PASSWORD POLICY

Principle

Edinburgh Napier University recognises the importance of information security and the need to ensure that only authorised access to systems and electronic information is permitted, whether by people or other systems. This must be done in a way that is both robust and proportionate to the information risk. Passwords are the main means of user authentication in use. This policy ensures that passwords are used in the most secure way.

Responsibilities

Individuals

1. Individuals shall keep their passwords private and never reveal them to or share them with anyone else.

2. Individuals shall be accountable for all activity associated with their University account, even if performed with their knowledge or permission by someone else.

3. Individuals who suspect that any of their passwords have been revealed to or discovered by another person shall change the affected password(s) immediately.

4. Individuals shall use a unique password for their University account, different to any other passwords they may have for personal or work purposes.

5. All passwords shall meet the requirements of the current Passwords Technical Standard (Appendix A) and individuals shall be required to update their passwords if required when the Passwords Technical Standard is revised.

6. Individuals may write a password down if it is not feasible to memorise it, for example if the password is used infrequently or for specific business-continuity purposes. If this is done, the written password shall be stored in a secure location such as a safe or locked filing cabinet and there shall be no information kept with the password that would enable it to be used inappropriately.

7. Individuals may use a password manager application to store passwords securely. If individuals choose to use a password manager application, the master password and all the generated passwords shall meet the requirements of the current Passwords Technical Standard.

System Owners and System Administrators

8. In certain cases shared use of a password by multiple authorised people is unavoidable, for example the password associated with the ‘Administrator’ account on Windows, the ‘root’ account on Linux and similar accounts including those used for disaster recovery or business continuity

purposes. All such passwords shall be stored securely and changed immediately whenever a person is no longer authorised to use the password, for example if they change role or leave the University.

9. Systems owners shall ensure that password authentication systems meet the requirements of the current Passwords Technical Standard. When the Passwords Technical Standard is revised, they shall be required to update their system accordingly.

Exceptions

Edinburgh Napier University recognises that it may be necessary on occasion, for example to exploit strategic or operational opportunities, to permit defined and limited exceptions to this policy. Anyone who believes such an exception is necessary should contact the IS Service Desk in the first instance. Their request will be assessed by Information Services staff, including if necessary the Information Security Board and the Director of Information Services. If approved, the exception will be documented and reviewed regularly by the Information Security Board.

Compliance

Edinburgh Napier University will conduct information security compliance and assurance activities, facilitated by the University's Information Security Team, to ensure that information security objectives and the requirements of information security policies are met. Wilful or repeated failure to comply with any information security policy will be treated seriously by the University and may result in enforcement action being taken, including disciplinary action.

This policy applies to University staff, students and to external parties working with the University.

Annex A – Passwords Technical Standard

All users (staff, students and external parties working with the University)

Password

Any secret sequence of letters, numbers and special characters which can be used – often in conjunction with a user name – to prove your identity to a computer system or website. Passphrases (sequences of words) and PINs (sequences of numbers) are also considered passwords for the purposes of this Policy.

Composition, Complexity and Length

- Passwords may contain lowercase letters, uppercase letters, numbers and symbols (including spaces).
- Passwords shall be at least 15 characters in length (unless this is constrained by the system).

Age, History and Reuse

- Passwords shall have a maximum age of 365 days.
- Passwords shall be changed whenever they are suspected of being, or known to be compromised, regardless of age.
- When selecting a new password for a given account, it should not be the same as any of the previous passwords used for that account, or any other account belonging to the same person.

Additional Requirements for system owners and system administrators

Composition, Complexity and Length

- Any password which is used for application to application authentication or which grants administrative privileges shall contain lowercase letters, uppercase letters, numbers and symbols.
- Any password which is used for application to application authentication shall be at least 30 characters in length.

Secure Generation

- Passwords and passphrases automatically generated for use by people shall meet the requirements of this Standard, but should be user friendly – the generation of truly random passwords for this purpose is to be avoided.
- Generated passphrases comprised of random dictionary words shall contain at least 4 dictionary words and shall meet the minimum length requirement of this Standard.
- Passwords used for application to application authentication or which grant administrative privileges shall be randomly generated in accordance with the complexity and length requirements of this Standard.

Password Authentication Systems

- Systems which implement password authentication should:
    - Allow passwords to be up to 256 characters in length
    - Only transmit passwords over TLS or another strong transport mechanism
    - Not store plaintext or encrypted passwords
    - Add unique cryptographic salts to passwords prior to hashing
    - Hash passwords using multiple rounds of a secure password hashing algorithm
    - Not use MD4, MD5, SHA1 or SHA256 as a password hashing algorithm
    - Utilise Multi-Factor Authentication (MFA)
    - Utilise rate-limiting to limit the effectiveness of brute-force attacks, allowing no more than 10 guesses within 5 minutes
    - Prevent users from selecting insecure passwords, by checking them against a list of banned passwords and rejecting any matching those on the list
    - Prevent users from selecting any of the 24 historic passwords they have previously used with the same account
    - Log failures to allow suspicious activity to be detected and investigated
    - Not inhibit the use of Password Managers, for example by blocking the use of copy-and-paste in username or password fields
- Where possible, the use of password authentication should be avoided. Think about whether the resource being protected actually requires password authentication, or if an alternative mechanism such as Single Sign-On (SSO) or WebAuthn could be used instead.

Application to application password

Any form of static alphanumeric secret e.g. a password, pre-shared key, API key, etc. which is used to authenticate one software component, service or application to another, whether or not in the context of a particular user or service account.