Password Policy

1.0 Overview

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 JGSFC entire network. Assuch, all JGSFC employees (including contractors and vendors with access to JGSFC systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password. (*See Physical Protection Policy for additional information).*

2.0 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.

3.0 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 JGSFC facility, has access to the JGSFC network and/or LEIN/NCIC network, or stores any non-public JGSFC LEIN-based Criminal Justice Information (CJI).

4.0 Policy

4.1 General

- All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.
- All production system-level passwords must be part of the Information Security administrated global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days and cannot be reused the past 10 passwords.
- User accounts with access to LEIN/NCIC privileges must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level, system-level, and LEIN/NCIC access level passwords must conform to the guidelines described below.

4.2 Guidelines

Password Construction Requirements

i. Be a minimum length of eight (8) characters on all systems.
ii. Not be a dictionary word or proper name.
iii. Not be the same as the User ID.
iv. Expire within a maximum of 90 calendar days.
v. Not be identical to the previous ten (10) passwords.
vi. Not be transmitted in the clear or plaintext outside the secure location.
vii. Not be displayed when entered.
viii. Ensure passwords are only reset for authorized user.

4.3 Password Deletion

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

J. G. Shah Financial Consultants Pvt. Ltd.

Director / Authorised Signatory

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

When a password is no longer needed, the following procedures should be followed ***(See User Account Access Validtion Policy for additional information/requirements)***:

- Employee should notify his or her immediate supervisor.
- Contractor should inform his or her point-of-contact (POC).
- Supervisor or POC should fill out a password deletion form and send it to *[agency's POC]*.
- *[Agency's POC]* 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 deletion form will be filed in a secure filing system.

4.4 Password Protection Standards

Do not use your User ID as your password. Do not share JGSFC passwords with anyone,including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential *[agency name]* 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 mail 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.

If someone demands a password, refer them to this document or have them call [*list name of Information Security Officer (ISO) or Agency POC]*.

If an account or password is suspected to have been compromised, report the incident to [name of ISO or POC] and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the MSP/FBI or *[agency Security Department or POC]*. If a password is guessed or cracked during one of these scans, the user will be required to change it.

4.5 Application Development Standards

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

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.

J. G. Shah Finance & Consultants Pvt. Ltd

Director / Authorised Signatory

- 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.
- Should support Terminal Access Controller Access Control System+ (TACACS+), Remote Authentication Dial-In User Service (RADIUS), and/or X.509 with Lightweight Directory Access Protocol (LDAP) security retrieval, wherever possible.

4.6 Remote Access Users

Access to the *[agency name]* 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.).

5.0 Penalties

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

Other Related Resources:

- Physical Protection Policy (Required)
- User Account – Access Validation Policy (Required)

J. G. Shah Financial Consultants Pvt. Ltd.

Director / Authorised Signatory