Developed Policy Documents

- **Password Protected Policy**

1. **Overview**

Passwords are a critical aspect of computer security. A weak or compromised password can result in unauthorised access to our most sensitive data and/or exploitation of our resources. All staff, including contractors and vendors with access to ACME Healthcare systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. **Purpose**

The purpose of this policy is to establish a standard for the secure use and protection of all work related passwords.

3. **Scope**

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any ACME Healthcare facility, has access to the network, or stores any non-public ACME Healthcare information.

4. **Policy**

- **Password Creation and Use**
- All user-level and system-level passwords must conform to the Password Construction Guidelines. Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.
- Staff are allowed to use authorised, approved password managers to securely store and manage all their work related passwords.
- User accounts that have 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. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts

5. **Password Change**

- Passwords should be changed only when there is reason to believe a password has been compromised or fails to meet our Password Creation Requirements.. We do not recommend the use or setting of regular password expiration.

6. **Password Protection**

- Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential ACME Healthcare information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.
- Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.
- Passwords may be stored only in password managers authorised by the organisation.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any individual suspecting that their password may have been compromised must report the incident and change all relevant passwords.

7. **Application Development**

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

- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- 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.

8. **Multi-Factor Authentication**

- Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also

9. **Policy Compliance**

- Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

- **Exceptions**
  Any exception to the policy must be approved by the Infosec team in advance.
- **Non-Compliance**
  An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

10. Related Standards, Policies and Processes

Password Construction Guidelines