Version:	Modified By:	Date:	Approved By:	Date:
1.0	Lisa Zaelit	February 7, 2014	Dan Bowden	February 28, 2014
2.0	Kim Stringham	August 12, 2015	Lisa Zaelit	August 18, 2015
3.0	Stu Schrager	May 14, 2018	Lisa Zaelit	May 16, 2018

DEPARTMENT PROCEDURE FOR STANDARD 7 – Implement Strong Access Control Measures

Purpose

The purpose for strong access control is to ensure that critical data is only accessed by personnel who need to know, and have access to those systems and processes, to perform the duties of their job. This procedure applies to all systems and processes that involve cardholder data. Privileges are determined by the responsibilities of the employee. Role based access determines the least amount of access necessary to perform duties. Any and all system components require access controls.

Procedure

A. Access Controls – Standard 7.1:

1. A list of roles shall be created according to the position and duties of an employee.
   a. Departments shall then assign the level of access to these roles, and maintain documentation of it.
   b. Employees shall only have the least amount of access necessary to perform their duties.

2. For automated systems, access controls should be implemented into the system as soon as they are created.

   a. Every component shall have the required access controls implemented.
   b. Department documentation should reflect dates of creation and implementation of each access control, and all the components that require access control.
   c. It shall also contain the description of the access, which roles need the access, and the positions within the role.
   d. Users should be made aware of what their access is and the required security responsibilities.
   e. Roles for access controls shall be reviewed annually, or when any changes are made.
   f. Proof of review shall be sent annually, or when changes are made, to the Income Accounting and Student Loan Services department.
   g. Approval documentation shall be completed by an authorized party, and maintained within the department.

h. All access control documentation shall be completed and maintained within the department.

3. For manual processes, access controls shall be created prior to the beginning of the process.

    a. Department documentation should reflect dates of creation and implementation of each access control.
    b. It shall also contain the description of the access, which roles need the access, and the positions within the role.
    c. Users should be made aware of what their access is and the required security responsibilities.
    d. Roles for access controls shall be reviewed annually, or when any changes are made.
    e. Proof of review shall be sent annually, or when changes are made, to the Income Accounting and Student Loan Services department.
    f. Approval documentation shall be completed by an authorized party, and maintained within the department.