**Password Policy**

**General Comments -**

* This is a template/precedent document only. It should be tailored as appropriate to suit the needs of each individual firm.
* All sections should be considered and implemented as deemed appropriate for the firm. This cover page should not be included.
* The LQSI cannot accept any responsibility for any errors or omissions contained in this template document.
* The document should be reviewed on an annual basis, or as required.

**Specific Comments –**

* This policy has been updated to remove reference to changing passwords as this requirement has been removed from the IT questionnaire, in line with current best practice IT security recommendations.

**The Legal Quality Standard of Ireland**

**Reviewed March 2024**

**[FIRM NAME]**

**Password Policy**

**Overview**

Passwords are an important aspect of computer security and are an integral part of the firm’s overall IT security policy.  They are the frontline of protection for user accounts.  A poorly chosen password may result in a compromise of [firms name]’s entire network.  Within Ireland and globally, major IT security breaches continue to occur each year due to poor password management. As such, all employees are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

**Matters to be Considered when Choosing a Password**

* Consider using passphrases; these are easier to remember but hard to guess and help in creating longer, more complex passwords.
* Use random and unrelated words; the greater the complexity, the stronger the password
* Consider using words from different languages
* Use a combination of random numerical and special characters throughout the passphrase
* Do not use a word from a dictionary
* Do not use names, dates of birth, ages, telephone numbers, pet’s names, football teams or anything related to you
* Do not use sequences or repeated characters (123456, 222222, abcdefg) or adjacent characters on your keyboard (qwerty)
* Do not use words or abbreviations associated with your firm or industry
* Do not use the same passwords for multiple different purposes
* Do not share your passwords with anyone else, **ever**
* Passwords should never be stored on line
* Consider using Password managers as an easy way to manage multiple complex passwords.
* Decline the ‘remember password’ prompt box on web browsers regardless as to whether you are using a private or shared computer.

An ideal password is long and has letter, punctuation, symbols and numbers and contains **at least 12 characters.  [Ensure all of your staff always follow the most up to date best practice advice in terms of length and complexity of passwords. We advise liaising with your IT provider on this matter at least annually.]**

All employees should be aware that even a very long, complex password is no defence against one very common practice – using the same password for all services.  

Employees are once again reminded of the importance of secure password hygiene (i.e. following tips above), not just with work related accounts but also with personal accounts**.**

**~~[Firm should re-consider the requirement to regularly change passwords as complexity is preferable to regularly changing a password]~~** ~~It is firm policy that all passwords must be changed every 90 days.  Employees should not use a previous password.~~

If an account or password is suspected to have been compromised, report the incident to [insert name] and immediately change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by [IT provider/office manager].  If a password is guessed or cracked during one of these scans, then the user will be required to change it.  

**Multi Factor Authentication – *include if applicable***

The firm has now enabled Multi Factor Authentication (also known as MFA or 2FA) across all work issued devices. This involves using your user-name and password and one other piece of information. [firm should confirm what this is, suggestions include –

A physical object in the possession of the user – eg mobile phone;

A physical characteristic of the user (biometrics) or

An additional piece of information that is only known to the user]

Where remote access to centrally held information is required, the firm should ensure that MFA is enabled.

Any employee found to have violated this policy may be subject to disciplinary action.  

**Signed:**

**Date:**

**Date of next review:**