Contents

[1. Introduction to Password Policy 5](#_Toc79157533)

[2. Purpose 5](#_Toc79157534)

[3. Scope 5](#_Toc79157535)

[4. Policy 5](#_Toc79157536)

[**4.1 General** 6](#_Toc79157537)

[**4.2 Use of passwords for remote access users** 6](#_Toc79157538)

[**4.3 Passphrases** 6](#_Toc79157539)

[**4.4 Application Development Standards** 6](#_Toc79157540)

[**4.5 Storing Passwords** 7](#_Toc79157541)

[5. Guidelines 7](#_Toc79157542)

[6. Security controls 7](#_Toc79157543)

[7. Enforcement 8](#_Toc79157544)

**DOCUMENT REVISION CONTROL**

REVISION HISTORY

| **Date** | **Author** | **Version** | **Change Reference** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

REVIEWERS

| **Name** | **Position** | **Date** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

DISTRIBUTION

| **Date** | **Distributed to** | **Version** | **Distribution Format** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

APPROVALS

| **Date** | **Version** | **Approved by** | **Designation** | **Signature** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**LIST OF ABBREVIATIONS**

|  |  |  |
| --- | --- | --- |
| **Index** | **Abbreviation** | **Stands For** |
| I | IT | Information Technology |
| 2 | SLA | Service Level Agreement |
| 3 | IOT | Internet of things |
| 4 | IAS | International Accounting Standards |
| 5 | FDP | Finance Department |
| 6 | ITSM | Information Technology Service Management |
| 7 | NDA | Non-Disclosure Agreement |

1. **Introduction to Password Policy**

Password policy defines how the password is to be created, importance of password for security, and other features of password. This policy, also defines the requirements for the proper and secure handling of passwords in <Company Name>.

Passwords are first line of protection and an important aspect of information security.

1. **Purpose**

Password policy is created to establish a standard for creation of strong passwords, the protection of passwords, and the frequency of change, and defining responsibility of password.

1. **Scope**

This policy applies to all the users in the <Company Name>, including temporary users, visitors with temporary access to services with limited or unlimited access time.

1. **Policy**
2. All passwords are to be treated as sensitive and confidential information.
3. Any system that handles valuable information must be protected with a password-based access control system.
4. Every user must have a separate, private identity for accessing IT network services.
5. Identities should be centrally created and managed.
6. Each identity must have a strong, private, alphanumeric password to be able to access any service. They should be as least [XX] characters long.
7. Each regular user may use the same password for no more than [XX] days and no less than [XX] days. The same password may not be used again for at least one year.
8. Password for some special identities will not expire. In those cases, password must be at least [XX] characters long.
9. Use of administrative credentials for non-administrative work is discouraged. IT administrators must have two set of credentials: one for administrative work and the other for common work.
10. Sharing of passwords is forbidden. Password should not be revealed or exposed to public sight.
11. All passwords will be governed by password lock-out control (XX Times) where possible.
12. Whenever a password is deemed to have been compromised, it must be changed immediately and information security team must be informed, immediately.
13. For critical applications, digital certificates (encryption) and multiple factor authentication using smart cards should be used whenever possible.
14. Information Asset, which is digital, must be locked if password guessing is suspected on the account.
15. All users must not use “Remember Password” features, it should be manually changed.
16. Password shall not be stored in any insecure location (e.g. purse, wallet).

## **4.1 General**

* All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
* All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
* 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.
* Passwords must not be inserted into email messages or other forms of electronic communication.
* Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
* All user-level and system-level passwords must conform to the guidelines described below.

## **4.2 Use of passwords for remote access users**

Access to the Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase

## **4.3 Passphrases**

* Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.
* Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks.

## **4.4 Application Development Standards**

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

• should support authentication of individual users, not groups.

• should not store passwords in clear text or in any easily reversible form.

• should 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

## **4.5 Storing Passwords**

* Employees must refrain from writing passwords down and keeping them at their workstations.
* Employees are encouraged to use password managers but should discuss with the SLT or IT support to agree suitability of chosen application and best use practices

# Guidelines

Passwords are used for various purposes at. Some of the more common uses include user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

• The password contains less than eight characters

• The password is a word found in a dictionary (English or foreign)

• The password is a common usage word such as:

* Names of family, pets, friends, co-workers, fantasy characters, etc.
* Computer terms and names, commands, sites, companies, hardware, software.
* The words "<Company name>", "sanjose", "sanfran" or any derivation.
* Birthdays and other personal information such as addresses and phone numbers.
* Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc. Any of these spelled backwards.

Strong passwords have the following characteristics:

• Contain both upper- and lower-case characters (e.g., a-z, A-Z)

• Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&\*()\_+|~- )

• Are at least eight alphanumeric characters long.

• Are not a word in any language, slang, dialect, jargon, etc.

• Are not based on personal information, names of family, etc.

# Security controls

* To protect against ‘brute-force’ attacks all internet-facing services will have lock-out mechanisms to deter repeated attempts to guess account details. These mechanisms will ensure that the account is suspended under such conditions. All <Company name> IT systems will be configured to ensure that passwords can only be transmitted in an encrypted format to reduce the risk of compromise via interception. Any passwords stored by the company will be in an encrypted format that includes ‘password salting1’ to ensure that actual passwords cannot be recovered from the stored hashes.
* The IT Service Desk will never ask for full details of your password or other security credentials (unless you have self-initiated a password reset with the Service Desk), and therefore you should never provide these either over the phone or in an email message

# Enforcement

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