Password Policy

1. Purpose

1.1. The main purpose of this policy is to have a standard password system in place to ensure the security of confidential official data. Effective implementation of the Password Policy will minimize risk from password cracking or guessing and ensure the Confidentiality, Integrity and Availability of data.

2. Scope

2.1. This policy applies to all users who have access to computer systems and confidential data.

3. Policy

3.1. All users should be responsible for managing the passwords of their systems.

3.2. Users should change their default password allotted by the administrator, on their first log-in.

3.3. The password should be alphanumeric and should have punctuation characters as well as letters, for example the following characters can be used along with letters: 0-9,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

3.4. The complexity of the password should vary with the level of Information that it is used to protect.

3.5. The length of the password should be minimum (6) characters and not more than (12) characters.

3.6. The password should be changed every 14 days and must be different from previous 3 passwords.

3.7. The password should not be disclosed to any other person either over the phone, mail or any other medium.

3.8. The “remember password” feature present in applications should not be used.

3.9. As good practice passwords for official mail account and non-official mail personal accounts should be different.

3.10. If you enter an erroneous password on 3 consecutive occasions, your account will get locked.

3.11. Reset of password shall set the password to a default password

3.12. User shall not be allowed to set the default password as new password