PASSWORD POLICY

For

Sundarlal Sawji Urban Co-operative Bank Ltd

PASSWORD POLICY

I. 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 **Sundarlal Sawji Urban Co-operative Bank Ltd.** (herein referred to as “Bank”) entire network. As such, all Bank employees (including contractors and vendors with access to Bank systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

II. PURPOSE

Identification and authentication access controls play an important role in helping to protect Information Systems. The purpose of this policy is to protect Information Systems by defining requirements for new passwords and changes to passwords.

III. SCOPE

This policy applies to all **Sundarlal Sawji Urban Co-operative Bank Ltd.** staff that utilize Information Systems with IDs and passwords (credentials). This policy applies whether Staff is using **Sundarlal Sawji Urban Co-operative Bank Ltd.** Information Systems, Staff owned devices for Company approved work, or Staff use Information Systems of third party service providers for work related activities.

IV. POLICY

The Chief Security Officer (CSO) shall ensure:

- Policies and procedures manage the process of creating, changing, and safeguarding passwords/phrases
- Policies and procedures prevent staff from sharing passwords/phrases with others.
- Procedures advise staff to commit their passwords/phrases to memory and not allow them to be written down.
- Policies and procedures govern the password/phrase change frequency.
- Policies and procedures dictate when passwords/phrases must be supplemented with additional access controls such as tokens and biometric.

This Policy applies to all **Sundarlal Sawji Urban Co-operative Bank Ltd.** related authentication activities including, but not limited to, the following:

- Administrator accounts.
- User accounts.
- Network infrastructure devices (e.g. firewalls, routers, wireless access points, etc.).
- Third party service providers.
- Web applications.
- Screen savers.
- Mobile devices.

A. NEW USER ACCOUNTS

When granting access for a new user/account:

- System administrators will establish a unique ID and unique password/phrase.
- The user password will be conveyed to the user in a secure manner.
- When the user logs on for the first time, the user will be required to change their initial password/phrase to something that meets the requirements of this policy.

B. SELECTING PASSWORDS/PHRASES

Phrases are not the same as passwords. A phrase is a longer version of a password and is typically composed of multiple words. By converting some letters to numbers and special characters the phrase is even more secure.

When selecting a new password/phase, system administrators and users must select passwords/phrases that are long, strong, and complex. Where possible, Staff shall choose passwords/phrases that meet the following requirements:

- Contain both upper and lower case characters (e.g., a-z, A-Z).
- Include both numbers (0-9) and special characters (e.g. @, #, $, *).
- Have a minimum of at least 10 characters and preferably 15 characters long and is a phrase.
- Where possible, use different passwords/phrases for general office activities (e.g. e-mail, file access) vs. systems that store sensitive or confidential data.

- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Staff should not choose passwords/phrases that:

- Include common words such as those found in a dictionary.
- Are the same as passwords/phrases used on Staff personal accounts (e.g. personal e-mail, on-line banking, or social media).
- Contain personal information such as a spouse or pet's name, social security number, driver's license number, street address, phone number, etc.
- Contain sequences or repeated characters. For example, 1234, 3333, etc.
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware,
- Software.
- The words "Data Center", "msb", “dc" or any derivation.
- Birthdays and other personal information such as addresses and Phone Numbers.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret) .

Staff with special system privileges, assigned by a transaction, program, process, or group membership, should select a unique password/phrase from other accounts held by that individual.

C. PASSWORD/PHRASE GUIDELINES

Staff shall following security guidelines to ensure passwords/phrases are not compromised. Security training and awareness programs shall ensure Staff is:

- Educated on security related risks.
- Reminded of security requirements when selecting and protecting passwords/phrases.
- Educated not to select the "Remember Me" or “Remember Password” feature in web applications and browsers.
- Reminded to be careful when using social media so the password/phrase is not compromised.

Passwords/phrases must not be:

- Revealed to anyone.
- Stored, written down, or transmitted in clear (unencrypted) text.
- Inserted into unencrypted e-mail messages or other forms of electronic communications.

If a Staff member believes that their password/phrase has been compromised or made available to others, the Staff member must immediately change their password and notify IT security Staff.

If someone demands a password, refer them to this policy or have them contact the IT Department.

D. Password/Phrase Changes

Passwords/phrases must be changed on a regular basis according to the following schedule:

- All administrator passwords/phrases must be changed at least every 30 days.
- All user passwords/phrases must be changed at least every 90 days.

When selecting a new password/phrase, Staff shall not repeat any of their prior five passwords/phrases.

E. Software Applications

Application developers must ensure programs contain the following security precautions:

- Applications must require each user to have their own unique ID (e.g. not shared, no user groups).
- Passwords/phrases and Sensitive Information must be protected using strong encryption.
- Passwords/phrases and Sensitive Information must not be transmitted or stored in clear text.
- Ensure applications timeout and require the user to enter a password/phrase after a period of inactivity.

Password Protection Standards

- Don't reveal a password
  - over the phone to ANYONE
  - in an email message

  - to the boss
  - to co-workers while on vacation.
  - on questionnaires or security forms
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")

V. ENFORCEMENT

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination as per IT Act 2000 and Amendments, Data protection Act and other subordinating clauses.

VI. DISTRIBUTION

This policy is to be distributed to all Staff members of **Sundarlal Sawji Urban Co-operative Bank Ltd.**