BORDERS COLLEGE

Password Guidance

May 2023

History of Changes

Version	Description of Change	Authored by	Date
1.0	Initial Document	C Bradley	1/3/19
1.1	Updates to add guidance on • Domain admin accounts • Default passwords for network equipment • Password compromise	C Bradley	1/5/19
1.2	Implemented JCC comments to add ‘special characters’ to section 4 and fix spelling mistake	C Bradley	3/2/20
1.3	Added section on ‘login attempts and account lockouts’	C Bradley	28/7/20
1.4	Updates to • Password restrictions • Password creation and management	P Wawrzyczny	12/12/2022
1.5	Updates to • Password restrictions • Password creation and management • Administrator level password guidance	P Wawrzyczny	15/05/2023

Password Guidance

1. Introduction

All users of computer systems provided by the College must adhere to the password guidance defined below to protect the security of the network and to protect the integrity and confidentiality of data and computer systems.

Passwords are an important aspect of computer security as they are the front line of protection for user accounts. A poorly chosen password may result in the compromising of College IT Facilities.

All users are responsible for taking the steps, as outlined in this guidance to select and secure their passwords.

With the College's use of "single sign-on" i.e. one password for access to many systems, strong passwords and user responsibility for password management become even more essential.

2. Scope

This guidance applies to passwords for the use of all IT services administered by the College, including services provided under contract for the College.

3. Password restrictions

The College's password restrictions: password length – all passwords must have a minimum of 12 characters. Uppercase and lowercase characters – password must include at least one lowercase and uppercase character. Special characters – password must contain special character.

ISLT do not mandate the changing of passwords over time other than in instances where we suspect an account has been compromised. In these events ISLT will contact the relevant user and support them to change their password.

While this is ISLT's only enforced password restriction, we would ask that users follow the password creation and management advice below to help ensure their digital information is as secure as possible.

4. Password creation and management

The purpose of passwords is to protect the confidentiality and integrity of College IT facilities and assets. The combination of a particular username and password also provides an audit trail identifying which particular authorised user accessed a resource at a particular time. IT will disable any accounts identified as having shared passwords, and makes the following recommendations to users as password best practices:

Do not use the same password for College accounts as for other access (e.g. personal bank account, personal email account, etc.).

Make your password strong:

- Password strength is generally qualified in terms of how long it would take a computer to crack it, and under most circumstances, longer is better.
- The longer your password is, the more possible combinations there are for a computer to try, and it becomes difficult to crack in any reasonable amount of time.
- IT recommends using random sequences of words while creating passwords and avoiding the use of a single dictionary word.
- One possible method for picking a good password is to make up an acronym of a favourite song title, place you visited at the weekend etc. For example: “My favourite film is lord of the rings” could be: Mff2005L0tR$$.
- The use of special characters (e.g. “£$%^&) can increase the strength of a password but common substitutions, i.e. ! for I or @ for a, should be avoided.
- Do NOT use the example passwords used in this guidance.
- Avoid commonly used passwords such as the 25 most commonly used online passwords in 2016 as shown here (123456, password, 12345678, qwerty, abc123, 123456789, 111111, 1234567, iloveyou, adobe123, 123123, admin, 1234567890, letmein, photoshop, 1234, monkey, shadow, sunshine, 12345, password1, princess, azerty, trustno1, 000000).
- Avoid passwords based on easily discoverable information like your username or the name of a favourite pet.

Keep your password safe:

- Ideally, passwords should be sufficiently memorable so that there is no need to write it down. If a password must be written down to memorise it, then it should be stored securely e.g. in a sealed envelope in a secure cupboard.

The use of password managers such Chrome Password Sync, Apple Keychain, 1Pass, Lastpass etc. is acceptable for storage of College passwords. Users making use of a password manager must make sure that their master password for that system is sufficiently strong and securely stored.

You should never disclose your password. If someone demands a password, refer them to this document or instruct them to contact the IT Help Desk either by telephoning 01896 662645 or emailing itsupport@borderscollege.ac.uk.

Do not store passwords in a file on ANY computer system (including phones or similar devices) without encryption.

5. Login attempts and account lockouts

All College services are set to lock accounts after ten or fewer unsuccessful login attempts, or limit the number of login attempts to no more than ten within five minutes to defend against brute-force attacks.

6. Password compromise

If a user believes that their password has been compromised (shared with users other than themselves) they must:

- Inform their line manager of the potentially compromised account
- Reset the password at the earliest opportunity
- Inform the helpdesk of the potentially compromised account

7. Administrator level password guidance

The guidance in this section applies only to users who are provided with administrator level access. The granting of administrator level access is authorised by the Director of IT+Digital.

Domain Admin accounts

Where staff are provided with Domain Admin level accounts, these accounts should not be used for everyday IT usage such as:

- Email
- Administration
- Internet browsing

Domain Admin accounts must be reserved for essential server and network related work where that level of access is required.

Network/infrastructure equipment setup

Where staff are setting up new equipment on the College internal network, any default passwords (in particular for admin accounts) must be changed as part of the set-up procedure. New passwords should comply with the guidance in this document.

8. Exceptions

Some third-party systems may not be able to comply with College password guidance.

If an exception is requested, it may be granted at the discretion of the Head of ISLT.

9. Related Procedural Documents

- Information Security Policy