PASSWORD CONFIGURATION

MINIMUM BASELINE SECURITY STANDARDS

INFORMATION TECHNOLOGY AND COMMUNICATIONS DEPARTMENT

Revision History

Name & Designation	Date	Description of Change	Version
Marcel D. Cabrera, IT Security Officer	02/24/2021	Original	1.0
Information Technology and Communications Steering Committee (ITCSC)	11/16/2022	Approval	
Board of Directors	11/23/2022	Approval	
Jake C. Jaen IT Security Administrator	11/11/2025	Amendment	1.1
Information Technology and Communications Steering Committee (ITCSC)	11/20/2025	Approval	
Board of Directors	12/16/2025	Approval	

I. OBJECTIVE

This document sets the Minimum Baseline Security Standards of the Bank for Password Configuration. It is important all connections into Information Systems are authorized, properly managed, and secured. Also, to educate all users of systems and applications on the characteristic of a Complex/Strong Password and on how to securely maintain and manage passwords.

II. SCOPE

This guideline applies to all users (i.e., Bank employees, temporaries, consultants, and third-parties) whether you are an end user or a system administrator having a username and password to at least one system or application.

III. RESPONSIBILITIES

IT Security Administration Unit Head
Formulate Password Configuration Minimum Baseline Security Standards to provide guidelines on how to securely maintain and manage complex/strong passwords.

IT Security Staff
Ensure that the guidelines defined by the IT Security Administration Unit Head are fully implemented and monitored. They shall handle all technical issues with regard to password configuration.

Chief Information Officer (CIO)/IT Head
Sr. Management
Information Technology and Communication Steering Committee (ITCSC)
Board of Directors (BOD)
Shall review and approve the guidelines formulated by the IT Security Administration Unit Head.

All Employees of the Bank
They must abide with the Password Configuration guidelines set herein to ensure a secure network for CSBank.

IV. STANDARD POLICY

Creating a Complex/Strong Password	
Complex Password ***should -***	✓ All passwords must have at least eight (8) characters. ✓ Must contain both upper and lowercase alphabetic characters. (e.g. A-Z, a-z) ✓ Must contain at least one numerical character (e.g. 0-9) ✓ Must contain at least one special character (e.g. ~!@#$%^&*()_-+=)
Complex Password ***should not -***	✓ Spell a word or series of words that can be found in a standard dictionary. ✓ Spell a word with a number added to the beginning and the end. ✓ Must not based on any personal information such as user id, family name, car plate number, pet, birthday, etc. ✓ Must not employ passwords like "CSB1Jan" in January, "CSB1Feb" in February. ✓ Must not construct passwords that are identical or substantially similar to password that they had previously employed.

**A Complex Password is defined as a password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software.*

Maintaining your User ID and Password
Do not share your Password with Anyone for any reason.
Change your Password upon indication of compromise.
Avoid reusing a Password.
Avoid using the same Password for multiple accounts.
Do not write down, display, printing your Password or store it in an insecure manner.

Do not store Password in easily reversible form.
Consider using a Passphrase instead of Password.
Do not use Automatic logon functionality.
User must Logout properly before leaving their computer.
Avoid storing passwords in browsers such as Chrome, Edge, Firefox, Safari, and etc. or clicking "Save Password" when prompted.
Super admin credentials must be stored in a secure vault to ensure that access credentials are protected, monitored, and only available to authorized personnel under strict access controls.

Provisioning and Support to User Accounts
Enforce Complex/Strong Password.
Require a change of initial "first-time" Password.
Force expiration of initial or "first-time" Passwords.
Periodic Forced Password Changes after (60) days.
Limit on Consecutive Unsuccessful Attempts to Enter Password.
Requisition Required for All Users Forgetting Passwords.
Always verify a user's identity before resetting a Password.
Do not allow Password to be transmitted in plain-text.
Unknown User ID's must not be assigned to users.

Automatic Log-off Process after (15) minutes, if there has been no activity on computer terminal.
Implement Automated notification of a Password change or reset.
Changing Vendor Default Passwords.
Administrator's Password Common to all Workstations, to avoid problems and delays during set-up of devices and applications.