UNIVERSITY OF WESTMINSTER

Information Systems and Support - IT Password Policy

1. Introduction

1.1 This policy sets out the password requirements for any account used to access or federate to University systems, network, and computer devices, be that an unnamed system account or that of an individual user.

1.2 This policy supports the Cyber Essentials certification principles to ensure that passwords used to access computer resources are selected, maintained, and updated in line with the University security profile standards.

1.3 The University IT Acceptable Use Policy state that Users must take all necessary steps to protect and maintain the security of any equipment, software, data, storage area and/or passwords allocated for their use. This policy dictates the minimum that a user must do to conform to this requirement when selecting and updating a password.

1.4 This password policy is used to mitigate possible attacks against the University network infrastructure and the data held within it. Use of long, complex passwords helps to mitigate attacks that attempt to guess passwords, and regular password changes to mitigate long term exploitation of any disclosed or discovered passwords.

1.5 This document sets out the policy and guidance on password structure, technical standards and technology required to keep the University IT estate secure and confidential.

2. Password Policy

2.1 All passwords must adhere to the following length and complexity requirements:

- Use a minimum of 10 characters.
- Each new password should be different from the previous one and must meet the same requirements for length and complexity.
- Contain at least 1 character from three of the following 5 categories: uppercase letters, lowercase letters, numbers, special characters, unicode character that's categorised as an alphabetic character but isn't uppercase or lowercase. For further details, please see the technical standard for password complexity.
- Do not use names associated with yourself such as family or pet names, team names, common dictionary words or anything associated with the University.
- Guidance to select a non-guessable password is to select three or four random words. Using mixed upper and lower case, combine the words using punctuation marks or numbers as separators. Some examples: onlytimewillt3LL, Keyz2the.Kingd0m, 0Tempora.0Mor3$. Attention: Do not use any of the above examples as your password!

2.2 When users are first issued with an account, a temporary password will be created and shared with them in a secure manner. Users will be required to change their password upon first logon.

2.3 Colleagues must register for the self-service password reset service as per University guidance, to allow them to safely and quickly reset their own password. If you do not do this, you will not be able to re-set your password and will lose access to University services.

2.4 Change your password when you receive notification to do so, don't let it expire. Passwords for colleagues expire every 6 months. Passwords for students expire after 12 months.

2.5 Passwords may be requested to be changed without notice in response to security incidents or suspicion of password compromise and account misuse. Any such request will be made by the ISS Service Desk and users will always be required to reset their password on the self-service password reset facility.

2.6 Store your password in a suitable application if available, such as a password manager.

2.7 Do not use the same University password for your non-University accounts.

2.8 Do not share your password with anyone including colleagues and students. ISS Support Staff will never ask you for your password. If anyone asks you for your password, do not give it to them.

2.9 Never write down your password on a piece of paper.

2.10 In addition to using a password, multi-factor authentication (MFA) must be used to access certain University systems/data. More information on what this applies to is available on the University Intranet. Often known as two-factor authentication (2FA), is a security system that requires more than one form of identification in order to access something, such as a password and a unique code.

Where you have been provided with a MFA access you must protect the device on which the additional authentication relies (for example your mobile phone). Make sure the device is not left unattended and ensure the device is configured with a passcode for access.

3. Related Policies

3.1 This policy forms part of the information security management system (ISMS) at the University of Westminster. The IT password policy should be read in conjunction with all other University information management policies.

4. Publishing Policies

4.1 This policy is published on the University website at https://www.westminster.ac.uk/about-us/our-university/corporate-information/policies-and-documents-a-z and can be requested in a range of formats e.g. Word, PDF, plain text, alternative formats such as large print or Braille.