Passwords Protection

- Users shall have different passwords for different accounts.
- All default passwords shall be changed upon installation of new software or new Operating System (OS).
- Passwords shall be securely hashed and stored. Never store plain text passwords, and use strong, industry-standard encryption algorithms.
- Failed login attempts shall be logged and limited to three times and then lock the user.
- Account lockout duration shall be a minimum of 20 minutes to a maximum of 1 hour.
- A two-factor authentication shall be set up for critical applications and/or systems.

Revision #2
Created 11 July 2025 15:33:48 by RISA
Updated 11 July 2025 18:27:54 by RISA