Password Security & Control

Table Of Contents

1.1 Policy Statement

All information system resources of company must have appropriate password controls in place to protect assets from unauthorised or illegal access. The password controls must be automated using system features and parameters wherever possible.

1.2 Scope

This Policy and the associated Procedures apply to all the IT users of company and any individuals/groups using the information systems resources of company. This includes contractors, consultants, third-party associates and any temporary employees and covers passwords at the Network, Database, Operating System and Application levels.

1.3 Execution Responsibility

The Administrator-Systems is responsible for implementing the procedures mentioned in this chapter. It is the responsibility of all IT users to adhere to the policy for password security. The overall execution & monitoring of procedures is the responsibility of CISO.

1.4 Detailed Procedures

1.4.1.1 Password Management

1.4.1.2 Confidentiality of Passwords

All User (normal users, administrators) passwords must remain confidential and not shared, posted or otherwise divulged in any manner.

1.4.1.3 Password Composition

Passwords must consist of at least eight characters. The passwords selected must be combination of alphanumeric characters along with special characters wherever the system supports. The passwords must not contain the user's name, user-ID, spouse/child’s name or words appearing in dictionary.

1.4.1.4 Password Expiration

Passwords must expire after a maximum period of 30 calendar days. The same password should not be repeated within a cycle of 10 password changes.

1.4.1.5 One Time Use of Initial Passwords

An initial password must be provided to the users & the system must be configured to force the users to change the initial password immediately after the first logon.

1.4.1.6 User Capability to Select Passwords

Users must be provided with the capability to change their password on the login interface (after authentication).

1.4.1.7 Password Reset

User password resets will be performed only on request of the user, after verification of the users identity. The ‘Password Reset Request’ form must be filled up by the user (Refer Annexure 7A-Password Reset Request). The new password must be a one-time password. Only the individual to whom the user-ID is assigned must request for user password reset. The Head-Infrastructure must be informed whenever a password is reset for a particular user.

1.4.1.8 Protection of Transmitted Passwords

- Details in relation to user ID, Password etc. should not be sent using clear text across mail systems.
- The user-ID and password must be authenticated as a whole. Authentication failure must provide an error message to the user that does not indicate whether the user ID or password is incorrect (e.g. "incorrect login" and not "incorrect password").

1.4.1.9 Super User Passwords

- All the privileged user passwords for Operating Systems, Databases, Applications, Network Equipment like routers, switches etc., must be sealed in an envelope and kept in a fire proof safe. This is necessary in case the password is forgotten or the related person has left the organization without surrendering the passwords.
- These sealed envelopes must be opened with the written permission of Head-Infrastructure and the password should be changed immediately and kept in a new sealed envelope. Details of such activity should be entered in the Sealed Envelope Maintenance Log Book (Refer Annexure 7B-Sealed Envelope Maintenance Register)

1.4.1.10 Screen Saver Password

Every user must enable the screen saver with password, which must be activated after 3 minutes of inactivity.

1.4.1.10 Power-on Password

Users must be encouraged to use the power-on passwords. Sharing of power-on passwords to be allowed only if multiple users need to access the same physical system and the passwords should be maintained solely within the members of the group sharing the system. The power-on passwords should be subject to the same controls as personal passwords.

1.4.1.11 Account Lockout

Three successive failures must result in a user’s account being locked out. The users will not be able to login until the account is unlocked and the password reset. The user should submit a formal request to the Assistant Manager-IT to carry out the exercise. (Refer Annexure 7A- Password Reset Request)

1.4.2 Password Best Practices

1.4.2.1 Where the software permits

- Files containing passwords should be encrypted one-way
- Initial passwords, issued must be valid for one logon only
- The software must enforce a password change following the initial logon.

1.4.2.2 Disabling Default Passwords

Vendor Supplied User-IDs/Passwords, encryption keys, and other access codes included with vendor-supplied systems must be changed. Default passwords shipped with software must be disabled or changed.

1.4.2.3 Prohibition of Group Passwords

Group passwords must not be allowed to the extent possible so that individual accountability is maintained. Where used, they must be maintained solely within the members of the group, and should be subject to the same controls as personal passwords.

1.4.2.4 Specific password policies

Policy must be implemented for reporting the “password strength” and the password strength or weaknesses should be analyzed for the following:

- The minimum length of password is 8.
- The password is not the same as the user’s name and ID.
- The password is not equal to any user’s name on the system.
- The password is alphanumeric with special characters
- Create word list with common local words of company related terminology and check if these passwords are given.

1.4.3 Password Selection Rules

Passwords should not be based on any of the following:

- Months of the year, days of the week or any other aspect of the date
- Family names, initials or car registration numbers
- Company names, identifiers or references
- Telephone numbers or similar all-numeric groups
- User ID, user name, group ID or other system identifier
- More than two consecutive identical characters
- All-number or all-alphabetic groups

Annexure 1A-Password Reset Request

Password Reset Request

ACCOUNT UNLOCKING / PASSWORD RESET FORM

Name of user/ Emp ID

Login-ID

Server/Application:

Reason for request :

□ Account Locked Out

□ Password Forgotten

□ Other (Please specify)

Requestor's Signature: ______________________ Date: __________

FOR USE BY INFRASTRUCTURE TEAM

User request processed Yes / No

Account Unlocked / Password reset by

Signature

Date

Annexure 2B-Sealed Envelop Maintenance Register

Sealed Envelop Maintenance Register

Date of sealing/opening of envelope	Reason	Opened/ Sealed by	Signature	Approved by (CISO)	Approved by (Head-Infrastructure)