



PCI DSS Compliance

Introduction

What is PCI DSS?

PCI DSS is the Payment Card Industry Data Security Standard. It is a series of over 300 rigorous technical, auditing, training and human resource controls designed to safeguard the storage, processing and transmission of payment card data.

Why must LSE comply?

LSE's payment acquirers have determined that *all* LSE's payment streams that involve credit and debit card transactions must be compliant with PCI DSS. Compliance must be re-assessed annually. Failure to comply could lead LSE to face unlimited fines or the withdrawal of its ability to take credit and debit card transactions.

Who owns the PCI DSS compliance?

- The Finance Division is accountable for the LSE's overall compliance.
- Departments and Divisions within individual payment streams are responsible for the compliance in their areas
 - The Departments and Divisions shall designate the business managers who are responsible to ensure such compliance.
- The PCI DSS Compliance Group provides assurance of the compliance via annual or ad-hoc audit.
- Audit findings must be addressed by the Departments and Divisions.

LSE implementation

This policy identifies levels of the standard that the School can and cannot meet with the current resources available to it..

Future Provision

Future business provision that will require credit and debit card payments must state as part of its Business Case what level of compliance is required, and provide the ongoing human and financial resourcing if it wishes to move beyond the current provision.

Policy Purpose

This policy consequently outlines the level of PCI DSS compliance that the School can currently achieve for any part of the business, given the current resources engaged in the activities mandated by PCI DSS and the primary focus of the School on teaching and research. The policy outlines the ownership and accountability of the PCI DSS compliance, and mandates that any business proposal breaching this level of compliance should:

- Be altered to fit the achievable level, or
- Provide the resources and change of School focus to be able to achieve a higher level of compliance, or
- Have the risk of non-compliance signed off by both the Chief Operating Officer *and* the Director of Finance.

Scope

- All activities within LSE that require the processing, storage or transmission of credit card data, whether or not any of those activities take place in house.
- All transmission of credit card data across the LSE network, where that transmission is initiated by a third party (e.g. a tenant).

Out of Scope

- Transmission of credit card data by a tenant over a leased line.
- Transmission of credit card data by a tenant that meets PCI DSS P2PE encryption requirements.
- Both the above points will instead be within any tenant's PCI DSS compliance scope.

Assumptions

- No significant increase in resources available to implement, monitor and maintain PCI-DSS compliance.
- No significant change in the School's business model away from a primary focus on teaching and learning.
- Sufficient resources are made available across the School to enable the PCI DSS Compliance Group to function effectively and achieve continued appropriate PCI DSS compliance.

Policy

Compliance overview

LSE is currently defined by its acquirer as a **Level 3** merchant.

As a result of this, LSE is required to fill in Self-Assessment Questionnaires (SAQ) annually to demonstrate its level of compliance with the PCI DSS standard. Different Self-Assessment Questionnaires are required for different payment categories, as laid out below. Different categories require compliance with different controls from the complete PCI DSS control set. Compliance with all controls is only required by PCI DSS SAQ D category payment card streams.

Achievable PCI DSS levels of compliance for LSE

LSE can achieve compliance at PCI DSS version 3.x for the following categories:

SAQ A: "applicable to merchants whose cardholder data functions are completely outsourced to validated third parties" and where "The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s)".

SAQ B: "applicable to merchants who process cardholder data only via imprint machines or standalone, dial-out terminals" and where "The standalone, dial-out terminals are not connected to any other systems within your environment".

SAQ P2PE-HW: "applicable to merchants who process cardholder data only via hardware payment terminals included in a validated and PCI-listed Point-to-Point Encryption (P2PE) solution".

SAQ C-VT: "applicable to merchants who process cardholder data only via isolated virtual payment terminals on a personal computer connected to the Internet."

Caveat

Achieving these levels requires careful planning and implementation, including enrolment of staff in a PCI DSS security awareness programme.

Compliance for any application or project is not achieved ***by default*** of other projects being compliant, and *always* requires a project and interaction with the PCI DSS Compliance Group.

