Helios Password Policy Update Guidelines

Effective Immediately!

Password Complexity
All new or modified accounts require updates to meet the new password complexity requirements outlined below.

- Characters allowed: Alphanumeric characters and symbols in the set ['*', '!', '#', '_', '$'].
- The password must be at least 10 characters.
- The password cannot be any of the previous three passwords used.
- The password must contain at least one capital letter, one numeric character, and one special character from the given set.
- The password must be changed every 180 days.

Process
All Account Modification Forms should follow the process below to ensure compliance with this policy.

1. Submit a screenshot of the GPO settings aligning to the requirements outlined above.
2. Enable the **User must change password at next logon** option.
    - For Active Directory accounts, use **dsa.msc** to access this option.
    - For local user accounts, use **lusermgr.msc** to access this option.
3. Attempt a logon as the user using a noncompliant password and submit a screenshot of the error message received as a result of this noncompliant password.