|  |  |  |
| --- | --- | --- |
| **Question** | **FINDING** | **Proposed Corrective Action(s)** |
| What is the password policy (length and combination of characters)? | At least 6 characters, with 1 lowercase, 1 uppercase and one numeric character | Incorporate a password policy, based on best practices, that:  • Require a minimum length of at least six (6) characters and  • Contain both numeric and alphabetic characters. |
| How often are passwords changed? | The passwords have expiration dates. This is set by an administrator. | Based on best practices, the password shall change at least every 90 days. |
| Does the application force a password change for “new” users upon first login into the application? | A temporary password is created for every new user, and on first login, the new user is asked to change their password | Based on best practices, the administrator shall provide the user with their credentials and, upon first login, the user shall be forced by the application to change their password. |
| Can the user change their password at any time? | **No** | Based on best practices, the user shall be able to change their password at any time. |
| Can the system administrator enforce password policy and/or complexity such as minimum length, numbers and alphabet requirements, and upper and lower case constraint, etc.? | No. The policy of ‘At least 6 characters, with 1 lowercase, 1 uppercase and one numeric character’ is hard coded in the system | Based on best practices, applications shall provide the system administrator with the ability to define the password policy (complexity, length, etc.). |
| Can the application force password expiration and prevent users from reusing a password? | Yes | Based on best practices, applications shall be able to force password expiration and prevent users from using a password that was used the past 3-4 times. |
| Can the application be set to automatically lock a user’s account after a predetermined number of consecutive unsuccessful logon attempts? | **Currently the user can keep trying without getting locked out of the system** | Based on best practices the application shall enforce account lockout after not more than 5 unsuccessful attempts. |
| Does the application prohibit users from logging into the application on more than one workstation at the same time with the same user ID? | **No, currently the same user can log in to the system from different stations at the same time with the same user ID** | Based on best practices, the application shall prohibit simultaneous logging, from different workstations, with the same credentials. |
| Can the application be set to automatically log a user off the application after a predefined period of inactivity? | **Yes, after a period of inactivity, the user is logged out** | Based on best practices, the application shall automatically log out the user following an inactive period of 15 minutes |
| Capturing data access inquiry activity such as screens viewed and reports printed? | No | Based on best practices, user data access inquiry shall be captured for accountability and compliance and purposes. |
| Capturing data entries, changes, and deletions? | Yes, a traceability log is present which records all the actions performed by the user | Based on best practices, data entry and data edit shall be captured for accountability and compliance and purposes. |
| Can the audit log "data" be exported from the application for further processing? | **Yes, the traceability log can be exported in excel format.** | Based on best practices, there shall be a mechanism in place for extracting log data for investigation purposes. |
|  |  | Based on best practices audit log files shall protected and all changes shall be recorded.  Having access to logs identifying changes, additions, and deletions can help retrace steps made by unauthorized personnel. |
| Which connection method(s) is/are used to accomplish remote support (VPN, VPN with IPSec, etc.)? | **VPN** |  |
| Is the application located in a segregated/isolated network? | Yes, on local network | Based on best practices, applications holding sensitive personal data shall be placed in a network that is properly segmented/isolated from other networks.  The Center is strongly advised to deploy Firewall(s) to properly isolate VLANs hosting systems with sensitive information. |
| Is the system covered by a commercial anti-virus software? Is it updated? | **Yes, McAfee** |  |
| Users shall not be able to stop/pause the anti-virus software | **Yes** |  |
| Are updates to application software and/or the operating system controlled by a mutual agreement between the support vendor and the application owner? | **Yes** |  |
| Are the servers patched/ updated as needed? | Yes |  |
| Is data backed up regularly? How often? Do you perform tests on backups? | Data on storage server is backed up every day, occasionally we perform test |  |