Version:	Modified By:	Date:	Approved By:	Date:
1.0	Kim Stringham	August 12, 2015	Lisa Zaelit	August 18, 2015
2.0	Stu Schrager	May 14, 2018	Lisa Zaelit	May 16, 2018

DEPARTMENT PROCEDURE FOR STANDARD 11 – Regularly Test Security Systems and Processes

Purpose

The purpose of regularly testing PCI components is to discover vulnerabilities that are continually being introduced by malicious individuals. New vulnerabilities must be addressed in order to maintain the security and integrity of all PCI systems.

Procedure

A. Internal and External Network Vulnerability Scans – Standard 11.2

1. Weekly internal scans will be initiated by the Information Security Office on all third party software system components and/or desktops computers that access a third party vendor's hosted web service for processing payment cards.
    a. Newly discovered vulnerabilities will be remediated within 30 days of their discovery.
    b. Scans will be rerun until all "high-risk" vulnerabilities are resolved.
    c. Internal scans should be initiated by the department as patches and updates are made to their cardholder data environment.
2. External Network Vulnerability Scans will be run on a monthly basis on all public facing PCI systems.
    a. Newly discovered vulnerabilities will be remediated within 30 days of their discovery.
    b. Scans will be rerun until all "high-risk" vulnerabilities are resolved.
    c. External scans should be initiated by the department, through Income Accounting and Student Loans, as patches and updates are made to their cardholder data environment.
    d. A passing ASV attested external scan will be sent to the bank on a quarterly basis by Income Accounting and Student Loans.

B. Penetration Testing – Standard 11.3

1. Penetration testing will be performed, on the applicable PCI systems, by a qualified internal or external entity as designated by Income Accounting and Student Loans and the Information Security Office.
2. The University will ensure that the designated entity uses testing methodology as outlined in PCI DSS Requirement 11.3
3. Penetration testing will be completed at least annually, and whenever system changes have been made to the PCI environment. System changes are defined as the following.
    a. Standard Change: Well documented, low risk, and proven. Standard changes are done on a regular basis and been implemented successfully multiple time before. The first instance of a standard change needs to be submitted and reviewed by the CAB before implementation. Afterwards, standard changes are considered pre-approved and can be implemented during the next available change window without CAB approval or using required lead times. Coordination activities can be done at the discretion of the Systems Analysts.
    b. Minor Change: A minor change has a low impact either in terms of the number of users affected or the criticality of the service and has a low risk of failure. Minor changes are reviewed by the Change Management team and approved by the Change Manager. Minor changes need to have the required lead time. Coordination activities can be done at the discretion of the Systems Analysts.
    c. Major Change: A major change has significant impact on users or services, a high risk of failure, or is complex and requires multiple teams to implement. This may also include new, high-profile applications that are being used in production for the first time or changes to applications where a high degree of coordination between multiple organizations needs to occur.
    d. Emergency Change: This is a change that needs to be implemented IMMEDIATELY to fix an incident due to severe loss in service capability.
    e. Significant Change: May include standard, minor, major or emergency changes. From PCI Guidance: The determination of what constitutes a significant upgrade or modification is highly dependent on the configuration of a given environment. If an upgrade or modification could allow access to cardholder data or affect the security of the cardholder data environment, then it could be considered significant. Refer to Significant Change Requirements.

C. Intrusion Detection – Standard 11.4

1. All departments with Third Party systems will deploy the University approved intrusion detection software.

2. The University Security Assurance Group will monitor all traffic and notify departments of any suspected threats and/or compromises.
3. Departments will respond immediately following notification of a problem.

D. Change Detection – Standard 11.5

1. University approved File Integrity Monitoring (FIM) software will be deployed on all systems using Third Party Vendors in order to detect changes, additions, and deletions of critical system files, configuration files, or content files, including operating system programs and application executables.
2. The University Security Assurance Group will do a weekly comparison of the FIM reports.