Ownership of the compliance

The Finance Division is accountable for LSE's overall compliance. Departments and Divisions within individual payment streams are responsible for the compliance in their areas

New payment stream

Where a new payment stream is initiated, the business managers within the responsible Departments or Divisions shall:

- Notify the Finance Division of the new payment stream
- Update Finance Division with details of PDQ devices or other payment solutions
- Notify Finance Division of the acquirer and Payment Service Provider (PSP)
- Complete an assessment of the compliance with the guidance of the PCI DSS Compliance Group

The Finance Division shall

- Advise on the compliance submission requirements by the acquirer
- Update the PDQ inventory list and other payment stream information
- Obtain the Attestation of Compliance (AOC) of the acquirer and PSP

Change of existing payment stream

This can be change of acquirer, PSP, change and decommissioning of PDQ devices, change of card payment method, and the introduction of new technical solutions.

The business managers within the responsible Departments or Divisions shall:

- Inform the Finance Division of any changes within their responsible areas
- Consult the PCI DSS Compliance Group for an assessment of the continuous compliance status

The Finance Division shall:

- Update the PDQ inventory list and other payment stream information
- Obtain the AOC should there be a change of the acquirer or PSP
- Advise on the compliance submission requirements should there be a change of the

- acquirer
- Change or decommission the PDQ device where applicable

PCI DSS compliance audit

Annual audit

An annual PCI DSS compliance audit shall be commissioned by the PCI DSS Compliance Group.

Ad-hoc audit

Where a new, payment stream is introduced, or an existing payment stream is changed, an ad-hoc audit shall be carried out as appropriate. Where a new project involves card payment solution, a PCI DSS compliance audit shall be incorporated to the project plan.

Audit findings

Audit findings must be addressed by the responsible Departments and Divisions. The PCI DSS Compliance Groups tracks the remediation status and escalates to the School's senior management where necessary.

Unachievable levels of PCI DSS compliance

With the current levels of resource in IMT, the networking technologies currently in place, and a primary focus for those resources on supporting teaching and research activities, the following types of compliance are not achievable

SAQ A-EP: "e-commerce merchants with a website(s) that does not itself receive cardholder data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the consumer's cardholder data". Applicable where the cardholder data is entered into a merchant's website and then forwarded on to a PCI DSS compliant third party for processing.

SAQ B-IP: "applicable to merchants who process cardholder data only via standalone, PTS-approved point-of-interaction (POI) devices with an IP connection to the payment processor" and where "The standalone IP-connected POI devices are not connected to any other systems within your environment (this can be achieved via network segmentation to isolate POI devices from other systems)"

SAQ C: "applicable to merchants whose payment application systems (for example, point-of-sale systems) are connected to the Internet (for example, via DSL, cable modem, etc.)"

SAQ D: "applies to SAQ-eligible merchants not meeting the criteria for any other SAQ type"

Options for any project requiring unachievable levels of PCI DSS compliance

1. Outsource processing, storage and transmission of credit card data to a PCI DSS compliant company in such a way that LSE compliance can be achieved under levels defined in this policy.
2. Change the scope of the project so that LSE compliance can be achieved under levels defined in in this policy.
3. Provide resources for ongoing compliance at levels defined above. This would require major a re-orientation of School-wide resources
4. Gain explicit sign-off from the Director of Finance and the Chief Operating Officer in order to accept the risks (including LSE receiving unlimited fines and/or the removal of its ability to process credit and debit card payments) of non-compliance

Non-compliance

There may be circumstances where one element in the chain of compliance required by the PCI DSS standard cannot be achieved. For instance, while a room booking system may be hosted in a PCI DSS compliant environment, with the on-site components also successfully assessed against the appropriate SAQ, the Online Travel Agent (OTA) used as a payment channel may not be compliant, and may have no inducement to become compliant. In this case, the risk of using the OTA must be accepted by the School Secretary and one of either Director of Finance or the CFO, otherwise the payment channel must not be used.

