Password Policy v1.0

Organisation	Oxford Brookes University
Title	Password Policy
Creator	Gareth Packham - Head of Information Management
Approvals Required	1. Information Security Working Group 2. CIO 3. Executive Board
Version	Version 1.0
Owner	Chief Information Officer
Subject	The formal, approved, Password Policy of Oxford Brookes University
Review date and responsibility	Annually by Head of Information Management

Revision History			
Date	Author	Version Number	Comments
20/09/16	Gareth Packham	0.1 (draft)	Original draft
14/09/16	Gareth Packham	0.2 (draft)	Minor revisions only
28/09/16	Benedict Barry	0.3 (draft)	Minor revisions only
20/03/17	Gareth Packham	1.0 (live)	Minor revisions only

1 Introduction and Policy Objectives

1.1 The purpose of this Password Policy is to protect Oxford Brookes University (OBU) information assets from unauthorized use, and possible accidental or intentional misuse, through weak password security practice.

1.2 The policy applies to all users (students, staff, consultants, contractors and visitors) who have been given access to OBU information and communication systems or who are using third-party systems or services which have been contracted for by OBU.

1.3 On joining OBU staff shall be required as part of their terms and conditions that they will keep all personal secret authentication information private and keep any group secret authentication information solely within the members of the group.

2 Password Creation

2.1 All user-level and system-level passwords must conform to current best practice guidelines (so called, ‘strong’ passwords). For further information please contact the IT Service Desk, however in general ‘strong’ passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g. 0-9, -_.!~*()
- Are at least twelve alphanumeric characters long
- Are not based on personal information, names of family, etc.

2.2 Users must not use the same password for OBU accounts as they do for personal / non-OBU accounts.

2.3 Where possible, users must not use the same password for different accounts.

2.4 User accounts that have system-level privileges granted through group memberships, or programs such as Sudo, must have a different password from all other accounts held by that user to access system-level privileges.

3 Password Change

3.1 Users must abide by local or application-specific guidelines on the frequency of password changes. Changing passwords in itself is not a guarantee of security.

4. Password Protection

4.1 Passwords must not be shared with anyone (including other OBU staff). All passwords are to be treated as sensitive and confidential OBU information.

4.2 Do not write passwords down and store them in your office or place of work. Do not store passwords in a computer file unless the file itself is encrypted.

4.3 The use of 'remember my password' in applications (e.g. browsers) is not recommended for OBU passwords.

4.4 Any user that suspects their password may have been compromised must change it and inform the IT Service Desk immediately.

4.5 The use of password manager (also known as password vault) applications is permitted. For further information please contact the IT Service Desk.

5. Multi-Factor Authentication

5.1 It is recommended that users enable multi-factor authentication functionality on all system accounts where available

6. Application Development

6.1 Application developers must ensure that their programs contain the following security precautions:

- Applications must support authentication of individual users, not groups
- Applications must not store passwords in a reversible form and use PBKDF2 where possible.
- All password hashes must be salted.
- Applications must not transmit passwords in cleartext over the OBU network.