Policy Reference: P0010
Classification: Public

BIRMINGHAM CITY
University

Student Password Policy

1. Summary

The purpose of this policy is to manage student network accounts and the password credentials used to gain access to University systems and networks. This is designed to minimise the risk of loss, unauthorised disclosure, or modification of University information accessed whilst students use these accounts.

Various sources of reference have been utilised in the preparation of this policy to ensure it addresses modern security approaches. Consideration has been given to the UK National Cyber Security Centre (NCSC) recommendations, security industry best practices and approaches by the Higher Education community.

The University protects user accounts with Multi Factor Authentication (MFA).

2. Introduction

This policy covers:

a) The management of University student network accounts.

b) The password complexity standard for University student network accounts.

c) MFA requirements for student network accounts.

3. Scope

This policy applies to student accounts used to gain access to Birmingham City University systems and networks.

Supplementary guidance for protecting your IT credentials is provided in the document Guidance notes for use of Computer Systems and Networks at BCU.

4. Management of Student Accounts & Passwords

a) All network accounts must be carefully safeguarded by their owners who are fully accountable for their use, as detailed in the Policy for Use of Computer Systems and Networks at Birmingham City University.

b) Students must not share their University account credentials with other users, including other students, staff or visitors. Failure by students to safeguard their account credentials will be deemed as an act of negligence and may be subject to disciplinary proceedings.

c) Students must lock or logout of their workstation, laptop, or other University provided device when not in use to prevent misuse of their account by others, e.g. when leaving their desk or device unattended.

d) Network accounts will be disabled automatically 24 months following the date when a student graduates from their University course

e) Network accounts may be disabled without prior notice due to exceptional circumstances e.g. disciplinary proceedings or a known compromise of the account.

f) Students must immediately report any suspicion of their network account and password credentials being compromised/misused by another user to the IT Help Desk via ithelp@bcu.ac.uk or 0121 331 6543.

g) Student passwords will not expire. Students whose accounts are enrolled in MFA can reset their own passwords through the Microsoft Password self-service portal. Additionally, student passwords can be reset by the IT Helpdesk upon request IF the student has reason to believe that their account has become compromised.

h) As part of our ongoing commitment to IT Security at BCU we will use industry standard tools to assess the strength of your password. If your chosen password is found to be too weak, in a compromised list, or, we notice suspicious account activity, we will require you to choose a new password.

5. Student Password Requirements

1. Passwords should not contain the username of the student network account.

2. Student passwords must meet the following minimum length:

   a) Be at least 8 characters in length.

3. Student passwords must contain characters from at least three of the following categories:

   a) Uppercase letters (A-Z)

   b) Lowercase letters (a-z)

   c) Numbers (i.e. 0-9)

   d) Special characters (i.e. !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

4. Some specific common keywords – such the word “password” may be blacklisted, students may not be able to set passwords that contain these words.

5. Password management:

   a) Password History: Last 24 passwords will be retained, to ensure they can’t be immediately reused.

   b) Minimum Password Age: Set to 2 days before a password can be changed, ensuring previous password usage can’t be undertaken by cycling through the password history defined in a) above.

   Exceptions to the standard set out in a) and b) above include where an account is believed to have been compromised. Under such circumstances the IT Help Desk must be immediately notified to change the password.

   c) Maximum Password Age: The student password will not expire. A reduced password age of 180 days may be enforced on a risk assessed approach for students accessing systems containing sensitive information e.g. as part of a research or dissertation project.

6. MFA

Historically, University systems and data sources have been protected simply by passwords. However, as computing power has increased the time required to ‘crack’ passwords and break encryption has greatly reduced. This means that successful attacks on previously secure systems are now becoming commonplace putting University data and infrastructure at risk.

Multi-Factor Authentication (MFA) is an industry standard solution to tackle this issue. MFA combines two or more independent factors to access secure systems and information,

For BCU students the first factor is their account password.
The second factor is typically provided by something in the student’s possession – such as a trusted mobile phone. A typical example of second factor authentication could be a passcode texted to a registered phone number, or, a simple confirmation touch within an App on a registered smartphone.

All BCU student network accounts will be subject to MFA enrolment this applies to all electronic devices used to access BCU resources

7. Exceptions

There are no policy exceptions, any queries related to the policy may be forwarded to the IT Security Manager at itsecurityhelp@bcu.ac.uk

8. Policy Review

This policy will be reviewed on an annual basis, or if there is a change in legal or other business related requirement.

Review Date	Description	Reviewer
03/08/2021	Students Password Policy	IT Security Manager

Document History

Version	Date	Description	Authors
0.1 draft	13/04/2017	First draft for discussion: v0.1 (draft)	IT Security Manager
0.2 draft	15/04/2017	Internal peer review	IT Security Manager
1.0	20/04/2017	Policy approved and ratified, by Information Governance Board (IGB)	Information Governance Board (IGB) approval
1.0	16/04/2018	Policy Reviewed – No Changes	IT Security Manager
1.0	08/04/2019	Policy Reviewed – No Changes	IT Security Manager
1.1	03/08/2020	Policy Updated – Added MFA section.	IT Security Manager
1.1	09/08/2020	Policy Reviewed – further clarifications	Head of Business Continuity
1.1	10/08/2020	Policy Updated – changes as per feedback	IT Security Manager
1.2	19/08/2020	Policy updated to provide further clarity about MFA process	Associate IT Operations Director
2.0	27/08/2020	Policy approved and ratified, by Information Governance Board (IGB)	Information Governance Board (IGB) approval
2.1 draft	26/11/2020	Section 4 D: Changed 18 months to 24 months. Change reviewed and approved by UEG on 20th November 2020	Lilia Pegg