SIDDHARTHA COMMODITIES PRIVATE LIMITED

REGD. OFFICE: C-73, ADARSH NAGAR, NEAR ADARSH NAGAR POLICE
STATION, JAIPUR, RAJASTHAN-302004CIN: U51109RJ2004PTC019795
Email Id: siddharthacommodities.com, Tel.: 0141-4911811

Password Policy & Procedure

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 the compromise of Siddhartha Commodities Pvt.Ltd'sentire corporate network. As such, all Siddhartha Commodities Pvt.Ltd. employees (including contractors and vendors with access to Siddhartha Commodities Pvt.Ltd. systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for 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 Siddhartha Commodities Pvt.Ltd. facility, has access to the Siddhartha Commodities Pvt.Ltd. Global network, or stores any non-public Siddhartha Commodities Pvt.Ltd. Global information.

Policy

General

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
- Account must be locked upon a minimum of 3 failed logon attempts or a maximum of 5 failed logon attempts.
- A minimum of 3 previous passwords should be remembered and cannot be reused.
- For the password history to be effective, the user should not be allowed to change password more than once within the same day, i.e. enforce a minimum password age of 1 day or more.
- Systems should not provide information on the cause of unsuccessful logins (e.g. identifying which portion of login credentials was correct).
- Upon new installation, all default passwords must be changed immediately.
- 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.

Guidelines

General Password Construction Guidelines

Passwords are used for various purposes at Siddhartha Commodities Pvt. Ltd. Some of the more common uses include: user level accounts, web application accounts, email accounts, screen saver protection, voicemail password, and local network equipment 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 ten characters
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 " Siddhartha Commodities Pvt.Ltd ", "fsm" 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 the above spelled backwards.
Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

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 **ten** alphanumeric characters long.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

Password Protection Standards

Do not use the same password for Siddhartha Commodities Pvt. Ltd. accounts as for other non- Siddhartha Commodities Pvt. Ltd. access (e.g., personal ISP account, trading platforms, benefits, etc.). Where possible, do not use the same password for various Siddhartha Commodities Pvt.Ltd. access needs. For example, select one password for the Accounting systems and a separate password for IT systems. Also, select a separate password to be used for a Windows account and a UNIX account.

Do not share Siddhartha Commodities Pvt.Ltd. passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Siddhartha Commodities Pvt.Ltd. information.

Here is a list of "DONT'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 supervisor/manager
- Don't 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 co-workers while on vacation

If someone demands a password, refer them to this document or have them call to Tech Risk.

Do not use the "Remember Password" feature of applications and browser.

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including personal portable devices) without encryption.

Change passwords at least once every three months.

If an account or password is suspected to have been compromised, report the incident to IT Department and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by IT Department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Application Development Standards

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

- should support authentication of individual users or groups.
- should not store or transmit passwords in clear text or in any easily reversible form. (Applicable to Investment Accounts and admin systems) 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.

Passwords Implementation

User and administrator account

- You will be prompted to change password every 3 months.
- Password must have a minimum length of 10 characters.
- Password must have characters from 3 of the following 4 categories - uppercase, lowercase, numbers, special characters (Eg. @, #, $).
- Password must not contain login username.
- 10 previous passwords would be remembered, and cannot be used.
- 5 failed logon attempts are allowed before account is locked for 30 mins.

Service account

Service accounts are used to perform automated tasks that require privileges atypical to a normal account. As no user interaction is required, such accounts should have stricter password policy to prevent unwanted access to such privileged accounts.

On top of the General Password Construction Guidelines above, the service account password should:

- 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, !@#$%^&*()_+|~-
- =\`{}[]:";'<>?,./) Be at least twenty-five (25) alphanumeric characters long. (Based on industry best
- practice) Never be written down or stored privately.
- No account lockout will be set to prevent service distruption.
- Be set with 2 year password expiry.

Service account should:

- Serve one purpose only, every service account should not be shared for other purpose. (e.g. endpoint management portal and anti-virus)
- The credential should enrol and manage by Privilege Access Management solution.

Considering the stricter password policy for the service account, and IT Security Operations department is monitoring for failed login attempts and account brute force attacks; therefore, the password expiry period is set at 5 years or detection of suspicious login.

After an internal risk and benefits assessment, the Management has given an exception to database service accounts. Rotating the database service account or schema password might cause application malfunction and the worse scenario is system downtime, factor in the likelihood of accessing the database via a compromised credential is very low with various preventive controls in place.

The Company implemented these preventive controls in multiple-layered, from network access control, such as network segmentation, VLAN restriction, network firewall, network IDS/IPS, data-in-transit encryption; to the user access control, access granted is at least-privileged and need-to-know principle; and various detection and monitoring process.

5.0 Application ID Password Reset Procedure

- This procedure applies when a permanent, contract or temporary staff has forgotten the password and wishes to request for a new one.
- When a permanent, contract, temporary staff or a trainee’s Tradeworks ID has become dormant as a result of not logging in for a continuously of 90 days (applicable to SG and MY) and wishes to unlock and reset the password.

- For validation purpose, staff will need to be physically present at the IT administrator or HR desk, phone HR to request for the password to be reset or send an email to HR for password reset.
- Staff will need to change the password immediately upon issue of a new password by IT administrator or HR.

6.0 Enforcement

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

7.0 Exception

To prevent default privileged user accounts from being locked out and leading to unavailability of the systems; all default privileged accounts (a.k.a. root accounts) are exempted from lockout configuration requirements.

Default privileged accounts (a.k.a. root accounts) and service accounts (a.k.a. system accounts) on Servers including Oracle database shall be controlled via CyberArk. CyberArk passwords shall follow the password strength settings but the other recommended baseline settings.

Oracle default profile shall be assigned to default privileged accounts and service accounts only.