HarborView Consulting, LLC

Password Policy

1. Purpose

The purpose of this policy is to protect HarborView Consulting, LLC systems, data, and customer information by ensuring that all user passwords are strong, unique, and properly managed. Passwords are a critical first line of defense against unauthorized access.

---

2. Scope

This policy applies to:

- All employees
- Contractors and temporary staff
- Any individual with access to HarborView Consulting, LLC systems, networks, or cloud services

---

3. Password Length Requirements

- All passwords **must be between 12 and 15 characters** in length.
- Shorter passwords are not permitted, even if they appear complex.

Rationale:
Longer passwords are significantly harder to crack through brute-force or automated attacks. However, HarborView recognizes that long passwords can be difficult to remember if created poorly. To reduce the risk of employees writing passwords down, users are encouraged to use **passphrases** (see Section 7).

---

4. Password Complexity Requirements

Passwords must include:

- At least **one uppercase letter**
- At least **one lowercase letter**
- At least **one number**
- At least **one special character** (e.g., ! @ # $ %)

Rather than using random or overly complex strings that are difficult to remember, users are encouraged to:

- Substitute letters with memorable symbols or numbers
  - O → 0
  - A → @
  - S → $
- Use meaningful substitutions that are easy to recall personally but difficult for others to guess.

Example:
`Br00k$hieldsDesert$Storm1991`

---

5. Password Expiration (Maximum Password Age)

- Passwords must be changed **every 90 days**.
- Users will receive automated reminders prior to expiration.
- Expired passwords will prevent system access until changed.

Rationale:
Regular password rotation reduces the risk of long-term credential compromise and limits damage if a password is unknowingly exposed.

---

6. Password History Enforcement

- The system will remember the **last 20 passwords** used.
- Users may not reuse any of these previous passwords.

Rationale:
Password expiration is ineffective if users are allowed to cycle back to old passwords. Enforcing password history ensures meaningful changes over time.

---

7. Minimum Password Age

- Passwords must be kept for a **minimum of 15 days** before they can be changed again.

Rationale:
This prevents users from rapidly changing passwords multiple times in order to reuse an old or familiar password.

8. Passphrase and Mnemonic Guidance (Strongly Encouraged)

To help employees remember long and complex passwords without writing them down, HarborView Consulting strongly encourages the use of **passphrases**.

A passphrase is:

- A unique and memorable phrase meaningful to the user
- Modified with capitalization, numbers, and symbols
- Easy to recall but difficult for others to guess

Tips for Creating a Good Passphrase:

- Base it on a personal interest, historical event, favorite book, or hobby
- Replace certain letters consistently with symbols or numbers
- Capitalize words in a predictable way for yourself

Example Approach:

- Original phrase: *Brooke Shields Desert Storm 1991*
- Modified password: `Br00k$hieldsDesert$Storm1991`

Once the substitution pattern becomes habit, the password becomes second nature and eliminates the temptation to write it down.

9. Prohibited Practices

Employees must not:

- Share passwords with anyone, including coworkers or IT staff
- Write passwords on sticky notes, notebooks, or unsecured documents
- Reuse work passwords for personal accounts
- Store passwords in plain text files or emails

10. Enforcement

Failure to comply with this policy may result in:

- Account suspension
- Mandatory security retraining

- Disciplinary action up to and including termination, depending on severity

---

11. Review and Updates

This policy will be reviewed annually and updated as needed to reflect changes in technology, threats, or regulatory requirements.