PASSWORD POLICY

KEYNOTE FINANCIAL SERVICES LIMITED

K E Y N O T E

(DATE)

31ST JANUARY 2025

Author:	MD(Designation)

Owner:	MD(Name)
Organization:	KFSL
Version No:	1.0
Date:	(Date)

Document Control

Document Title **Password Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	(Date)	MD(Name)	NA

Approvals

Name	Title	Date of Approval	Version No
MD(Name)	Password Policy	(Date)	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	(Date)	NA

1. PASSWORD POLICY

1.1 PURPOSE

The purpose of this policy is to provide best practices for creating strong passwords.

1.2 SCOPE

This guideline applies to employees, interns, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

1.3 POLICY STATEMENTS

PASSWORD CONSTRUCTION GUIDELINES

- Have minimum length of eight characters
- Must contain of alphanumeric characters
- Contain both upper- and lower-case alphabets
- Contain at least one numeric character (for example, 0-9)
- Contain at least one special character (for example,$%^&*()_+|~-=\`{}[]:";'<>?,/)
- Password should not be same as user ID
- Should not contain dictionary-based words or proper names, including foreign language, or exist in a language slang, dialect, or jargon
- Should not contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters
- Should not contain characters in sequential patterns such as aaabbb, qwerty, zyxwvuts, or 123321
- Should expire within maximum of 60 days
- Should maintain password history of last 10 passwords to restrict reuse of older passwords
- Should not be transmitted in clear or plain text
- Should not be written down in book, sticky notes or saved in notepad or excel files
- Interactive logon: Should prompt user to change password before expiration to five days. When their password expiration date is five or fewer days away, users will see a dialog box each time that they log on to the domain.

PASSWORD DELETION GUIDELINES

All user accounts and passwords that are no longer needed, must be deleted or disabled immediately. This includes, but not limited to:

- User retires, quits or dismissed from his service
- Default password should be changed immediately on all systems
- Contractor's account should be disabled immediately after their service is no longer needed

PASSWORD PROTECTION GUIDELINES

- Do not use your user ID as password
- Do not share your password with anyone, including your manager, administrative assistant, or secretary
- Do not share your password over phone to anyone
- Do not reveal password in an email message
- Do not talk about password in front of others
- Do not hint at format of password (e.g., "My Pet Name")
- Do not share your password with colleague while on vacation
- Do not use "Remember Password" feature of browsers or any other applications

If someone demands to share password, refer them to this document or ask them to call IT Security Head.

If an account or password is suspected to be compromised, report this incident to Head of Department, Head of IT or Head of IT Security & Governance.