Password Protection Policy

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to Noesya 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 creation of strong passwords and the protection of those 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 Noesya facility, has access to the Noesya network, or stores any non-public Noesya information.

4. Policy

A. Password Creation

A.1 All user-level and system-level passwords must be match this rules:

Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 14 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include “It’s time for vacation” or “block-curious-sunny-leaves”. Passphrases are both easy to remember and type, yet meet the strength requirements. Poor, or weak, passwords have the following characteristics: Contain eight characters or less; Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters; Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321; Are some version of “Welcome123” “Password123” “Changeme123”.

A.2 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.

A.3 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 recommend that some form of multi-factor authentication is used for any privileged accounts

B. Password Change

B.1 Passwords should be changed only when there is reason to believe a password has been compromised.

B.2 Password cracking or guessing may be performed on a periodic or random basis by the Security Team. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with this policy.

C. Password Protection

C.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential Noesya information.

C.2 Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.

C.3 Passwords may be stored only in “password managers” authorized by the organization.

C.4 Do not use the "Remember Password" feature of applications (for example, web browsers).

C.5 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

D. Application Development

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

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

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

D.3 Applications must not transmit passwords in clear text over the network.

D.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.

E. Multi-Factor Authentication

E.1 Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

5. Policy Compliance

A. Compliance Measurement

The security team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, internal audits, and feedback to the policy owner.

B. Non-Compliance

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

6. Revision History

1.0 Date of change: 01/09/2021 - Responsible: Technical team - Summary of Change: Initial release