Payment Card Industry Data Security Standard (PCI DSS) Finance Policy

Title	Payment Card Industry Data Security Standard (PCI DSS) Finance Policy
Version Number	4.0
Document Classification	Public
Effective Date	July 2024
Review Date	July 2025
Author	Peter Sullivan (Financial Accountant)
Owner	Nicola Davies (Chief Financial Officer)
Approved by	Finance & Resources Committee
Approval date	

Table of Contents

Introduction

This policy sets out the requirements for protecting the security of all credit and debit card payments received and processed by the University, which are governed by the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS compliance is mandatory for any company or organisation which stores, processes or transmits cardholder data. Failure to comply with these requirements could result in the University being fined and no longer permitted to process card payments.

Where organisations process credit and debit card data ("card data") to take payment for goods/services, there is a requirement to protect card data from theft and/or fraudulent use. The measures that organisations are required to have in place to protect card data are set out in the Payment Card Industry Data Security Standard ("PCI DSS").

PCI DSS is a global standard managed by the Payment Card Industry Security Standards Council.

This policy seeks to minimise the number of occasions when card data is processed by the University to take payment for services/goods. Where it is necessary for the University to process card data, this policy requires that the appropriate security measures are in place so that processing is PCI DSS compliant.

To reduce its exposure to compliance costs and the risk of monetary and reputational penalty from non-compliance, the University seeks to eliminate all processing of card data – transferring that responsibility and the requirement to be PCI DSS compliant to an accredited third party processor. By doing so the University will be taking steps to minimise the aspects of the PCI DSS standard to which it has to adhere to.

The policy applies to staff associated with the Cardholder Data Environment (CDE).

PCI DSS and the University of Liverpool

The University of Liverpool is committed to maintaining and achieving PCI DSS for all University managed payment services that process payments. As a Level 3 merchant (processing between 20,000 to 1 million transactions a year) the University has a contractual obligation to report its compliance to the card acquirer via a series of Self-Assessment Questionnaires (SAQ's). The Finance Department, with the support of IT Services will make returns on PCI DSS compliance to the University's acquirer.

Policy Objectives and Scope

The objectives of this policy are to:

- Ensure that no card data is held/stored by the University;
- As a standard approach look to minimise all forms of card data processing by the University, through transferring that responsibility to a certified PCI DSS level 1 (processing over 6 million transactions a year) third party processor;
- Ensure that any in-house card data processing is minimised and that those processes are and remain PCI DSS compliant; or
- Where it is not possible to process card data in-house within the scope of the PCI DSS standard, then an agreement between the University and the appropriate acquirer must be reached on alternative processing measures and that these are put in place before such processing can commence.

Policy Applicability

All employees, contractors, vendors and third parties involved in the storage, transfer or processing of cardholder data or any parties who can affect the security of the cardholder data environment must follow existing University PCI DSS policies.

This policy is applicable where the University is responsible for processing card data to receive payment for goods/services.

The PCI DSS policy applies to anyone at the University, or one of its subsidiaries, involved in acquiring, using, managing and maintaining systems or services used to take payments or taking payments by credit and debit card.

General Principles

The University must comply with PCI DSS to secure and protect customer card data irrespective of the nature of the transaction.

All staff involved with the CDE must have received PCI DSS training relevant to their role prior to commencing work within the CDE.

Computers and technologies used for, or in association with the CDE are not to be used for any purpose other than official University business.

Privately owned computers and other equipment (including mobile telephones, laptops and tablets) must not be used for the processing, storage or transmission of any cardholder data associated with any aspect of University business.

Departments must not implement business processes that involve the processing of card data without approval by the Finance Department. The Financial Accountant (Treasury, Debt and Payment Acceptance) must be contacted in the first instance with the Deputy Director of Finance authority required in all instances.

ServiceNow is to be used (by emailing helpdesk@liverpool.ac.uk) to record all changes, problems and incidents concerning any component within the CDE. No work can be carried out on any CDE component unless a requirement to do so has been recorded in ServiceNow.

Customer payment card details (Primary Account Number, cardholder name, and expiry date) must not be requested on paper without the authorisation of the Financial Accountant (Treasury, Debt and Payment Acceptance).

In the event that payment cannot be taken during a telephone call for any reason (e.g. a Payment Entry Device unable to connect to the network, or a network outage) a different payment method must be used or the payment taken at a later date. Cardholder information must not be written down for later processing.

Payment card details must not be requested by email. Any unsolicited emails that are received containing payment card data must be securely deleted. The customer must be informed not to send payment card details via email again.

No staff member should handle cardholder data unless they have a business need and authorisation by the Finance Department to do so.

Operational Governance

The authority of the University's Finance Department must be obtained prior to any new service being commissioned which will involve the storage, processing or transmission of card data.

No components, including PEDs, web payment servers, tills, car park payment machines and vending machines are to be added to or removed from the CDE without the explicit consent of the University's Finance Department.

Where possible, the University will out-source the processing of electronic card payments to PCI DSS compliant third parties (service providers) who will process the transactions on the University's behalf. These can only be engaged on the authority of the University's Finance Department and they must be certified as being PCI DSS compliant.

This policy is mandatory and staff who process card payments must adhere to this policy. Failure to follow this policy may result in disciplinary action.

Protection of Payment Card Data

Access to payment card systems and data must be restricted to staff who are authorised and trained to process card payments.

Payment card data must not be disclosed to anyone who is not associated with the transaction.

