**Requirement 1. Assign all users a unique ID before allowing them to access system components or Customer data.**

**PCI DSS 8.1.1/ ISO**

*Define System Components*

**Requirement 2. Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.**

**PCI DSS 8.1.2/ ISO**

1. Authorizations associated with User IDs.
2. System settings to verify each user ID
3. System settings to verify privileged user ID
4. Are privileges same as specified on the documented approval.

**Requirement 3. Immediately revoke access for any terminated users.**

**PCI DSS 8.1.3/ ISO**

1. Samples of users terminated in the past 6 months – both local and remote access
2. Physical access methods – tokens/ smart cards returned or deactivated

**Requirement 4. Remove/disable inactive user accounts at least every 90 days.**

**PCI DSS 8.1.4/ ISO**

**Requirement 5. Limit repeated access attempts by locking out the user ID after not more than six attempts**

**PCI DSS 8.1.6/ ISO**

1. inspect system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts

**Requirement 6. Once locked out as in the above scenario, it must remain locked for a duration to a minimum of 30 minutes or until an administrator enables the user ID.**

**PCI DSS 8.1.7/ ISO**

**Requirement 7. If a session has been idle for more than 15 minutes, require the user to re authenticate to re-activate the terminal or session.**

**PCI DSS 8.1.8/ ISO**

**Requirement 8. In addition to assigning a unique ID, every user must pass through a proper user-authentication by employing at least one of the following methods to authenticate all users:**

* **Something you know, such as a password or passphrase**
* **Something you have, such as a token device or smart card**
* **Something you are, such as a biometric.**

**PCI DSS 8.2/ ISO**

**8.2.1** Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.

**8.2.2** Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.