UNIVERSITY OF SUSSEX

Finance division

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) COMPLIANCE REQUIREMENTS

1. OVERVIEW AND PURPOSE

1.1 This document sets out the compliance requirements for protecting the security of all credit and debit card payments processed by the University which are governed by the Payment Card Industry Data Security Standard (PCI DSS).

1.2 Terms used within this document relating to the Payment Card Industry Data Security Standard are defined in the Glossary (see Appendix 2).

1.3 The Payment Card Industry Data Security Standard (PCI DSS) sets out an extensive and detailed list of requirements and security assessment procedures. The goals and requirements of the standard are summarised under 6 headings and 12 requirements, as set out in Appendix 1. Full PCI DSS details are available at https://www.pcisecuritystandards.org/document_library/

1.4 The standard applies to all organisations that store, process or transmit payment cardholder data. Failure to comply with these requirements could result in the University being fined and no longer permitted to process card payments. The standard is therefore part of the University's Financial Regulations and the University must ensure that its' business processes and technical systems conform to PCI DSS.

2. SCOPE

2.1 Compliance requirements in this document apply to:

- All staff within the University involved in payment card processing, or who have access to cardholder data and therefore have a responsibility to protect that data.
- All payment card processing arrangements across the University.
- Both manual and IT-based payment card processing.

2.2 For the purpose of this document, staff means all staff, either remunerated or not, including senior managers, officers and directors; employees (whether permanent, fixed-term, temporary or casual); contract, seconded and agency staff; volunteers, apprentices and interns; and any other associated with the University (i.e. performing services for or on its behalf) who are otherwise deemed to be covered by the Chief Operating Officer.

2.3 The University does not store or transmit payment card data but does process card payments which are subsequently handled by external 'service providers' who are each certified as being PCI-DSS compliant.

2.4 The University is a 'Level 3 Merchant' which means that certification to the Standard requires the completion of an annual Self-Assessment Questionnaire (SAQ) to demonstrate compliance.

3. RESPONSIBILITIES

3.1 Taking Payments

Staff, Schools or Professional Services Divisions must not plan, commission, use or modify any payment card processing procedures or systems without authorisation from the Chief Financial Officer. This includes any payment card processing activity to be undertaken on behalf of the University or which involves any use of University IT or networking equipment.

3.2 Awareness

The Finance Division, along with Executive Deans and Professional Services Directors, are jointly responsible for making all relevant staff aware of the importance of the cardholder security strategy and the requirements stated in this document.

The Lead Financial Accountant is responsible for ensuring that, where appropriate, all new and existing staff receive documentation and training in PCI DSS requirements.

3.3 Compliance Contact

Schools and Professional Services Divisions working in a card payment environment must nominate a locally responsible person to maintain PCI DSS compliance for that department.

3.4 Training

Any staff requesting a PDQ card machine or intending to work with card payments will need to obtain PCI DSS awareness training from the Finance Division and comply with the PCI DSS compliance requirements, before being allowed to do so.

3.4 Authorised Use

A list of all staff currently authorised to use devices to process payment cards, such as tills, PIN Entry Devices (PEDS), PDQ machines etc. must be maintained by the School/Professional Services Division responsible for providing that service and a copy submitted to the Lead Financial Accountant who will maintain a central register of authorised users.

3.5 Unauthorised Use or Suspected Loss of Data

Staff are responsible for reporting any incident relating to the unauthorised use or suspected loss of data in accordance with the Incident Response Plan, see https://www.sussex.ac.uk/finance/how/income.

3.6 IT Services Responsibilities

IT Services are responsible for arranging and assessing the results of the external and internal network security scans required for PCI DSS compliance. (Approved external and internal network scans must be run at least quarterly to check for security against external access to any networked devices that process payment card data).

3.7 **Computer Use**

Computers used by University staff to access outsourced e-commerce solutions, such as WPM on behalf of customers, must have the required level of security measures on the computer - including automatically updating anti-virus / anti-malware software. IT-managed computers should conform to the necessary standards. If in doubt advice should be sought from IT Services.

4. COMPLIANCE REQUIREMENTS

4.1 Card Payment Processing Requirements

- Staff must not request or agree to accept transmission of any payment card information from University customers via email to other end-user messaging technologies, whether or not encrypted. Any cardholder data received in this way should be deleted immediately, please raise an ITS Service Desk ticket to get support with this action [ITServicedesk@sussex.ac.uk].
- Staff must not ask for 3D Secure or Verified by VISA codes, when processing through an online interface.
- Staff must not store any electronic payment card information, whether or not encrypted, on any computers or storage devices whether by scanning, keying or any other means. This applies to all types of payment card data including PAN/PIN, three-digit security codes and full track data.
- Any electronically stored legacy payment card data, or data stored in error, must be deleted immediately, please raise an ITS Service Desk ticket to get support with this action [ITServicedesk@sussex.ac.uk].
- Staff must fully comply with the Use of IT Regulations and the Information Security Policy https://www.sussex.ac.uk/infosec/policies

4.2 Electronic cardholder data handling

- Payment card information, including full PAN numbers, must not be displayed or made visible to anyone except authorised staff. For example, payment equipment such as PDQ's must not show or print details of the full PAN. (The first six and last four digits are the maximum number of digits that can be displayed).
- Systems, which are specially designed and deployed to transfer cardholder data electronically such as tills, PEDS and PDQs and outsourced e-commerce solutions, must do so in the same way that meets PCI DSS compliance requirements.

