The
University
Of
Sheffield.

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

Security Policy

Version and Ownership

Version	Date	Author	Comments
0.01	05/09/2016	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	20/12/2016	Sinead O'Brien	Updates to section "General Rules for University of Sheffield"
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	12/06/2017	Sinead O'Brien & Chris Willis	Updated to cover additional PCI DSS requirements and statement that UoS is not a Service Provider
0.04	27/07/2017	Sinead O'Brien & Chris Willis	Version 0.4 approved by CiCS Exec and Robert Hebblethwaite
0.05	31/10/2017	Sinead O'Brien	Version 0.5 approved by CiCS Exec and Robert Hebblethwaite
1.0	30/01/2018	Sinead O'Brien, Chris Willis & Tom Griffin	Updated to clarify statement that UoS is not a Service Provider. Version 1.0 approved by CiCS Exec and Robert Hebblethwaite
1.1	17/04/2018	Sinead O'Brien, Chris Willis & Tom Griffin	Updated to include additional information relating to responsibilities of personnel.
1.2	01/05/2018	Sinead O'Brien, Chris Willis & Tom Griffin	Remove requirements that are no longer applicable due to reduction in CDE scope.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 provides an overview of the rules and regulations in place across The University of Sheffield to allow us to achieve and maintain compliance to the Payment Card Industry Data Security Standard (Henceforth PCI DSS) (PCI DSS 12.1). PCI DSS is a global standard managed and maintained by the Payment Card Industry Security Standards Council (PCI SSC), details can be found on their website here: https://www.pcisecuritystandards.org. This document and those sub-documents referred to below deal with security from a PCI DSS standpoint. This document will be reviewed at least annually, in accordance with the requirements of PCI DSS, and be updated when business objectives or the risk environment changes (PCI DSS 12.1.1). For our more general overview information security policy please visit the University of Sheffield CiCS Information Security Page.

PCI DSS and the University of Sheffield

The University of Sheffield is currently a Level 3 Merchant[1] reporting to its acquirer via a series of SAQs (Self Assessment Questionnaires). The University of Sheffield handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation. The University of Sheffield commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end, all University staff involved with any aspect of handling cardholder data are committed to maintaining a secure environment in which to process information so that we can meet these promises.

Policy Applicability

All employees, contractors, vendors and third-parties involved in the storage, transfer or processing of cardholder data or that can affect the security of the cardholder data environment at The University of Sheffield must follow existing University of Sheffield PCI DSS Policies.

University of Sheffield Standards

The University of Sheffield has split its policies across the following standards:

Standard
PCI DSS Finance Standard
PCI DSS Systems Security Standard
PCI DSS Incident Response

[1] A merchant processing 20,000 to 1M Visa, Mastercard or Maestro e-commerce transactions per year.

Responsibilities (PCI DSS 12.4, 12.5)

All personnel (e.g. employees, contractors, vendors and third-parties) involved in the storage, transfer or processing of cardholder data or that can affect the security of the cardholder data environment at The University of Sheffield must abide by relevant PCI DSS policies and procedures. All PCI DSS policies define responsibilities for relevant personnel.

The University's Information Management Group (IMG) supports and drives the broader information management agenda and provides the University with the assurance that effective and proportional information governance mechanisms are in place within the organisation. This includes the management of information security risk and controls. IMG reports to the University's Executive Board through the IMG Chair's (Director of CiCS) line reporting.

