Implement secure authentication user account controls to secure data integrity and transmission

1. Enforce strong password policies that require complex passwords, regular password changes and avoid easily guessable passwords.
2. Monitor user activity to detect suspicious behavior, such as unauthorized access attempts, unusual access patterns, or changes to critical system configurations. This can identify potential breaches early on.
3. Maintain up-to-date software, including operating systems, applications, and security patches, to address vulnerabilities that could be exploited by attackers. Prompt patching minimizes the window of opportunity for exploiting known weaknesses.
4. Implement additional verification factors beyond just a password, such as one-time passcodes, security tokens, or biometric authentication.
5. Implement policies that automatically lock out accounts after a certain number of failed login attempts. This prevents brute-force attacks and limits the potential damage from compromised credentials.