4.3 Retention of cardholder data

Sensitive card authentication data must not be recorded on paper.

4.4 **Physical security of payment card processing equipment**

Devices used to process payment cards, such as tills, payment gateway admin sites, PEDS and PDQ machines must:

- Only be used by staff authorised to do so as part of their duties.
- Be protected from physical access out of hours by those not authorised to use the equipment or authorised to be in the area.
- Be subjected to routine visual inspection, preferably each day or before use. Equipment, calling and connections should be inspected for signs of tampering. The working area in the vicinity of the equipment should be checked for any suspicious devices, hidden cameras etc.
- Out-of-hours visitors to areas giving access to payment equipment must be supervised and details of such visits must be logged.

Support and training is provided by Finance on complying with these requirements.

4.5 **Incident Response Plan**

In the event of an incident in which sensitive card data may have potentially been viewed, stolen, or used by an unauthorized party, the University will take prompt action and follow an approved incident plan. The Incident/Breach Response Plan is published here https://www.sussex.ac.uk/finance/how/income and will be reviewed annually.

If an employee suspects an incident as occurred, they must report this to the Finance Service Desk (FinanceServiceDesk@sussex.ac.uk) immediately, who will in turn notify the relevant staff identified in the Incident Response Plan.

4.6 **Third Parties**

Any third parties commissioned to handle cardholder information on behalf of the University of Sussex must be approved by the Finance and IT Services Division based on due diligence prior to engagement. The PCI DSS Team must assess their compliance status. If they are a PCI DSS compliant Service Provider for the contracted services they provide to the University, they will be required to provide the University with an up-to-date version of their Attestation of Compliance before engagement and each year thereafter.

Any contracts or written agreements with third party providers must make clear their responsibility for maintaining/protecting the University's compliance, including explicit reference to these compliance requirements. The PCI DSS Team will maintain a full list of Third-Party Payment Service Providers and will check the service providers PCI DSS compliance annually.

4.7 **Review**

The University will undertake a PCI DSS compliance review on an annual basis. This will include:

- A self-certification form completed by the PCI DSS Team to ensure all areas of the University, with no exceptions, are PCI-DSS compliant.
- The Lead Financial Accountant will do annual and ad hoc spot checks on all PDQ machines and payment methods.
- All third-party suppliers who provide card payment facilities must provide the PCI DSS Team with an up to date copy of their Attestation of Compliance to PCI DSS, on an annual basis.
- The University will carry out regular vulnerability testing on the University network and the results passed to the PCI DSS Team.

5. BREACH OF THESE REQUIREMENTS

5.1 Where there is a deliberate misconduct or behaviour amounting to willful breach of these compliance requirements, or gross negligence causing a breach of these requirements, the matter may be considered under the University's Disciplinary Procedure under Regulation 31.

Review / Contacts / References	
Document title:	Payment Card Industry Data Security Standard (PCI DSS) Compliance Requirements
Date approved:	05/09/2019
Approving body:	Information Governance Committee
Last review date:	December 2024
Revision history:	2.0
Next review date:	12 months from last review date
Related internal policies, procedures, guidance:	Finance Regulations — University Regulations and Financial responsibilities. ISROI — Regulations for the Use of Information Technology — This is the effective Acceptable Use policy of the University. https://www.sussex.ac.uk/ogs/policies/goodconduct/raisingconcerns- Guidance on raising concerns including Fraud. PCI Security Standards website — Regulatory body advice for PCI DSS
Document owner:	Chief Financial Officer

UNIVERSITY OF SUSSEX

Finance division

Lead contact / author:	Lead Financial Accountant
Further info contact	FinanceServiceDesk@sussex.ac.uk

UNIVERSITY OF SUSSEX

Finance division

Appendix 1 - PCI DSS outline

PCI Data Security Standard — High Level Overview: The PCI-DSS is based upon 12 technical and operational requirements which are mandated by the PCI Security Standards Council as prescriptive controls.

Area	Requirements
Build and Maintain a Secure Network & System	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
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Access	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

UNIVERSITY OF SUSSEX

Finance division

Appendix 2 — Glossary

Cardholder Data — At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

Cardholder Data Environment — The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components.

PAN — 'Primary Account Number' and can also be referred to as 'account number'. It is a unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

Payment card — A card backed by an account holding funds belonging to a cardholder or offering credit to the cardholder such as a debit or credit card.

PCI DSS— The Payment Card Industry Data Security Standard.

PCI DSS Breach - A breach is an incident in which sensitive card data may have potentially been viewed, stolen, or used by an unauthorized party.

PCI DSS Team —The staff responsible for ensuring that the University is PCI DSS compliant. Comprising of the Assistant Director of Finance — Finance Corporate Services, the Lead Financial Accountant, Head of Financial Operations — Billing & Income, Corporate Accounting Services Supervisor & the Finance Systems Manager.

PDQ Machine — 'Process Data Quickly'. A credit card swipe machine.

PED — A PIN entry device.

PIN — 'Personal Identification Number'. A secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typically, PIN's are used for automated cash machines and where the PIN replaces the cardholder signature.

PSP— 'Payment Service Provider'

Stripe/track data — data coded in the magnetic stripe or chip used for authentication and/or authorisation during the payment process.