The University Of Sheffield.

Payment Card Industry - Data Security Standard (PCI-DSS) v3.2

Systems Security Standard

Version and Ownership

Version	Date	Author(s)	Comments
0.01	26/9/2016	Sinead O'Brien	Initial document creation (PCI DSS v3.2)
0.01	04/01/2017	Sinead O'Brien	Version 0.01 approved by CiCs Exec
0.02	15/1/2017	Sinead O'Brien	Updated to cover additional PCI DSS requirements
0.02	10/02/2017	Sinead O'Brien	Version 0.02 approved by CiCs Exec.
0.03	09/03/2017	Sinead O'Brien	Updated to cover additional PCI DSS requirements
0.03	12/05/2017	Sinead O'Brien	Version 0.03 approved by CiCs Exec.
0.04	26/05/2017	Sinead O'Brien	Updated to cover additional PCI DSS requirements
0.04	28/07/2017	Sinead O'Brien, Chris Willis & Tom Griffin	Version 0.04 approved by CiCs Exec.
0.05	31/10/2017	Sinead O'Brien, Chris Willis & Tom Griffin	Updated to cover additional PCI DSS requirements. Version 0.05 approved by CiCS Exec.
1.0	30/01/2018	Sinead O'Brien, Chris Willis & Tom Griffin	Updated to clarify details of requirement 4.1. Version 1.0 approved by CiCs Exec.
1.1	17/04/2018	Sinead O'Brien, Chris Willis & Tom Griffin	Responsibilities section added. Usage Policy reduced and reformatted to cover IT specific responsibilities only. Tasks related to finance moved to the University PCI DSS Finance Standard
1.2	01/05/2018	Sinead O'Brien, Chris Willis & Tom Griffin	Remove requirements that are no longer applicable due to reduction in CDE scope.

Introduction

This document is part of a suite of documents to support the University's compliance to the Payment Card Industry Data Security Standard (PCI DSS) (PCI DSS 12.1). This document details the systems security procedures for all staff working in or with the cardholder data environment. The controls described in this document apply to systems in the CDE or that can impact upon the security of systems in the CDE. This document will be reviewed at least annually and be updated when business objectives or the risk environment changes to ensure that it continues to be in compliance with the Standard (PCI DSS 12.1.1).

General Principles

All staff involved in maintaining the technical systems for the CDE in the University must adhere to and be aware of the following additional documents and adhere to the rules and regulations defined within them:

- University of Sheffield PCI DSS Security Policy
- University of Sheffield CiCS Information Security Page
- The University of Sheffield Code of Connection
- The University of Sheffield CiCS Code of Practice

Responsibilities

All personnel involved in maintaining the technical systems for the CDE in the University are responsible for adhering to the rules, regulations, policies and procedures defined within this document. Particularly relevant personnel include but are not limited to: staff with roles in Network Security, Voice & Data and Web/Application Development.

Network Diagrams and Payment Card Data Flows

PCI DSS Requirement Number	Requirement Details
1.1.2 **1.1.3**	A current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks must be maintained and available from the PCI DSS incident response plan. A current diagram that shows all cardholder data flows across systems and networks must be maintained and available from the PCI DSS incident response plan.

Portable computing devices connecting to CDE

PCI DSS Requirement Number	Requirement Details
1.4	Personal firewall software or equivalent functionality is required for all portable computing devices that connect to the Internet when outside the network, (for example, laptops used by employees), and which are also used to access the CDE. The use of personal portable computing devices to connect to the CDE is strictly prohibited. Only University supplied and managed portable devices are allowed. Specific configuration settings are defined for personal firewall or equivalent functionality. For further information please visit www.sheffield.ac.uk/cics/firewall Personal firewall or equivalent functionality must be configured to actively run. Personal firewall or equivalent functionality must be configured to not be alterable by users of the portable computing devices.

