Password Security Policy

1. Overview

This policy is intended to establish guidelines for effectively creating, maintaining, and ensuring the security of passwords at Verner Wheelock.

2. Scope

This policy shall apply to all employees and associates of Verner Wheelock and shall govern acceptable password use on all systems that connect to the Company's network or access or store the Company's data.

3. Password Security

- Passwords will always be allocated by the Administration Controller
- They will be allocated to a specific individual for their access only to the identified system
- They must not be shared with anyone else.

4. Good Practice

- Each member of staff will have a unique password for the system that they access
- All computers will have a screen saver password activated with activation time no more than 5 minutes
- Computers must be logged off the network when left unattended
- Passwords must be removed when employees leave the company
- It is not permitted to display passwords on the computer or in any other place with easy access
- Only in exceptional circumstances may the password be written down, and in such cases, it must be retained in a secure place
- Passwords must not be displayed on the screen as they are entered
- Temporary passwords will remain in use for the absolute minimum of time
- In there is a suspected breach of password use the incident will be reported and logged as required in the company non conformance procedures
- Passwords will be a minimum of eight characters, at least one of which should be a numeric character
- There will be no correlation between the password and the system being entered
- No elements of the password will relate to the user (family names, nicknames etc.).

5. **Password Maintenance**
    - Passwords will be changed regularly (minimum three monthly)
    - Re-use of passwords is not permitted
    - In the case of a suspected breach, the password will be changed immediately
    - Password software will require the entry of the old password before the new one is entered and accepted
    - New passwords will need to be entered twice
    - Password data will be held in encrypted format.

6. **Enforcement**

It is the responsibility of the end user to ensure enforcement with the policies above.

If you believe your password may have been compromised, please immediately report the incident to the Administration Controller and change the password.

RELATED DOCUMENTATION
Information Security Policy
Mobile Computing Policy

REFERENCES
ISO 27001:2013, ISO 27002:2013