Password Policy

Policy Statement:

This policy establishes guidelines for creating strong and secure passwords to protect the confidentiality, integrity, and availability of our organization's information assets.

Scope:

All users, including employees, students, contractors, and third-party vendors, must adhere to the following password requirements:

Password Length:

Passwords must be a minimum of 20 characters in length. Longer passwords provide increased security against brute force and dictionary attacks.

Password Complexity:

Passwords are allowed to be a phrase that can easily be remembered. Passwords containing special characters within that phrase are more secure and difficult to hack.

Password Expiry:

All passwords must be reset annually. Users will receive notifications prompting them to change their passwords before expiration.

Password History:

Users are prohibited from reusing their last eight passwords. This prevents the reuse of previously compromised passwords and enhances overall security.

Password Storage:

Passwords must not be stored in plaintext format. They should be stored securely using industry-standard encryption methods. Passwords must not be written down or stored in easily accessible locations, such as ohp0.0000012 vme p1371 2ng

Password Recovery:

Users must follow the organization's established procedures for password recovery. These procedures may include verification of the user's identity before resetting passwords. You may