**Team #5**

**Inject Number: 10**

**Merlin’s Storage Password Policy**

**1.0 Overview**

Passwords are used to both access and secure organizational computer systems. A weak password may result in unauthorized access and/or exploitation of Merlin’s Storage resources. All users with access to the company’s systems must strictly follow the steps and rules, as outlined below, to select and secure their passwords.

**2.0 Purpose**

The purpose of this policy is to create password standards across all user accounts, the protection of those passwords, and the required minimum amount of time between password changes.

**3.0 Scope**

This policy applies to all users, employees, and personnel that have access accounts to the company’s computer systems.

**4.0 Policy**

### 4.1 Password Creation

1. Minimum Length - 9 characters

2. Maximum Length - 25 characters

3. Passwords must include at least one special character.

4. Users must create easy to remember, secure passwords.

5. Passwords should not contain common phrases or words (such as, password)

6. Users cannot use a previous account password.

7. Users may not use the same password for Merlin’s Storage accounts as for non-company access.

8. User accounts with system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.

### 4.2 Password Change

1. All system-level passwords must be changed on at least a quarterly basis

2. All user-level passwords must be changed at least once a year.

3. If a password is not changed within the required timeframe, users will be prompted to change their password

### 4.3 Password Protection

1. Passwords must not be shared with anyone. Passwords are treated as sensitive Confidential

Merlin’s Storage information.

2. Passwords can never be written down.

3. Passwords can never included in email, messages, or any other form of electronic communication

4. Passwords should not be told over the phone to anyone.

5. Passwords should not be revealed on questionnaires or security forms.

6. Do not hint at the format of a password.

7. Never store passwords in non-encrypted files anywhere.

8. Never write passwords down and store them anywhere.

9. Do not share Merlin’s Storage passwords with anyone, including administrative assistants, secretaries, managers, co-workers, and family members.

### 4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

1. Applications must support authentication of individual users, not groups.

2. Applications must not store passwords in clear text or in any easily reversible form.

3. Applications must not store passwords in clear text or in any easily reversible form.

4. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

**5. Policy Compliance**

### 5.1 Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

### 5.2 Exceptions

Any exception to the policy must be approved by the IT Team in advance.

### 5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.