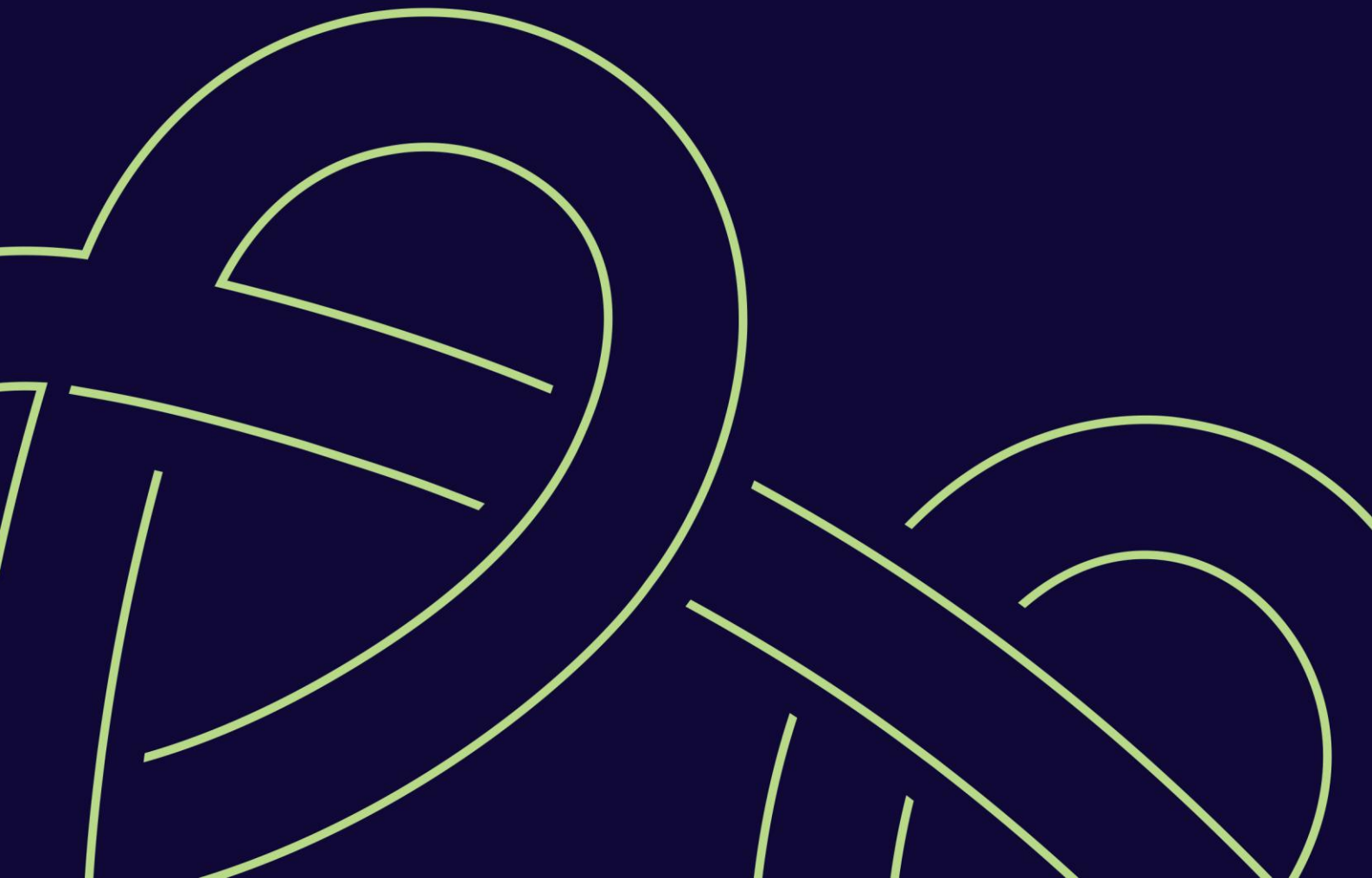


Password Policy

Infrastructure



Name of Policy:	Password Policy
Purpose of Policy:	This Password Policy establishes the requirements for creating, managing, and securing passwords in compliance with the Cyber Essentials Plus standard.
Intended audience:	Digital Services Staff
Approval for this policy given by:	Digital & Technical Services SMT
Date of Approval:	12/5/25
Proposed Review Date:	12/5/28
Individual Responsible for review:	Cyber Security Manager
Name of person completing this coversheet	James Eaton
Classification category of this policy:	Restricted

1. SCOPE

This policy applies to all accounts within all internal, external and 3rd party hosted university IT systems and services, including, but not limited to user accounts, privileged accounts and service accounts.

