Protect: Minimum Password Strength

COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

2.B: Does the WWS require a minimum length for passwords?

Recommendation: Implement a minimum length requirement for passwords. Implementation can be through a policy and/or administrative controls set in the system.

Why is this control important?

Using short passwords at a WWS is a significant security risk, as passwords play a vital role in preventing attackers from gaining access to users' accounts. Attackers use programs to guess user passwords, and a longer and more complex password is harder for an attacker to crack. Enforce password length, complexity (e.g., using upper- and lower-case letters), and ensure users are following best practices for password security (e.g., no sticky notes with reminders stuck on monitors).

Implementation Tips

Create a policy or set administrative controls that mandate a minimum password length (15 or more characters is recommended) for all password-protected OT and IT assets as feasible.

For Windows-based OT and IT assets, depending on the version of Windows, the System Administrator can use the Local Security Policy to set a minimum length for passwords. To access this feature, type "Local Security Policy" in the search box in the Start menu and click on the Local Security Policy App. Once the menu pane opens, click on "Account Policies" and then "Password Policy" to adjust password length.

Additional Guidance

- ✓ In instances where minimum password lengths are not feasible, use compensating security controls (e.g., utilizing a single sign-on) and record all login attempts. Also, if computer assets cannot support longer passwords, prioritize them for upgrade or replacement.
- ✓ Utilize longer passwords or phrases as a password (e.g., "Iliketoeatapplesandbananas").

If a WWS utilizes a Microsoft Domain with many systems and user accounts are connected to a single domain, it can manage these settings using Group Policy Objects (GPOs). The System Administrator can configure the Password Policy settings in the following location in the Group Policy Management Console: Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy. The Microsoft Windows Password Policy Settings Reference linked below provides additional details.

For all other passwords on non-Windows-based assets, the Administrator should review existing passwords to ensure they meet the password policy where possible. These assets may include network hardware (e.g., network switches, wireless access points, network routers); communications assets (e.g., radios); OT assets (e.g., PLCs and HMIs); and software applications that use passwords to authenticate users.

`

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: Provides a proactive and systemic approach to develop and make available a comprehensive set of safeguarding measures for all types of computing platforms. See control AC-1 (page 39) for more information on "Access Control Policy and Procedures". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

NIST Policy Template Guide: See Identification and Authentication Policy (4.m) Authenticator Management. A policy document that addresses the requirements for minimum length for passwords. *https://www.cisecurity.org/wp-content/uploads/2020/06/Identification-and-Authentication-Policy.docx*

Password Guidance from NIST: NIST created a short video explaining password protection and guidance on implementing best practices. *https://www.nist.gov/video/password-guidance-nist-0*

CIS Control Password Policy Guide: The Center for Internet Security (CIS) provides a detailed breakdown of how to create and implement a password policy, specifics on password length start on page 7. *https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide*

CISA Security Tip (ST04-002): The U.S. Department of Homeland Security offers tips for effective passwords. *https://www.cisa.gov/uscert/ncas/tips/ST04-002*

Microsoft Windows Password Policy Settings Reference: This page describes how to configure password policy settings on Windows systems. *https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy*