THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Technical

LSE PCI DSS Cardholder Data Environments

Information Security Policy

Introduction

This policy provides essential information for everyone tasked with handling credit and debit cards, credit and debit card data and the systems processing such data within LSE. It outlines key controls to maintain the integrity of the Cardholder Data Environments (DCE) that the System / Service Owners at LSE are responsible for implementing.

It is designed to ensure we can meet the standards required by the Payment Card Industry's Data Security Standard (PCI DSS), which LSE is obliged to meet in order to be able to process credit card payments.

It is limited **exclusively** to LSE's Cardholder Data Environments (CDE).

Within LSE's CDEs, beyond the requirements below, the stipulations of PCI DSS will apply (e.g. to the configuration of systems including Virtual Terminals). If there is any contradiction between PCI DSS and the below instructions, PCI DSS's required controls will take precedence.

Scope

All environments within the London School of Economics where credit and debit card data are handled, which are designated by PCI DSS as "Cardholder Data Environments".

The policy is applicable to all people within any LSE CDE, including but not limited to:

- LSE employees,
- 3rd parties acting on LSE's behalf,
- contractors that handle credit and debit cards,
- and LSE system owners within any CDE.

Other PCI DSS Compliance Requirements

LSE cardholder data environments and the systems within them are required to meet LSE's PCI DSS Compliance Policy, which outlines what PCI DSS levels LSE can and cannot meet.

Cardholder Data Definition

- The 16 digit card number (Primary Account Number - PAN)
- Issue and expiry dates
- Cardholder's name as shown on the card
- The three digit Card Verification Value (CVV).

Training

- All staff handling the cardholder data, including the third-party contractors and temporary staff, and LSE managers of those staff, must complete LSE's PCI DSS Moodle training on an annual basis.
- The business managers within the Departments and Divisions, who are responsible for the PCI DSS compliance in their areas, are responsible for administering the training course and ensuring all their staff handling cardholder data have completed the course annually.

Cardholder Data Handling

This section provides the minimum mandatory requirements that need to be applied by all employees, or contractors that handle or come across credit or debit cardholder data, in any format within the LSE environment.

Cardholder Data Treatment

- The PAN and CVV should never be written down or stored **anywhere**, whether on a piece of paper any electronic format, even if encrypted.
    - The only exception to this is storing the cardholder data temporarily (pre-authorisation) whilst you arrange to take the payment.
    - After the transaction the cardholder data *must be destroyed immediately*.
- If during the performance of your job you can see, by error or intention, a full card number when it is not required for you to do your job, please report this urgently to *Cyber Security and Risk Team* (dts.cyber.security.and.risk@lse.ac.uk).

Card Data Handling Requirements – what not to do

- Credit card data must **NOT** be stored on LSE systems or transmitted across the LSE network unless it is within a School-approved and commissioned PCI DSS solution.
- All employees, 3rd parties and contractors must **not** attach or use within LSE's CDEs devices including but not limited to remote access technologies, wireless technologies, removable electronic media, personal laptops, tablets, smartphones or personal storage media. Card data must NOT be sent via end user messaging technologies such as email, chat.

Handling Paper Documents Containing Card Data

- There are numerous cases where card data is legitimately stored on paper, be it a post order, chargeback letter, a fraud document, an exceptions report etc.
- This data needs to be retained, securely, only until the relevant transaction has been successfully achieved. Once the transaction is complete, the card data must be destroyed with an electronic shredder with cross-cut method.

Vigilance and Awareness

- Credit card data can be inadvertently received or otherwise discovered on printers, on a desk, on a screen, in email, in the 'recycle bin', in a temporary file, memory swap files etc. Where it is so discovered you must:

- secure the data, e.g. lock your screen or lock it in your desk,
- report it to your manager and
- report the incident to the *Cyber Security and Risk Team* immediately via dts.cyber.security.and.risk@lse.ac.uk.

Physical Security

Device Checking

- An up-to-date list of Point of Interaction (POI) devices must be maintained, including:
  - Make and model of the device
  - Location of the device
  - Device serial number and other means of unique identification
- POI must be periodically inspected by staff to look for tampering (for example, addition of card skimmers to devices) or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device)
- The PCI DSS user awareness training, accessible via Moodle, provides information on how to be aware of suspicious behaviour and to report tampering or substitution of devices
- The business area is advised to maintain a device checking log;
- Any tampering or suspicion that tampering has taken place must be reported to the *Cyber Security and Risk Team* via dts.cyber.security.and.risk@lse.ac.uk

Personnel Checking

- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices
- Do not install, replace, or return devices without verification
- Be aware of suspicious behaviour around devices (for example, attempts by unknown persons to unplug or open devices)
- Report suspicious behaviour and indications of device tampering or substitution to the *Security Office* on extension 2000

Entry control

Appropriate facility entry controls must be in place to restrict physical access to systems in the CDE.

Device decommissioning

Devices that are no longer in use must be decommissioned via the Finance Division, and must not be connected to the School's network.

Third-Party Due Diligence

The business areas handling card details must maintain an updated list of TPSPs with a description of their services provided. Written agreement with the TPSPs must exist which includes the acknowledgement from the TPSPs that they are responsible for the security of account data they process.

Due diligence process must exist prior to engagement with the TPSPs. Information is maintained about the division between LSE and the TPSPs of responsibilities around meeting the PCI DSS requirements.

Monitoring mechanisms must exist to ensure the TPSPs' PCI DSS compliance status is up-to-date and renewed at least once every 12 months

Incident response

Incident response where there is a suspected breach shall follow the Information Security Incident Response Plan, invoking the School's Major Incident Initial Recovery Plan (MIIRP) is required.

Further LSE Policies

LSE Policies affecting the entire LSE – not just the LSE cardholder data environment – can be found at: https://info.lse.ac.uk/staff/services/Policies-and-procedures. Where contradictions arise within the cardholder data environment, this policy takes precedent.

Document Control

Policy owner:	Director of Cyber Security and IT Risk Management
Policy author:	Jethro Perkins
Responsible office:	DTS
Approving body:	Policy Committee
Effective date:	13 May 2026
Date of next review:	13 May 2029
Review schedule:	1 year

Version history

Version	Date	Approved by	Details of amendments
v1.10	13 May 2026	PCI DSS working group	Minor updates.

Version History

Date	Version	Comments
01/10/25	1.9	Previous authorised version.

Contacts

Position	Name	Email	Notes
Director of Cyber Security & Risk Management	Jethro Perkins	j.a.perkins@lse.ac.uk	

Communications and Training

Will this document be publicised through Internal Communications?	Yes – on website.
Will training needs arise from this policy	Yes
PCI DSS Awareness training must be completed by all staff in scope of the CDE	