# PASSWORD SECURITY

1. Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.

2. Change passwords at least once in 30 days.

3. Use Multi-Factor Authentication, wherever available

4. Don't use the same password in multiple services/websites/apps.

5. Don't Save passwords in the browser or in any unprotected documents.

6. Don't share system passwords or printer pass code or Wi-Fi passwords with any unauthorized persoNS.

7. Common password such as admin@ 123, Password, admin or which contain words such as unit name, room no, telephone, mobile or other things which is generally known to other colleagues must be avoided.