Any instance where non-compliant payment streams are being used within LSE or by LSE tenants in such a manner as to bring LSE within the scope of their compliance requirements, the payment stream will be blocked by IMT from operating. This includes in cases where compliance is theoretically possible (i.e. cases that would fall into categories of compliance defined in 3.2) but where interaction and assessment have not taken place either by the PCI DSS Compliance Group or the PCI DSS project.

Tenants

As laid out in the 'IMT Support for LSE Tenants' paper endorsed by July 2014 Information Technology Committee, tenants must ensure all credit and debit card payments are processed using leased lines or using a PCI SSC-approved P2PE hardware solution, and are not otherwise passed across LSE's network.

Review and Development

This policy shall be reviewed and updated regularly by the PCI DSS Compliance Group as appropriate to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations. It will be endorsed by the Data, Technology and Digital Management Board.

Additional regulations may be created to cover specific areas.

Responsibilities

Divisions / Departments / Projects

- It is the responsibility of any division, department or project that is implementing a solution requiring the storage, transmission or processing of cardholder data to ensure that this solution is PCI DSS compliant, and meets with the achievable levels of PCI DSS compliance laid out in Section 3.2 of this policy
- Administering the PCI DSS training within the Divisions / Departments

Finance Division

- Responsible for the School's overall PCI DSS compliance
- Inventory of payment streams information and PDQ devices
- Change and decommissioning of PDQ devices
- Advise on acquirers' PCI DSS compliance submission requirements
- Obtain the up-to-date AOC of acquirers and PSP

Director of Finance / Chief Operating Officer

- Responsible for the explicit written sign-off for any non-compliant payment stream or non-compliant element of a payment stream in order for its operation to continue.
- Responsible for signing off the Self-Assessment Questionnaires for each payment stream.

PCI DSS Compliance Group

- Ensuring ongoing assessment of payment streams that have achieved PCI DSS compliance under the PCI DSS project.
- Compliance guidance for any future projects.
- Assessment of capability to meet Self-Assessment Questionnaire levels.
- Control of Security Awareness Programme.
- Assessing and reviewing PCI DSS-specific information security policies.
- Maintaining at least two PCI-qualified Internal Security Assessors within the School
- Stating what SAQ categories of compliance are feasible within the School

Business Improvement Unit

- Ensuring awareness of potential PCI DSS compliance is assessed by the Cyber Security Team at the appropriate Business Case stage
- Referring any projects (existing or potential) that require credit or debit card payments to the Compliance Group that have otherwise not been previously identified as requiring PCI DSS compliance

Cyber Security and Risk Team:

- Reviewing all Business Cases that require credit card payments
- Chairing PCI DSS compliance group
- Administering PCI DSS Awareness Programme
- Developing, maintaining and reviewing appropriate PCI DSS-focused Information Security Policies
- Authorising blocks on any non-compliant payment stream that has not been explicitly authorised for operating by the Director of Finance or the Chief Operating Officer
- Assessing the School's posture against the appropriate PCI DSS Self Assessment Questionnaire requirements and recommending to the Compliance Group where compliance is possible

Data, Technology and Digital Management Board

Responsible for approving data, technology and digital policies that do not address personally identifiable information.

School Secretary

Required, along with one of Director of Finance/Chief Financial Officer, to provide explicit sign off for any non-compliant payment stream or non-compliant element of a payment stream in order for its operation to continue

Review schedule

IT Services reference: ISM-PY-120

Review interval	Next review due by	Next review start
3 years	January 2024	December 2023

External document references

Title	Version	Date	Author
Payment Card Industry Data Security Standard Self Assessment Questionnaires (https://www.pcisecuritystandards.org/security_standards/documents.php?category=saqs)	N/A		Payment Card Industry

Contacts

Position	Name	Email	Notes
----------	------	-------	-------

Director of Cyber Security and Risk	Jethro Perkins	j.a.perkins@lse.ac.uk	
-------------------------------------	----------------	--	--

Communications and Training

Will this document be publicised through Internal Communications?	No
Will training needs arise from this policy	Yes
If Yes, please give details PCI DSS training must be undertaken for all staff handling credit card data.	