PASSWORDS POLICY

Introduction

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of [agency name]'s entire network. As such, all [agency name] employees (including contractors and vendors with access to [agency name] systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

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 AAG facility, has access to the AAG network and/ or any other electronic system that is used by AAG.

Policy

General

1. All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.
2. All production system-level passwords must be part of the Information Security administrated global password management database.
3. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 180 days and cannot be reused the past 10 passwords.
4. Passwords must not be inserted into email messages or other forms of electronic communication.
5. All user-level, system-level, and access level passwords must conform to the guidelines described below.

Guidelines

All passwords must comply with the following requirements:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the User ID.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear or plaintext outside the secure location.
7. Not be displayed when entered.
8. Ensure passwords are only reset for authorized user.

PASSWORDS POLICY

Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

- When a user retires, quits, is reassigned, released, dismissed, terminated etc.
- Default passwords shall be changed immediately on all equipment.
- Contractor accounts, when no longer needed to perform their duties.
- As directed by the General Manager.

When a password is no longer needed, the following procedures should be followed:

- The worker must notify his or her immediate supervisor.
- Supervisor must notify National Human Resources Manager in writing (email).
- The HR will then delete the user's password and delete or suspend the user's account.
    - A second individual from that department will check to ensure that the password has been deleted and user account was deleted or suspended.
    - The password email request will be filed within HR.

Password Protection Standards

Do not use your User ID as your password. Do not share AAG passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential AAG information.

Here is a list of "do not's"

- Don't reveal a password over the phone to anyone
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don' talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to a co-worker while on vacation
- Don't use the "Remember Password" feature of applications
- Don't write passwords down and store them anywhere in your office
- Don't store passwords in a file on ANY computer system unencrypted

PASSWORDS POLICY

If someone demands a password, refer them to this document or have them call the National HR Manager. If an account or password is suspected to have been compromised, report the incident to the HR Manager Immediately.

The ICT department is responsible for overall management of all password related issues however, they are not to be contacted directly by any worker. All password requests will be through the National HR Manager.

The ICT Department may perform password cracking or guessing may be performed on a periodic or random basis as requested by the General Manager to the ICT Department. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Where directed by the General Manager, two factor authentication (2FA) may be required to access a system(s). It is the responsibility of the worker requiring use of 2FA to maintain this always.

Application Development Standards

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

- Should support authentication of individual users, not groups.
- Must store passwords in a protected environment that is limited to key account contact.
- Should provide some sort of role management, such that one user can take over the function of another without having to know the other's password.
- Computer security software must be installed on all devices that are used to carry out application development for AAG.

Remote Access Users

Access to the AAG networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required) or a form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.).

Penalties

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

Aussie Automotive Group

3 August 2021