 

**ACCOUNTS CONFIGURATION SETTINGS**

|  |  |  |  |
| --- | --- | --- | --- |
| **Password Parameter Setting** | **Quanta Standard** | **Disclose To Users?** | **Rationale for Standard** |
| 1. Maximum Age (Days) | 90 | Yes | Generally Accepted Standard. |
| 2. Minimum Age (Days) | 0 | No | To discourage Users from repeatedly changing their Password to quickly cycle through Retained History to get back to the same (desired) Password. If there becomes a known Security Threat to the User's Login Account, then the User may contact a System Administrator to have their Password "reset". |
| 3. Minimum Length | 12 | Yes | Generally Accepted Standard. |
| 4. Retained History (Prior Instances) | 24 | No | System "Remembers" the User’s twenty-four (24) previous Passwords so that they may not be re-used. |
| 5. Must meet Complexity Requirements? | Yes (Enabled) | Yes | Password must contain at least one character from at least three of the following four categories:   * English Uppercase Characters (A -Z) * English Lowercase Characters (a -z) * Numeric Digits (0 - 9) * Non-Alpha-Numeric (! $, #, or %) |
| 6. Store Passwords using Reverse- Encryption? | No (Disabled) | Yes | A User's Password should be known only to the User. Reverse Encryption would enable the User's existing Password to become known to System Administrators, which potentially undermines the User's 100% Accountability for all activity that occurs under their Login Account. |
| 7. Account Lockout Threshold (# of Unsuccessful | 16 | Yes | Generally Accepted Standard. A System *I* Application Administrator would have to be contacted to "Reset" the  User's Password. This setting was realigned from 8 to 16 in light of vendor guidance on acceptable controls. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Password Parameter Setting** | **Quanta Standard** | **Disclose To Users?** | **Rationale for Standard** |
| 8. Account Lockout Duration (Minutes) | 0-forever | Yes | If the User becomes Locked Out, a System *I* Application Administrator would have to be contacted to “Reset" the User's Password. In this way, an Administrator could quickly become aware of potential intrusion attempts, thus eliminating the requirement of "Logging Failed Login Attempts" and then having to periodically review such Logs. |
| 9. Reset Lockout Counter (Minutes) | 360  minutes | No | This is the Maximum Setting Value that may be associated with this Parameter. 60 MPH x 24 HPD=1,440 MPD. Therefore, 99,999 Minutes=Approximately 69  Days. This Counter Controls the minimum duration between Successful Logins that the Account Lockout Threshold (Item- 7 above) is maintained in protecting against Invalid Login Attempts. |

`