BUCKINGHAMSHIRE
NEW UNIVERSITY
EST. 1891

PASSWORD POLICY

bucks.ac.uk

Contents

Approved by: **ITSC**
Version No. **3.0**
Owner: **IS&T**

Date first published: **Feb-2015**
Date updated: **May-2019**
Review Date: **Apr-2021**

Introduction

1 Passwords are an important aspect of computer security and are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Bucks New University's entire network.

2 All users of IT facilities provided by Bucks New University including students, staff, partners, contractors and third parties must comply with this password policy to protect the security of the university network and to protect the integrity and confidentiality of data.

Policy Scope

3 This policy applies to all University students, staff, partners, contractors as well as staff working for 3rd party agents at the behest of the University, who require access to systems that are protected by a username and password.

Policy Intent

4 The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Policy

5 Passwords must be kept confidential. Do not share your password with anyone, including IS&T. All passwords are to be treated as sensitive, confidential Bucks New University information.

6 Passwords must not be written down anywhere that other people might be able to see or discover them or stored in a file on ANY computer system (including phones or similar devices whether they are University or personally owned) without encryption. Contact the IT Service Desk if you require advice on the safe storage of passwords.

7 Passwords must be strong and meet the following requirements:

- Be a minimum of 8 characters long, preferably 15.
- Contain a mixture of upper and lower-case letters.
- Chosen entirely at random, with no connection to you or the University.
- Not based on a single dictionary word.
- Does not include your name or username.

See point 17 for additional guidance on creating strong passwords

8 When you are first issued with an account you wil be given a temporary password which you must change as soon as possible to a strong password known only to you. You are responsible for any activity that is carried out using your account.

9 To change your password, you should first register for self-service password reset by following the link on the IT web pages (bucks.ac.uk/it). Once registered you will be able to reset your password at any time.

10 You are required to change your password every 12 months however if you believe your password has been compromised or made available to others, you must immediately change it and notify the IT Service Desk.

11 You will receive regular reminders to change your password before the expiry date. When your password expires you will lose access to IT systems and services.

12 After five consecutive failed attempts to log in your account will be locked for 15 minutes.

13 Do not use the same password for Bucks New University accounts as for other non- University access (e.g., personal e-mail, on-line banking, and social media).

14 IS&T staff will never ask for full details of your password. IS&T staff are not permitted to remotely change your password for you instead you must use the self-service password reset facility.

15 Passwords must not be inserted into e-mail messages or other forms of electronic communication and must not be stored or transmitted in clear text (unencrypted).

16 Some University systems may have additional password requirements, depending on the type of system, regulatory or contractual requirements, or the type of data they process. Follow the password guidance given by the administrators of those systems.

Guidance on creating a strong password

17 To help create a password choose three random words and put them together for example;

greenbearjam or trainersroofwater

To make the password even stronger mix upper and lowers case and combine the words using a number or a punctuation mark for example;

Green1Bear-Jam or trainers.ROOF.water

Choose three words that are memorable to you but cannot be easily guessed such as 'onetwothree' or are the names of family members or pets.

18 Remember:

- Do not reveal a password over the phone to ANYONE.
- Do not select ‘yes’ when applications ask you if you want them to remember your password
- Do not reveal a password in an email message.
- Do not reveal a password to your line manager.
- Do not talk about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.
- Do not share a password with family members.
- Do not reveal a password to colleagues while on holiday.
- Be careful when using social media so that you don’t compromise your password

Enforcement

19 Failure to comply with this policy may result in disciplinary action in accordance with the relevant process.

Key Relevant Documents

Information Security Policy

Acceptable Use Policy

Revision History

Version	Status	Name	Reason for change	Date
3.0	Draft	JH	Updated document	24 May 19
3.0	Final	JH	Published	Jun 19