Firewalls

PCI DSS Requirement Number	Requirement Details
1.1.1	All changes made to network connections, firewall and router configurations must be tested and approved in accordance to the CiCS change management policy (https://www.sheffield.ac.uk/cics/change/policy) and follow the firewall operational procedures detailed below
1.1.4 **1.2.3**	A firewall is required: ● at each Internet connection, and ● between the CDE and any other network (e.g. University LAN, DMZ). ● between the CDE and all wireless networks Firewalls must be configured to permit only authorised traffic.
1.1.5 **1.1.6** **1.1.7**	Firewall and router configuration standards will be maintained by the Network Group. These will include; ● a description of groups, roles, and responsibilities for management of network components ● a documented list of all services, protocols and ports within the CDE, including business justification and approval for each. No insecure services, protocols, or ports are allowed within the CDE. Firewall and router rule sets must be reviewed at least every six months.
1.5	All staff involved in managing firewalls within the CDE or that can have an impact on the security of the CDE must be aware of and follow the security policies and operational procedures as detailed in the following documents ● Security policies: www.sheffield.ac.uk/cics/firewall/ ● Operational procedures: https://drive.google.com/open?id=1Uzm-8OvVa5Wm9C2p9ETfWxfkk9aJ1YdIjItkT9UOZFs ● PCI DSS Network Configuration: https://docs.google.com/document/d/1h--49WAtshUh23NL57hTS0Lh5yyWYNNrpn-2YBLN-uw/edit#heading=h.uclgnvhe0aaj
1.2.1	Where segmentation is used to isolate the CDE from other networks, inbound and outbound traffic will be restricted to that which is necessary for the cardholder data environment, and specifically deny all other traffic.
1.3.3	Anti-spoofing measures will be implemented at each Internet connection or where segmentation is used to isolate the CDE from other networks to detect and block forged source IP addresses from entering the network.
1.3.4	Where segmentation is used to isolate the CDE from other networks, unauthorized outbound traffic from the cardholder data environment to the Internet is not allowed.
1.3.5	Where segmentation is used to isolate the CDE from other networks, only “established” connections into the network will be permitted.

1.3.7	Private IP addresses and routing information must not be disclosed to unauthorized parties.

Network and system components

PCI DSS Requirement Number	Requirement Details
2.1	Always change vendor-supplied defaults **before** installing a system. Always remove or disable unnecessary default accounts **before** installing a system. This applies to ALL default passwords within the CDE, including but not limited to those used by operating systems, software that provides security services, application and system accounts, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings
2.3	All non-console administrative access must use strong cryptography.

Encrypt transmission of cardholder data across open, public networks

PCI DSS Requirement Number	Requirement Details
4.1	Unencrypted cardholder data must not be transmitted over the University network. Secure protocols and strong cryptography (as defined by the PCI SSC) must be used to safeguard the transmission of cardholder data. ● Only trusted keys and certificates are accepted. ● The protocol in use only supports secure versions or configurations. ● The encryption strength is appropriate for the encryption methodology in use. Only Worldpay provided PCI SSC approved PTS devices devices that support TLS 1.2 or higher may be used for standalone payment acceptance. Only Verifone provided PCI SSC approved PTS devices provided as part of a PCI SSC approved P2PE solution can be used where payment acceptance must be integrated with a till. If encryption fails on any device, this device must not be used to process transactions.

4.1.1	Any wireless network transmitting cardholder data or connected to the CDE must implement industry best practices (i.e. IEEE 802.11i/WPA2 or stronger) to implement strong encryption for authentication and transmission. The use of weak authentication and encryption standards (including WEP and WPA1) is prohibited.

Web servers redirecting to external service providers

The following requirements apply to both internally or externally hosted websites redirecting to external service providers (e.g. WPM) who are processing payments on behalf of the University.

PCI DSS Requirement Number	Requirement Details
8.1 / 8.2 **8.1.1** **8.1.3** **8.2.3**	Proper user identification management for non-consumer users and administrators on all system components must be in place as follows: Assign all users a unique ID before allowing them to access cardholder data or system components. Immediately revoke access for any terminated users. All users must have a password that meets the following requirements: ● Require a minimum length of at least seven characters. ● Contain both numeric and alphabetic characters.
8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: ● Generic user IDs are disabled or removed. ● Shared user IDs do not exist for system administration and other critical functions. ● Shared and generic user IDs are not used to administer any system components.

