Version:	Modified By:	Date:	Approved By:	Date:
1.0	Kim Stringham	August 14, 2015	Lisa Zaelit	August 20, 2015
2.0	Stu Schrager	May 14, 2018	Lisa Zaelit	May 16, 2018

Department Procedure for Standard 2 – Do not use vendor-supplied defaults for system passwords and other security parameters:

Purpose

The purpose of this procedure is to ensure that departments do not use vendor supplied passwords upon implementation and maintenance of third party software used to process cardholder data, thus preventing malicious individuals (external and internal to the University) to use well known default and vendor supplied passwords to compromise University systems. Other security parameters must also be met upon implementation of a new processing system or method.

Procedure

A. Change vendor-supplied defaults before implementing a system – Standard 2.1

1. Department system administrators will always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing the following on the University network.
    a. Operating systems
    b. Software that provides security services
    c. Application and system accounts
    d. Point-of-Sale terminals
    e. Simple Network Management Protocol (SNMP)
    f. Third Party PA-DSS software

B. Wireless Network (Wi-Fi) – Standard 2.1.1

1. The University wireless network is not to be used by Departments for any PCI system to process or transmit cardholder data including UConnect and UGuest.

C. System Hardening – Standard 2.2

1. All PCI system components will be configured accounting to industry-accepted system hardening standards including, but not limited to:
    a. Center for Internet Security (CIS)
    b. International Organization for Standardization (ISO)
    c. National Institute of Standards Technology (NIST)

D. Single Purpose Devices – Standard 2.2.1

1. PCI devices will be implemented so that each device has one primary function. This is to prevent functions that require different security levels from co-existing on the same device. Devices include:
    a. Servers – web servers, database servers, and DNS servers.
    b. Desktops – desktops may only have the card processing software or web access to the third party vendor, with no other program or web surfing capabilities.
2. Only necessary services, protocols, daemons, etc., as required for the function of the system will be enabled.

E. Secure Cryptography – TLS – Standard 2.2.3

1. Additional security features for required services, protocols, or daemons, such as NetBIOS, file-sharing, Telnet, FTP, etc., must be secured with the most recent version of TLS. SSL is no longer considered secure encryption.
    a. SSH, S-FTP, or IPsec VPN are also allowed.

F. Prevent System Misuse – Standard 2.2.4-2.2.3

1. All system components will only have the necessary configuration to support payment processing functionality. All unnecessary functions will be removed in order to prevent misuse and reduce risk to the PCI environment.

G. Maintain System Component Inventory – Standard 2.4

1. Departments will keep an inventory of all PCI devices and components including:
    a. Hardware serial #s, model names, and locations
    b. IP addresses, DNS, VLANs, and Operating Systems
    c. The purpose of the components
    d. Owners