Version:	Modified By:	Date:	Approved By:	Date:
1.0	Lisa Zaelit	February 7, 2014	Dan Bowden	February 28, 2014
2.0	Kim Stringham	August 14, 2015	Lisa Zaelit	August 20, 2015
3.0	Stu Schrager	May 14, 2018	Lisa Zaelit	May 16, 2018

DEPARTMENT PROCEDURE FOR STANDARD 12 – Maintain an Information Security Policy

Purpose

The purpose of maintaining a strong security policy is to ensure that every employee who handles cardholder data is aware of all PCI policies, and that these employees review these policies annually. Employees need to be aware of their responsibility and how to protect all sensitive card holder data.

Procedures

A. Establish, Publish, Maintain, & Disseminate Security Policies - Standard 12.1

1. All security policies are published on the Income Accounting & Student Loan Services web page.
    a. Anyone handling card holder data must do the on-line training, annually, and have confirmation that they have completed the training, sent to Income Accounting & Student Loans to maintain as proof of completion.
    b. The training includes all PCI DSS requirements.
    c. Departments will have risk assessments performed annually.

2. Departments must provide documentation of any changes to their card holder data software, or environment, as soon as it happens, or at least annually to Income Accounting & Student Loan Services.

B. Development Daily Operational Security Procedures - Standard 12.2

1. Each department shall maintain procedures to ensure that their daily operational functions are secure, for each PCI standard.
    a. These security procedures should include all technical and administration functions.
    b. Procedures should be in place and logs should be kept for user account additions, changes, and deletions.
    c. Procedures should be reviewed at least annually by employees, to ensure that card holder data is processed securely, and that all back-up is kept secure.
    d. Documentation of any system changes, or incidents should be dated and maintained by the department.

C. Develop Usage Policies - Standard 12.3

1. Each department must retain procedures demonstrating secure usage for remote access technologies, wireless technologies, removable electronic media, laptops, tablets, PDS's, e-mail usage, fax usage, and internet usage.
    a. Department must enforce the procedure that any third party software, or card holder data system, requires authentication by a user ID and password, or by a two factor authentication solution.
    b. Formal written authorization approving access to each technology must be kept by department.
    c. Documentation that lists all devices and the employee that uses that device should be kept and updated, and if appropriate should have their name on the device.
    d. Only devices approved by the Income Accounting & Student Loan Services department can be used.
        i. At this point in time, mobile devices cannot be used to process cardholder data.
    e. Access to use any University's wireless network needs approval from Income Accounting & Student Services.
        i. At this point in time, there are no approved University wireless networks.
    f. Departments can only use products approved by Income Accounting & Student Loan Services.
        i. Refer to the Payment Card Acceptance web page for approved devices.
        ii. Approval is required for any device not listed on the above web page.
    g. All devices should have an automatic disconnect of the session after a designated period of inactivity, usually 30 minutes.
    h. Vendors and Third Parties shall have limited access to University systems, and prior arrangements should be made to allow this access for only the required amount of time.
        i. Departments must have their vendor or third party use the University's 'Two Factor Authentication' solution.
    i. Ensure through internal procedures, that employees are informed that no cardholder data shall be copied, moved or stored on local hard drives, and removable electronic media.
        i. Procedure should include the protection of cardholder data according to the PCI standards.

D. Security Responsibilities Defined for Personnel – 12.4

1. Security for each responsibility shall be defined and distributed to personnel.

a. Documentation demonstrating that each employee understands their security responsibility shall be maintained and updated by the department.

E. Assignment of Security Management Responsibilities – 12.5

1. The responsibility of security management is shared by the Chief Information Security Officer, and the PCI team in Income Accounting and Student Loan Service.

a. The PCI team in Income Accounting and Student Loan Service is responsible to:

i. Establish, document, and distribute security policies and procedures. This is done by updating the Income Accounting and Student Loan Service web page, and the University Payment Card Policy.
ii. Updates are made whenever there is a change in a procedure.
iii. Create, maintain, and execute escalation procedures and process.

b. The Chief Information Security Officer is responsible to:

i. Establish, document, and distribute security incident response.

c. The department is responsible to:

i. Monitor, and control access to data.
ii. Administer, add, delete, and modify User access, and inform the Income Accounting & Student Loan Services.
iii. Distribute security incident procedure to employees.

F. Formal Security Awareness Program – 12.6

1. Formal training is required annually for every employee who has access to cardholder data.

a. Annually, all personnel with access to cardholder data must do the on-line training located on the Income Accounting & Student Loan Services web page.
   i. The Department must provide a list of employees with access to cardholder data either annually or whenever there is a new hire, change, or termination.
b. Once the employee completes the training, their name and ID will automatically updated to a data base.
c. Income Accounting & Student Loan Services sends notification to employees when it is time for them to do their annual training.
d. Updates of any type of PCI information, or changes in procedures, etc., will be e-mailed to employees, by Income Accounting & Student Loan Services

G. Background Checks – 12.7

1. Background checks must be performed on any employee who accesses cardholder data, to

comply with PCI DSS standards, and to comply with University of Utah Policy 5-130.

a. Before a position, that has the responsibility of accessing cardholder data, can be offered, a successful background check must be performed by Human Resource.

H. Procedures for Cardholder Data That is Shared by a Service Provider – 12.8

1. For departments who have contracted a Service Provider, and that Service Provider shares cardholder data with a University department, it must be listed in the agreement or contract that the Service Provider is responsible for the security of the cardholder data.

2. The Service Provider shall also sign a Business Associate Agreement (BAA).
    a. Departments must provide a copy of the contract or agreement, and the BAA, to the Income Accounting & Student Loan Services department.
    b. Income Accounting & Student Services maintains a list of all Service Providers, and also verifies and maintains annual PCI DSS compliancy.

I. Incident Response Plan – 12.9

1. Departments must maintain an internal incident response plan to report incidents to Income Accounting & Student Loan Services and the Chief Information Security Officer.
    a. As soon as an incident is identified, it should be reported to the Manager or Director of the department.
    b. The events should be documented and dated, then passed on to Income Accounting and Student Loan Services, and the Chief Information Security Officer, and include:
        i. Date incident was found.
        ii. What type of an incident was it?
        iii. How the department was made aware of the incident.
        iv. Has the department disable the breached device or system?