DEPARTMENT PROCEDURE FOR STANDARD 8 – Assign a Unique ID to Each Person with Computer Access

Purpose

The purpose for each employee to have a unique ID to access cardholder data systems is to ensure that each employee is responsible and accountable for all actions taken by that employee. Unique ID’s also allow the ability to trace all actions performed by an individual.

Procedure

A. Assignment of Unique ID - Standard 8.1:

1. All users shall be assigned a unique ID to access cardholder data within any component of a system or device.
   a. This documentation shall be maintained and kept by the department.
   b. A copy of this documentation shall be sent to Income Accounting and Student Loan Services annually, or whenever changes are made.

B. Assignment of Unique Authentication - Standard 8.2:

1. All users shall use one or more of the following items to be uniquely authenticated.
   a. Something you know, such as a password or passphrase.
   b. Something you have, such as a token device or smart card.
   c. Something you are.

C. Remote Access Procedure - Standard 8.3:

1. Departments needing to have their systems accessed remotely by their own personnel, or a third party vendor, must use a two factor authentication solution that has two unique items that authenticates the user. Refer to B.1.a, b, or c, above.
   a. Controls should be implemented to allow access to vendors, for a specific period of time, or for a specific event or issue.
D. Additions, Deletions, and Modifications or User IDs, Password Resets, Temporary Passwords, Inactive Users, & Documentation of Understanding of Policies and Procedures - Standard 8.5:

1. Department is responsible to request ID’s and passwords for all new employees, for all systems.
   a. Documentation should be retained by the department for all new ID’s and passwords, which should include the name, ID number, system, access type, and date of the ID request.
   b. All changes or modifications should be listed on the documentation.
   c. For both voluntary and involuntary terminations, access shall be removed immediately.
      i. Documentation should be retained by the department, and should include the name, ID number, system, and date of the termination.
      ii. Confirmation of the removal of access shall be retained by the department.
   d. Departments shall send additions and deletions of user access to the Income Accounting and Student Loan Services department quarterly, or upon request.
   e. Inactive user accounts that are 90 days or more, for any other reason, shall be inactivated and deleted.
   f. Enable vendor ID’s for only the minimum amount of time needed.
   g. Training for the authentication process should be given to all new employees and vendors.
   h. User ID’s and passwords should never be shared. Each person shall have their own ID and password.