University College of Osteopathy

This policy helps all staff and students at the University College of Osteopathy to select, store and use appropriate methods of authentication.

Password Policy

infosec@uco.ac.uk

Document Control

Contents

Core Documentation Cover Page					
Password Policy					
Version number	**Dates produced and approved (include committee)**	**Reason for production/ revision**	**Author**	**Location(s)**	**Proposed next review date and approval required**
V1.0	Jan 2024 SMT	Produced to assure the security of information processed by the UCO in line with legislative requirements.	IT Director	All master versions will be held in: Quality Assurance SharePoint Area	Jan 2027 Or in response to legislative changes

Equality Impact	
Positive equality impact (i.e. the policy/procedure/guideline significantly reduces inequalities)	
Neutral equality impact (i.e. no significant effect)	X
Negative equality impact (i.e. increasing inequalities)	

If you have any feedback or suggestions for enhancing this policy, please email your comments to: quality@uco.ac.uk

1. Purpose

Passwords are an important aspect of computer security. Effective password management will minimise the likelihood of user accounts being easily compromised and mitigate risks to UCO information and IT systems. Use of long, complex passwords help to mitigate attacks that attempt to guess them; regular password changes help to mitigate the long-term exploitation of any disclosed or discovered passwords.

The purpose of this policy is to establish the standard for the creation of strong passwords, the protection of those passwords and their ongoing management.

2. Scope

This policy applies to all individuals and groups with user accounts with which to access the UCO's IT and network facilities. This includes, but is not limited to:

- Staff (full-time, part-time, and temporary).
- Registered students.
- Consultants and contractors working for, or on behalf of the UCO.
- Associates, visitors, and conference delegates.
- External services used for UCO purposes, e.g. social media.
- Privileged accounts (used for managing IT systems and services).

3. Responsibility and Consequences of Policy Violation

The UCO has an obligation to comply with statutory, legal and contractual requirements. It is the responsibility of every individual with a UCO user account to protect it in accordance with the standards set out in this policy.

- Relevant disciplinary procedures will be used in cases where a student or staff member fails to adhere to this policy.
- Commercial contracts for third parties and contractors must contain clauses referring to this policy and the consequences of non-compliance.
- Any exception to this policy must be approved in advance, by the UCO's IT Director or nominated deputy.

4. Principles and Requirements

- All passwords must be treated as confidential UCO information and must not be shared with anyone or made public in any form – either written or verbally.
- The same passwords must not be used for multiple UCO IT systems, where Single Sign On (SSO) is not available and users have the option to set their own passwords.
- UCO IT account details must not be used for non-UCO systems or applications, e.g., social media sites, retail websites, personal email and other services.

- Any individual that suspects their password may have been compromised must change it and inform the IT Helpdesk immediately.
- Passwords must never be disclosed e.g., written on a note or stored digitally in clear text.
- Consequently, passwords must not be recorded (e.g., paper, software file or hand-held device) unless this can be stored securely.
- The use of password managers (also known as a password vault) are permitted. For further information please contact the IT Helpdesk However, their use would be subject to strong encryption to protect the stored passwords in addition to a strong master password.
- The IT Helpdesk and IT Staff will never ask for full details of your password or other security credentials and therefore you should never provide these, either over the phone or in an email.

5. Multi-Factor Authentication (MFA)

Passwords are a single factor of authentication, something you know, but they can be guessed, or otherwise known by a third party. Where systems hold important information, we now require an additional factor of authentication. This typically utilises a mobile phone app, but could include a phone call, SMS or biometric identification, such as a fingerprint.

6. Changing your Password

All user-level and system-level passwords must conform to current UCO best practice guidelines. These are detailed as follows:

- Newly issued passwords must be changed on first use.
- All UCO passwords must be at least 8 characters long.
- Your five previously used UCO passwords cannot be reused.
- After ten unsuccessful attempts within a ten-minute period, you will be locked out of your account for a period of 30 minutes.
- Passwords must not be easily guessed (avoid using your name, children or a pet's name, car registration number, football team etc.).
- Be creative and use words memorable to you, so that people can't guess your password.
- Avoid the use of 'remember password' features in applications such as web browsers for more sensitive UCO systems and services.
- Passwords should not be shared with colleagues, for instance when on annual leave - use functionality such as delegated access with email instead.
- In line with Government guidance, UCO does not typically enforce the regular changing of passwords, as this can lead to poor password management.
- UCO actively encourages the technique of using three random words. Numbers and symbols can still be used if needed, for example '3red!houseBananas'.

7. Privileged Access

Where an individual requires more access privileges than a standard account, such as a system administrator, these accounts should be handled with extra care due to the increased potential for harmful use. As such, ‘admin’ accounts should be separate from the standard user account and follow these principles:

- Passwords should be unique from all others, especially the individual’s standard account.
- MFA must be enabled wherever it is available.
- Passwords must be stored securely and used to elevate privilege only when required.
- UCO servers must be protected by additional MFA when using elevated permissions.

8. Staff Handling Card Payments

To comply with the Payment Card Industry (PCI) Data Security Standard, members of staff who handle payments via debit, credit, and pre-paid cards (e.g. Mastercard & Visa) must additionally:

- Must change passwords at least once every 90 days.
- Changed passwords must not be different to any of the previous four used by that individual.
- Must contain both numeric and alphabetic characters.