Password Management Policy

1 Objective

At SFO we are cognizant that passwords are a critical element in overall computer security. Passwords must be selected and secured following the guidelines outlined below to protect user accounts and SFO's network. This policy applies to all employees, consultants, outsourced employees and contractors (hereafter referred to as 'individuals') of SFO. It also covers all sites and divisions and IT and information communications facilities operated by SFO or on its behalf including its subsidiary companies and sister concerns under NeST group.

2 Purpose

The purpose of this policy is to ensure that secure practices are introduced and maintained by all employees with respect to password protected information infrastructure. This includes establishing a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

3 Scope

The policy is applicable for all IT systems and services and shall apply to all employees, contractors, and affiliates of SFO and shall govern acceptable password use on all systems that connect to SFO network or access or store SFO data.

4 Policy

4.1 Password Creation

a) All user and admin passwords must be at least 8 characters in length. Longer passwords and passphrases are strongly encouraged.
b) All user and admin passwords must meet the complexity requirements and be protected by strong passwords adhering to the Passwords parameters guideline.
c) Where possible, password dictionaries should be utilized to prevent the use of common and easily cracked passwords.
d) Passwords must be completely unique, and not used for any other system, application, or personal account.
e) Default installation passwords must be changed immediately after installation is complete.

4.2 Password Parameters

All user and system passwords, even temporary passwords set for new user accounts, should meet the following characteristics:

a) Be at least 10 characters in length
b) Consist of a mix of alpha, and at least one numeric, and special characters
c) Not be dictionary words
d) Not be portions of associated account names (e.g., user ID, log-in name)
e) Not be character strings (e.g., abc or 123)
f) Not be simple keyboard patterns

In addition, users are required to select a new password immediately after their initial logon.

4.3 Password Aging

g) User passwords must be changed every 30 days. Previously used passwords may not be reused.
h) System-level passwords must be changed on a quarterly basis.

4.4 Password Protection

a) Access to SFO resources shall be controlled and shall be based on an approved System Access Request Form for each of the systems.
b) Individuals shall be granted access only to those information systems necessary for the performance of their official duties; users must receive supervisor's and the IT Manager's approval prior to being granted access to SFO's information resources. This requirement includes contracted employees and all other non-SFO personnel who have been granted access.
c) Passwords shall be used on all SFO automated information systems to uniquely identify individual users.
d) Passwords must not be shared with anyone (including co-workers and supervisors) and must not be revealed or sent electronically, generic or group passwords shall not be used.
e) Passwords shall not be written down or physically stored anywhere in the office.
f) When configuring password "hints," do not hint at the format of your password (e.g., "zip + middle name")
g) User IDs and passwords must not be stored in an unencrypted format.
h) User IDs and passwords must not be scripted to enable automatic login.
i) "Remember Password" feature on websites and applications should not be used.

j) All mobile devices that connect to the company network must be secured with a password and/or biometric authentication and must be configured to lock after 3 minutes of inactivity.

4.5 Password and Account Security

a) Password accounts not used for 60 days will be disabled and reviewed for possible deletion. Accounts disabled for 60 days will be deleted. Accounts for SFO contractors shall terminate on the expiration date of their contract.
b) Intruder Lockout policy is implemented for unsuccessful login attempts. After 5 unsuccessful login attempts the user account will be locked.
c) Screen-saver password must be enabled after 10 minutes of inactivity of the user. Users are not allowed to change the inactivity time.
d) Administrative account passwords must be changed promptly upon departure of personnel (mandatory or voluntary) or suspected compromise of the password. User accounts will be disabled promptly upon departure of personnel (mandatory or voluntary). Users should immediately change their password if they suspect it has been compromised.
e) Vendor or service accounts will be removed from computer systems prior to deployment and new passwords are to be implemented on all systems immediately upon installation at SFO facilities.
f) Passwords may not be embedded in automated programs, utilities, or applications, such as: autoexec.bat files, batch job files, terminal hot keys.
g) Passwords may be not visible on a screen, hardcopy printouts, or any other output device

5 Enforcement

It is the responsibility of the end user to ensure enforcement with the policies above.

If you believe your password may have been compromised, please **immediately** report the incident to IT Security and change the password.

Unauthorized personnel are not allowed to see or obtain sensitive data. Any employee found to have violated this policy would be subjected to disciplinary action in line with the HR Policy.