Password Policy

- Password standards, like alphanumeric, minimum and, maximum length of characters are well enforced by system.
- Password expiry after fifteen day period is enforced.
- Password histories are maintained so that the user cannot reuse the previous six passwords.
- Password is masked at the time of entry.
- Passwords are stored in encrypted format in the database.
- Creation of new password is mandated by the system when the user logs in for the first time.
- Account disabled after three unsuccessful entries.
- Password can be unlocked by request on authorised mail.
- System controls are present to ensure login ID & passwords are not same. System is configured to reject such request.
- Password should not be stored on computers.
- Password should be shared.
- Password should not a person's name, birthdates or any object name.
- All successful and filled login attempts should be logged with details like IP address, mail address and other data to unable traceability.
- System controls to ensure that the Password is encrypted at members end so that employees of the member cannot view the same at any point of time.