The Director of CiCS is responsible for:

- The management of Information Security risks highlighted in the CICS departmental risk register and the University's Corporate Risk Register.
- The Information Governance function, which includes Information Security.
- Approval of high-level Information Security policies and processes

Working with colleagues across the University the PCI DSS Project Team[2] is responsible for ensuring that the following activities take place within the CHD:

- Establish, document, and distribute security policies and procedures. (PCI DSS 12.5.1)
- Ensuring that security policies and procedures clearly define information security responsibilities for all personnel. (PCI DSS 12.4)
- Monitor and analyze security alerts and information, and distribute to appropriate personnel. (PCI DSS 12.5.2)
- Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. (PCI DSS 12.5.3)
- Administer user accounts, including additions, deletions, and modifications. (PCI DSS 12.5.4)
- Monitor and control all access to data. (PCI DSS 12.5.5)

Responsibility for the approval and enforcement of PCI DSS policies is shared by the Finance and CiCS (IT) Executive.

Systems

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 the PCI DSS Systems Security Standard. (e.g. staff with roles in Network Security, Voice & Data and Web/Application Development)

Finance

Responsibilities for all operational and management personnel involved in storing, processing or transmitting cardholder data in the University are defined within the PCI DSS Finance Standard. (e.g. Device Supervisors, Device Operators, users of the Online Expenses System, users of the Records

[2] On completion of the project this responsibility will be passed onto the PCI DSS Steering Group.

Centre, Purchasing Card holders and anyone interested in exploring new payment acceptance methods)

Incident

Responsibilities for all personnel responding to an incident and those with an incident management role within the University’s cardholder data environment (CDE) are covered within the **PCI DSS Incident Response**

Core principles of PCI DSS

The core principles of the PCI DSS framework consist of the following twelve (12) requirements;

No.	Definition
1	Install and maintain a firewall configuration to protect cardholder data
2	Do not use vendor-supplied defaults for system passwords and other security parameters
3	Protect stored cardholder data
4	Encrypt transmission of cardholder data across open, public networks
5	Use and regularly update anti-virus software on all systems commonly affected by malware
6	Develop and maintain secure systems and applications
7	Restrict access to cardholder data by business need-to-know
8	Assign a unique ID to each person with computer access
9	Restrict physical access to cardholder data
10	Track and monitor all access to network resources and cardholder data
11	Regularly test security systems and processes
12	Maintain a policy that addresses information security

General Rules for University of Sheffield

The following rules apply to The University of Sheffield, its subsidiary Companies and any staff involved in storage, processing or transmission of cardholder information in the card data environment.

The University of Sheffield will adhere to the PCI DSS for the security of its customers cardholder data.
The use of personal equipment to connect to the CDE is strictly prohibited.
The use of email in the CDE is strictly prohibited.
The University of Sheffield is not a Service Provider[3] for payment processing and does not permit the storage, transmission or processing of cardholder data using any University of Sheffield staff or service (including but not limited to mail, email, fax, phone system and network) by any entity unless this entity has received written agreement to do so from the Authorised Financial Officer (as defined in the University's Financial Regulations) .
A PCI DSS specific risk-assessment process will be performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.) that identifies critical assets, threats, and vulnerabilities, and results in a formal, documented analysis of risk. (PCI DSS 12.2)
A formal awareness programme shall be implemented to make all staff associated with the card data environment aware of the University cardholder data security policy and procedures. (PCI DSS 12.6) ● Staff associated with the CDE will be trained in the requirements relevant to their role upon hire and at least annually. (PCI DSS 12.6.1) ● Staff will be required to acknowledge at least annually that they have read and understood the University PCI DSS policy and procedures. In the case where annual training is administered via the online PCI DSS training course, the course will track this information automatically. In the case where other methods of training are used training administrators are responsible for ensuring that all staff sign a training record to this effect.(PCI DSS 12.6.2)
Genuine credit card numbers (aka Live PANs) may not be used for testing or development. (PCI DSS 6.4.3)

[3] Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed Service Providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a Service Provider for that service (although they may be considered a Service Provider for other services).

Glossary of terms

Term	Definition
CDE	Cardholder data environment
CHD	Cardholder data
PCI DSS	Payment Card Industry Data Security Standard
PCI SSC	Payment Card Industry Security Standards Council
SAD	Secure authentication data
SAQ	Self Assessment Questionnaire