SecureCarolina University Information Security Office

Payment Card Industry (PCI) Vulnerability Management Standard

Issued Date: 26-March-2015

Purpose

This standard provides guidance on vulnerability management and remediation of the Payment Card Industry (PCI) environment at the University. It is to be used in conjunction with the overarching Vulnerability Management Standard and provides additional vulnerability scanning and remediation detail in order to comply with PCI compliance standards. It is not meant to be a standalone document.

Scope

This standard applies to:

- All university systems that transmit, process, store or access PCI data.
- This procedure is developed to satisfy the quarterly internal vulnerability scan requirement as part of the annual PCI compliance efforts.

Definitions

In the context of this document, the following terms are used as indicated here:

PCI System Administrator – Any employee, affiliate, contractor, or vendor of the university who has administrative and/or operational responsibility over university PCI data and/or technical systems.

Document Locker – An encrypted file system maintained and hosted by the QSA where compliance artifacts should be uploaded.

Qualified Security Assessor (QSA) – A person or organization that has been certified by the PCI Security Standards Council to audit merchants for Payment Card Industry Data Security Standard (PCI DSS) compliance.

CampusGuard – A third party vendor and QSA for the university.

Common Vulnerability Scoring System (CVSS) – A free and open industry standard for assessing the severity of computer system security vulnerabilities.

Timelines in this document are denoted as calendar days.

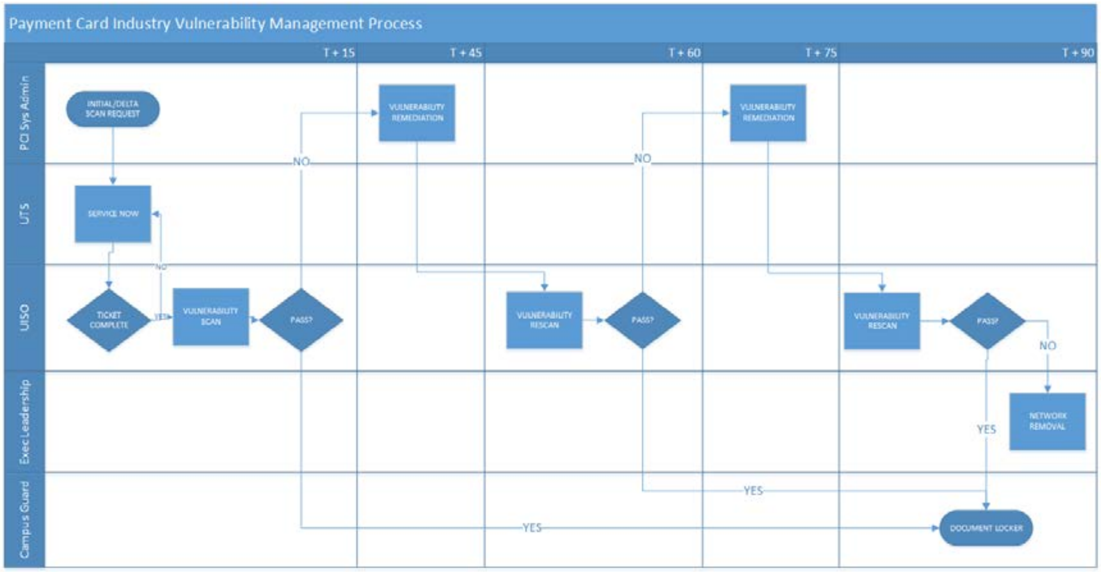
(continued)

Procedure

1. The PCI system administrator will submit an initial vulnerability scan request via ServiceNow to the attention of UISO. Please fill in all information from appendix A. ServiceNow tickets should also be submitted to document changes to existing scans (new machines added, old machines removed, IP address changes, etc.)
2. ServiceNow will route the task to the security team and it will be added to the security task backlog.
3. UISO will adjudicate the ServiceNow ticket for completeness and check with UTS Network Services group to ensure the correct firewall rules are in place.
    a. *If additional information is needed to initiate the scan, UISO will contact the PCI system administrator via ServiceNow.*
4. When all information is complete and the firewall rules in place, UISO will execute the scan using the Nessus Vulnerability Scanning tool.
    a. *A PCI specific vulnerability scan will be executed. A passing grade, as defined by the scan results and the Qualified Security Assessor (QSA), CampusGuard, is a report with no vulnerabilities or findings higher than and including a CVSS score of 4.0.*
5. At the completion of the scan, UISO will provide the results to the PCI system administrator.
    a. *If a passing grade is achieved, UISO will also post a copy of the results to the CampusGuard document locker. This will complete the quarterly internal scan requirement for PCI.*
6. If the scan produces a failing grade, the PCI system administrator will have 30 days to remediate the findings in advance of a rescan by UISO.
7. UISO will rescan 30 days after completion of the first scan.
    a. *If a passing grade is achieved, UISO will provide a copy of the results to the PCI sys admin and post a copy to the CampusGuard document locker. This will complete the quarterly internal scan requirement for PCI.*
    b. *If the scan results in a failing grade, the PCI sys admin will have 15 days to remediate the findings.*
8. In the event of a failing grade, UISO will conduct a final rescan of the PCI environment 15 days from completion of the last one.
9. A failing scan will result in escalation to Executive leadership and the beginning of the Removal from the Network process as defined in the Vulnerability Management Standard.
    a. *Executive Leadership can engage the QSA for advice on remediation of vulnerabilities or whether an exemption is acceptable.*

(continued)

Payment Card Industry (PCI) Vulnerability Management Standard Flowchart



A larger version of this flowchart image can be found in ***Appendix B*** *of this document.*

Contacts

http://security.sc.edu

Revision History

Author	Date	Comments
Anthony Ryan	26 Mar 2015	Initial Draft
Anthony Ryan	2 Apr 2015	Added “Appendix A”
Kyle Brown	6 Apr 2015	Review and formatting
Kyle Brown	23 Apr 2015	Removal of draft status – prep for publication

(continued)

Appendix A

PCI vulnerability scans are executed on the third Tuesday of each month. UISO has not seen, and does not anticipate, the scan having any adverse effects on the systems being scanned but we can't guarantee it won't. As a result, please ensure the scan window is scheduled to avoid peak usage of your devices. Please also ensure that the devices are powered on during the scan window. Scans typically complete in less than 1 hour. Scan results will be sent to system administrators as encrypted zip files.