2. POLICY STATEMENT

Selecting a secure password

To promote strong password security, the university recommends using the 'Three Random Words' model for password creation. This model encourages the use of three random words that are easy to remember but difficult for attackers to guess, e.g., Purple-Table-Laptop.

Minimum account password requirements

The university recognises that different account types present differing levels of risk, the minimum requirements that are tolerable for any account are detailed below, categories of higher risk accounts have stricter requirements which are detailed in the "Additional account hardening requirements" section:

- Have a password at least 8 characters in length.
- Not have any form of maximum length restriction applied.
- Use a combination of uppercase letters, lowercase letters, numbers, and special characters.
- Not include any part of the user's name, username, or other easily guessed information.
- Never be stored in plain text, Plain-text storage of passwords is prohibited under this policy.
- Never be shared, sharing passwords between users is strictly prohibited.
- Be configured with MFA for external access.
- Not be configured with a minimum age.
- Have automatic an auto-lockout policy applied which locks for 30 minutes after 30 failed login attempts (within a 30 minute period).

Users are strictly prohibited from reusing passwords across multiple accounts or systems. Systems should be configured to disallow the reuse of previously used passwords.

Wherever possible, known bad password prohibition via a block list must be implemented across university systems. This prevents the use of known compromised or weak passwords (e.g., password123, qwerty, or any commonly used passwords).

The university does not enforce regular password expiry (maximum age) as a security control. This decision follows guidance from the National Cyber Security Centre (NCSC), which has advised against periodic password changes as they have been shown to encourage weaker password practices. Instead, passwords should only be changed if there is a suspected compromise or if a user has forgotten their credentials.

Additional account hardening requirements

Additional hardening for standard staff accounts:

Configuration:	Setting:	Rationale:
Account Lockout	30 minutes automatic Account Lockout after 10 bad passwords	To prevent “dictionary/credential stuffing” attacks.

Additional hardening for privileged user accounts (including ‘a’, ‘c’, ‘d’ and ‘r’ accounts and administrative accounts network hardware):

Configuration:	Setting:	Rationale:
Minimum password length:	<i>12 Characters</i>	In line with recommended minimum password sizes, to reduce the risk of dictionary attacks.
Change Password at first use	Yes	To support wholly offsite users, including partner colleges and external examiners.
Account Lockout	<i>30 minutes automatic Account Lockout after 10 bad passwords</i>	To prevent “dictionary/credential stuffing” attacks.

Additional hardening for Service accounts (defined as a non-user account which is logged into programmatically, or, used by a service directly):

Configuration:	Setting:	Rationale:
Minimum password length:	<i>32 Characters</i>	In line with recommended minimum password sizes, to reduce the risk of dictionary attacks.
Account Lockout	<i>5 minutes automatic Account Lockout after 100 bad passwords</i>	Necessary to stop service accounts being locked. Where possible external login to these accounts should be blocked via conditional access rule.

Additional hardening for LAPS accounts:

Configuration:	Setting	Rationale
Minimum password length:	<i>16 Characters</i>	Password automatically changes monthly. Increased length (from 14) to mitigate lowered entropy due to the character loss of applying ‘Improved readability’.
Password Complexity:	Large letters + small letters + numbers (Improved readability)	To assist helpdesk and support staff Improved readability removes visually similar characters (e.g. ‘0’ and ‘O’).
Account Lockout	<i>30 minutes automatic Account Lockout after 10 bad passwords</i>	To prevent “dictionary/credential stuffing” attacks. Where possible external login to these accounts should be blocked via conditional access rule.

3. RESPONSIBILITIES

- The platforms team are responsible for ensuring the password requirements are applied against existing university systems.
- The Technical Design Authority (TDA) are responsible for ensuring that new IT solutions can comply with the outlined account security requirements.
- The Cybersecurity team is responsible for reviewing and updating this policy.
- Individual users are responsible for setting secure passwords (as detailed in the “Selecting a secure password” section) on university accounts issued to them.
- Passwords on service accounts are the responsibility of the team to which they are issued.

4. REFERENCES

- IT Regulations
- Firewall Change Process
- IT Bring Your Own Device Policy
- IT Accounts Creation Deactivation Removal Policy
- IT Remote Working Policy
- IT Patch Management Policy
- IT Access Control Policy
- Malware Protection Policy

5. SANCTIONS

- Any user found to have ignored the requirements outlined in this policy will be subject to disciplinary action.
- Violations of this policy will be addressed in accordance with the university's IT Regulations.

