Security Policy

Background: Security policy should be established at the top (corporate) level for easy maintenance. Sites may then modify the inherited security policy to align with their facility's electronic security policy.

Notice: If your facility is utilizing Single Sign on capabilities this Quick Guide is not applicable to you.

This functionality may not be available to all users. Contact your system administrator if you have additional questions.

To Do and Notice:

1. Navigate to and click on **Administration**
2. Navigate to **Facility Information** and select **Edit Security Policy.**
3. Select the desired Facility from the **Selected Facility** drop-down list.
4. At **Security Policy,** select **Use Native Settings** from the drop-down list.
5. Enter the appropriate number for each of the following areas (according to your Corporate/Facility policy):
    - Idle Timeout Minutes
    - Minimum password length
    - Minimum digit characters in password
    - Minimum special characters in password (e.g., !, @, #, $)
    - Both upper and lower case required (checkbox)
    - Maximum password age
    - Age reminder days
    - Lockout user after login failures (checkbox)
        - After how many?
        - For how long? (drop-down list)
6. Click **Save.**
7. Click **Done.**

So What? You can utilize these settings to help enforce your corporate electronic security policy within HST BOH.