Submit a UTS Service Desk request containing all of the following:

IP address and name of any servers to be scanned:
IP addresses of the subnets to be scanned:
Email address of system administrator where the vulnerability scan results will be sent to:

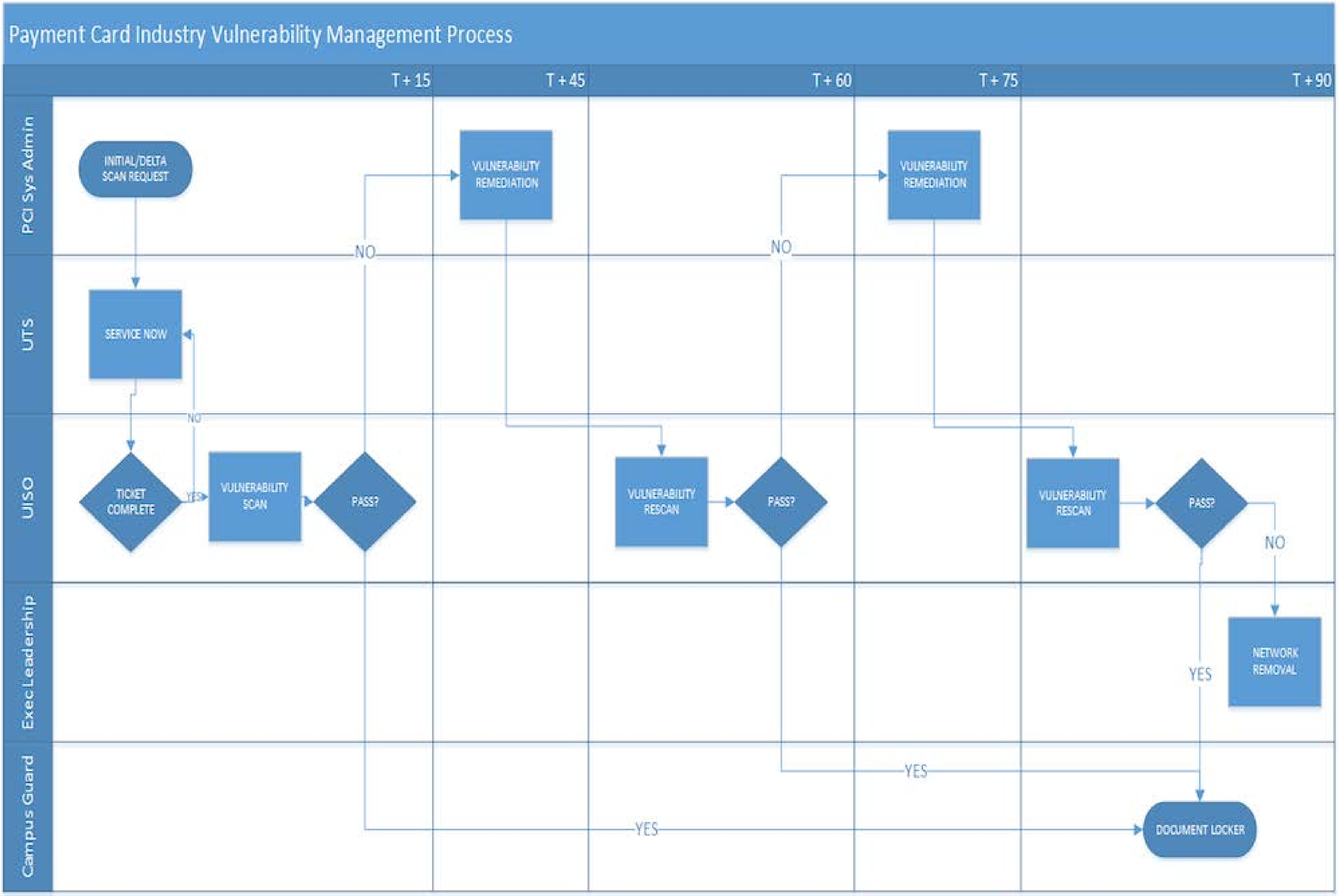
Phone number of system administrator where the vulnerability scan results will be sent to:
Please confirm that 10.250.100.147 has access through all firewalls – including any locally managed and host firewalls on your devices.

UTS Service Desk URL:

http://www.sc.edu/about/offices_and_divisions/university_technology_services/support/servicedesk.php

(continued)

Appendix B


Payment Card Industry Vulnerability Management Process
T + 15
T + 45
T + 60
T + 75
T + 90
PCI Sys Admin
UTS
UISO
Exec Leadership
Campus Guard
INITIAL/DELTA SCAN REQUEST
SERVICE NOW
TICKET COMPLETE
NO
YES
VULNERABILITY SCAN
PASS?
NO
YES
VULNERABILITY REMEDIATION
VULNERABILITY RESCAN
PASS?
NO
YES
VULNERABILITY REMEDIATION
VULNERABILITY RESCAN
PASS?
NO
YES
NETWORK REMOVAL
DOCUMENT LOCKER