Access to system components

PCI DSS Requirement Number	Requirement Details
7.1.2, **7.1.3**	Logical access to in-scope CDE components, and supporting components must be restricted to authorised technicians using the least privileges required to fulfil the role and based upon individual personnel's job classification and function.
8.1.5	IDs used by third parties to access, support, or maintain system components via remote access will be managed as follows: ● Enabled only during the time period needed and disabled when not in use. ● Monitored when in use.

8.2.1 **8.3.1**	Using strong cryptography, all authentication credentials (such as passwords/phrases) will be rendered unreadable during transmission and storage on all system components. Multi-factor authentication will be incorporated for all non-console access into the CDE for personnel with administrative access.
8.3.2	Multi-factor authentication will be incorporated for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the University network.
12.3.9	Where segmentation is used to isolate the CDE from other networks, remote-access technologies for vendors and business partners will be activated only when needed by vendors and business partners, with immediate deactivation after use.

Restrict access to cardholder data

PCI DSS Requirement Number	Requirement Details
9.1.2 **9.5, 9.5.1** **9.6, 9.6.1,** **9.6.2, 9.6.3,** **9.7, 9.7.1** **9.8.2**	Physical/logical controls must be implemented to restrict access to publicly accessible network jacks. No electronic or paper media backups of cardholder data may be created, stored or distributed, either on University premises or at any off-site facility. If any media backup of cardholder data is discovered it must be reported as a security event, in accordance with the PCI DSS Incident Response Policy. Electronic storage of cardholder data is strictly prohibited. In the event that electronic storage of CHD is discovered, this must be reported as a security event, in accordance with the PCI DSS Incident Response Policy.

Inventory maintenance

PCI DSS Requirement Number	Requirement Details
2.4 **9.9, 9.9.1**	It is the joint responsibility of the Income Office Team Leaders and the CiCS Network Group to maintain an up-to-date list of devices and system components in the CDE. This list will include the following: ● Make, model of device. ● The full address of the site where the device is located. ● Device serial number or other method of unique identification. ● Description of the function/use

Vulnerability management and penetration testing

PCI DSS Requirement Number	Requirement Details

6.1	Methods of identifying new vulnerabilities must use use reputable outside sources for security vulnerability information to assign a risk ranking to vulnerabilities that includes identification of all “high risk” and “critical” vulnerabilities. The PCI DSS Vulnerability Management Standard defines the process used to assess risks.
6.2	All system components and software within the segmented CDE will be protected from known vulnerabilities by installing all applicable vendor-supplied security patches within an appropriate timeframe as determined on a case by case basis taking into consideration the risk of the vulnerability and the impact to the business. In the case of critical security patches, these will be installed within one month of release.
11.2.2	Quarterly external vulnerability scans will be performed, via Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Rescans will be performed as needed, until passing scans are achieved.
11.3.4	Where segmentation is used to isolate the CDE from other networks, penetration tests will be performed at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.

Log management

PCI DSS Requirement Number	Requirement Details
10.1	Sufficient logging must be in place to link all access to system components to each individual user.

Time synchronisation

PCI DSS Requirement Number	Requirement Details
10.4 **10.4.1** **10.4.3**	All critical systems in the CDE must use NTP time-synchronisation technology to synchronise clocks and times to ensure that the following is implemented for acquiring, distributing, and storing time; ● Critical systems have the correct and consistent time. ● Time settings are received from industry-accepted time sources. (eg. GPS receiver)

Usage Policy for Critical Technologies

PCI DSS Requirement Number	Requirement Details
12.3 **12.3.8** **12.3.9** **12.3.10.a**	Any potential new component intended to accept online payments must undergo a security assessment, including a vulnerability scan, prior to going live. ● The results of the assessment will be shared with Finance and the use of the new component must be approved by both CiCS and Finance before going live. When performing remote administration on critical technologies in the CDE: ● Sessions must be automatically disconnected after a specific period of inactivity. (PCI DSS Requirement 12.3.8) ● Access for vendors and business partners only when needed by vendors and business partners must be immediately deactivated after use. (PCI DSS Requirement 12.3.9) ● Cardholder data must not be copied, moved, or stored to local hard drives or removable electronic media (PCI DSS Requirement 12.3.10.a)

Glossary of terms

Term	Definition
PCI DSS	Payment Card Industry Data Security Standard
CHD	Cardholder data
SAD	Secure authentication data
CDE	Cardholder data environment