Customer payment card details must not be entered or processed on any system or device other than those specifically provided by the University for this purpose.

Payment card details must not be captured, recorded, transmitted, processed or retained on any other University IT system or privately owned device.

Sensitive Authentication Data (SAD), which is made up of the 3 or 4 digit number printed on the back of a debit/credit card and the pin number, must not be recorded on paper or in digital format for any reason.

Vendor supplied default passwords, on the PED machines, must be changed to a more secure password and only shared with staff on a need to know basis.

Any historical card holder data discovered must be immediately destroyed. PCI DSS compliant methods of disposal which must be followed are:

- cross cut shredding,
- incineration,
- or pulping.

Card holder data may be rendered unreadable and a retention period agreed only with the specific consent of the Finance Department.

Found Debit/Credit Cards

Any debit or credit cards found on the University campus must be reported to the Finance Department and destroyed by close of business that working day.

Contact details and instructions on how to handle lost or found cards can be found in the PCI DSS Finance Operational Manual.

Destruction of the cards must follow the compliant methods highlighted above.

Access Control and Training

Each deployed PED must have a Merchant Owner (this will be the appropriate Line Manager) assigned to it. Merchant Owners must be agreed with the Finance Department in advance of any new PED deployment and are responsible for the following:

- Completing and passing the online PCI DSS training on a yearly basis.
- Being aware of the University's PCI DSS Policy and operational procedures.
- The physical security of the device and ensuring that PED's are stored in a secure manner.
- Overseeing the daily completion and logging of PED tamper checking.
- Keeping an up-to-date list of all staff (including casual staff) authorised to access each device.
- Making sure all new staff have completed PCI DSS training prior to taking any payments.
- Access to privileged user IDs (e.g. supervisor codes) must be restricted to least privileges necessary to perform job responsibilities.

The Finance Department will provide general training on the secure use of card data and an overview of the University's requirement to adhere to PCI DSS.

PCI DSS training will be provided by the following methods:

- E-Learning Module
- Face to Face sessions

All staff members involved in taking payments are required to confirm that they have completed the assigned training and understand the PCI DSS requirements for their role.

Internal Audit and Review

The Finance Department will regularly (at least once within a period of 12 months) undertake an audit/review of all card data operations to ensure that they are consistent with the objectives of this policy. If any breach of policy is identified, the Finance Department will make recommendations on what changes are required and potentially remove card machines if there are any repeat occurrences.

The University's Finance Department reserves the right to perform unannounced audits and request audit logs at any time.

The Finance Department will maintain an inventory log of all hardware within the CDE.

Review

This policy will be reviewed at least annually by the Financial Accountant responsible for Payment Acceptance; with any proposed changes initially approved by the Chief Financial Officer and then onto the relevant University committees. Updates will be applied as necessary in accordance with PCI DSS to reflect changes to business objectives, the risk environment, changes to the CDE and in-scope systems or the University's merchant level.

Third Parties

Any third party commissioned to handle cardholder information on behalf of the University must be approved by the Finance Department and CSD based on due diligence prior to engagement. Their compliance status must be assessed. 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 then each year thereafter.

Any contracts or written agreements with third party providers must make clear their responsibility for maintaining/protecting the University's compliance. The contracts/written agreements should state that:

- they are to remain compliant with PCI DSS throughout the term of the contract with the University;
- they are responsible for the security of cardholder data that they process on behalf of the University; and,
- the contract should be null and void should they fail to meet these requirements.

A full list of Third Party Payment Service Providers will be maintained by the Finance Department and the service providers' PCI DSS compliance will be checked by the Finance Department annually.

Contact Details

Position	Telephone	Email Address
Endowment and Compliance Officer	0151 794 3829	maguired@liverpool.ac.uk
Financial Accountant (Treasury, Debt and Payment Acceptance)	0151 795 1827	Peter.Sullivan@liverpool.ac.uk

Definitions and Glossary of Terms

Payment Card	A card backed by an account holding funds belonging to the cardholder, or offering credit to the cardholder such as a debit or credit card.
PCI DSS	The 'Payment Card Industry Data Security Standard'.
Stripe/Track Data	Information stored in the magnetic strip or chip on a payment card.
PAN	A 'Primary Account Number' is a 16 digit number embossed on a debit or credit card and encoded in a cards magnetic strip which identifies the issuer of the card and the account.
PIN	A 'Personal Identification Number' is a secret numeric password used to authenticate payment cards.
CAV2/CVC2/CVV2/CID	3-digit security code displayed on payment cards.
Cardholder Data	Payment card data including: Primary Account Number (PAN), name of cardholder, expiration date, service code.
SAD	'Sensitive Authentication Data' Full magnetic stripe data or equivalent on a chip, CAV2/CVC2/CVV2/CID or PIN.
CDE	'Cardholder Data Environment' compromises all aspects of payment card transactions including the technology, electronic resources, processes, procedures and people.
PDQ Machine	A credit/debit card swipe machine.
PED	PIN Entry Device.
QSA	'Qualified Security Assessor' is a person who has been certified by the PCI Security Standards Council to audit merchants for PCI DSS compliance.
ISA	'Internal Security Assessor' is a person who has been certified by the PCI Security Standards Council to assess their organisation's compliance.
Acquirer	An acquiring bank (also known simply as an acquirer) is a bank or financial institution that processes credit or debit card payments on behalf of a merchant.