choice

Users are required to choose sensible strong passwords at all times in order to protect their 'electronic identity', prevent unauthorised access to systems and preserve the availability and integrity of data.

Guidelines for choosing strong passwords can be found in the Appendix. All passwords used have to be unique i.e. you are not allowed to recycle passwords.

2.3. Password Aging and Forced Password Change

2.3.1 Forced Password Change

Corporate Systems administrators who operate their own systems (where **any** system or data access can be given independent of Active Directory) are required to implement a process to force-change the password of newly created accounts at first log-on, where this is technically possible.

2.3.2 Password Aging and Reuse

The University will not implement password aging, except in respect of those passwords that provide access to certain privileged access. However, where password aging is enforced for such access, system-forced changes will occur at least every 90 days.

2.4. Unforced Password Change

2.4.1 Users at Initial Logon

Users of systems that cannot be configured to force-change their initial default passwords at first logon are required to change them themselves at the first logon.

2.4.2 Default Passwords

Corporate System administrators and IT Services support staff who configure new systems and set up services are to ensure that all password settings are changed from their default settings before moving platforms into production.

This is particularly important in the case of databases that use standard default passwords. These must not be used and default passwords must be changed as soon as possible after a new system is acquired, or after any database or operating system upgrades that re-instate default accounts and passwords.

Peripherals with embedded software, such as printers and network equipment, often have default or null passwords which must be reset.

2.4.3 System-Level Passwords

All system-level passwords (e.g. operating system or application administration accounts, etc.) must be changed on at least an annual basis. However, where it is where practical changes

should be implemented monthly.

2.4.4 User Passwords

Passwords must be changed immediately on any occasion that a user believes that someone else may be aware of their password and on all occasions when a malpractice incident is discovered or suspected.

2.5. Systems-Level (Administrator and Super-User) Passwords

Staff may only have access to system-level passwords on a need to know operational basis, not because they may possibility need them at some time.

Shared administrator and super-user (global) passwords are not to be used on production systems except where passwords are hard-coded into applications.

Administrators and IT support staff are to be allocated secondary accounts which have the appropriate rights and privileges to enable them to support the systems and services for which they have a responsibility.

2.6. Shared Password

Passwords are not to be shared by users, except in the case of administrators and IT Services support staff who are responsible for the maintenance of systems and services that utilise hard-coded passwords.

Where there is a need for several users to have access to common data and mail boxes, such as those working collaboratively, access must be controlled in accordance with the *Access Control and Account Management Policy*.

2.7. Password Resets

2.7.1 Staff Passwords

The identity and association of a person with a particular account must be verified by administrators prior to resetting their password.

Passwords must generally only be reset when the person requesting a reset has been properly identified and verified against held documentation as being the account holder.

Passwords must not be reset on the basis of any other third-party request, regardless of the status of the individual making the request.

However, IT Services support staff may request a reset of a user's password in order to identify or fix a fault, and line managers can request a user's password to be reset when it is necessary to migrate services in the user's absence. In both cases, the user is to be informed of the new password at the first opportunity by the person who has requested the reset, and is to change this at the next logon.

2.7.2 Student Passwords

To reset their password, students will need to answer a selection of the questions using data from their student record held in the Student Administration System. All students' passwords must:

- comprise a minimum of seven characters;
- contain characters from three of the four following categories:

- English uppercase A-Z
- English lowercase a-z
- Digits 0-9
- Special Characters: eg, !,$,#,%

- not have been used before.

2.8. Help and Assistance

Any questions regarding the use and management of passwords should be directed to the IT Services Help Desk.

3. Annex

3.1. Selecting a Strong Password

1. When you choose a password, you should make it personally memorable but difficult for others to guess:

- Make sure that your password comprises at least 7 characters including special characters and numbers;
- Choose one that is easily remembered;
- Never write your password down;
- Immediately change your password if you think that it has been revealed to anyone else or compromised;
- Never use your user name in any form as your password;
- Never use your surname or given name in any form;
- Don't use any information about you that is easily obtainable, such as your car registration number, your birthday, your child or pets name, your favourite holiday destination or your favourite sports team or hobby;
- Don't use word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.;
- Avoid the use of an ordinary word preceded or followed by a digit (e.g., secret1, 1secret);
- Don't change your password by simply adding a number every time you have to change it;
- Don't reuse or recycle your password;
- Don't share your passwords with anyone, including administrative assistants or secretaries or tutors;
- Never use the same password for both your university and private computer accounts, such as on-line banking, Facebook etc.;
- Don't use the 'Remember Password' feature of applications.

If someone demands a password, refer them to this Policy or have them contact the IT Services Helpdesk.

2. In addition, make sure that your password is:

- Private - it is used and known by you only – you wouldn't like it if your identity was stolen, so why give it away?
- Not shared, even with your secretary or PA – if you have a secretary or PA who has a need to access your data, this can be facilitated through file permissions for both Exchange and File Store;
- Secret - it does not appear in clear text in any file or program in any medium.

3. Use one of the following methods to create a memorable but strong password:

- Use the first letter of each word in a memorable phrase, saying, nursery rhyme or song title. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. Please do not use this example.
- Substitute one or more letters with a numeric character (e.g. I = 1, A = 4, S = 5, L = 7 or O
  = 0);
- Take two words and splice them together with one or more non-alphanumeric characters, or;
- Take an ordinary word or phrase and change, delete or add characters so that it becomes nonsensical.

3.2. Protecting Your Passwords

All individuals' usernames issued at the University are unique and are not reused. Although usernames are not secret, they should be treated as personal. Details are not published and they should not be divulged to others.

Remember that a computer that is left unattended and logged in gives anyone access to information accessible to the authorised user. If a computer is left unattended, it should be shut down or locked.