Implement passwords policy

- Strictly use strong passwords with minimum 8 characters comprised of alpha numerical and special characters, as was described in section 6.3;
- Users should have different passwords for different accounts;
- All default passwords must be changed upon installation of new software or new Operating System (OS);
- Failed login attempts should be limited to three times and then lock the user;
- Account lockout duration should be at minimum 20 minutes at maximum 1hour.
- A two-factor authentication should be set up for critical applications and/or systems.

Revision #1
Created 1 October 2025 11:00:20 by RISA
Updated 1 October 2025 11:01:34 by RISA