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 (CDE) that the System Owners 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.

Scope

All CDEs within the London School of Economics where credit and debit card data are handled.

The policy is applicable to all LSE employees, 3rd parties acting on LSE's behalf and contractors that handle credit and debit cards, System Owners of the CDE.

Oher PCI DSS Compliance Requirements

LSE cardholder data environments are required to meet LSE's PCI DSS Compliance Policy.

Compliance with this Policy

Compliance with this policy is mandatory. Failure to follow this policy will be considered as gross misconduct and may result in disciplinary action, up to and including summary dismissal and, in extreme cases, legal prosecution. The manager of each business area that requires compliance is responsible for:

- Developing clear processes and procedures for how their staff are to perform their day-to-day activities in accordance with these policies
- Ensuring that their staff understand and adhere to these processes and procedures

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.

POLICY

Credit Card 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. Furthermore any third party that uses or accesses any of LSE's credit cardholder data, either physically or logically must also comply with this section.

Training

- All staff handling the cardholder data, including the third-party contractors and temporary staff, and LSE managers of those staff, must complete the 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 Definitions and Requirements

- 'Cardholder Data' means:
    - The long 16 digit card number (Primary Account Number - PAN)
    - Issue and expiry
    - Cardholder's name as shown on the card
    - The three digit security code (generally on the back of the card) known as the Card Verification Value (CVV).
- The PAN and CVV should be handled with great care and should never be written down or stored **anywhere**, whether on a piece of paper, a form, in a database, in a spreadsheet or any other electronic format, even if encrypted.
    - The only exception to this is where you are taking a payment and need to store the cardholder data temporarily (pre-authorisation) whilst you arrange to take the payment.
    - After the transaction has been authorised the cardholder data *must be destroyed immediately*.
- No staff member is allowed to handle cardholder data without explicit, written authorisation in their job description.
- Cardholder data must be handled only in such a manner as is explicitly authorised by job roles. Access to the CDE is assigned to users based on such job roles with least privileges necessary to perform job responsibilities.
- 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) so that procedures can be changed accordingly.
- If however your job requires that you need access to cardholder data and it is not mentioned in your job description, please report this to your line manager so that they can update your job description and confirm it with HR.

Card Data Handling Requirements

- Card data should 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 or contractors shall not attach or use within LSE's CDE network devices including but not limited to modems, remote-access technologies, wireless technologies, removable electronic media, personal laptops, tablets, smartphones or personal storage media (e.g. memory sticks). Card data should NOT be sent via end-user messaging technologies such as e-mail, instant messaging or chat.
- Credit card data is classified as confidential, in accordance with the LSE Information Classification Standard.
    - It must *never* be stored electronically outside School-approved, PCI DSS certified payment systems.
        - This includes but is not limited to storage on local hard drives, smart phones, memory sticks or other external or mobile media, or cloud storage.
    - It must not be stored on paper unless as otherwise described in the 'Handling Documents Containing Card Data' section below.
    - In the first instance, report **any** credit card number storage to the *Cyber Security and Risk Team* via dts.cyber.security.and.risk@lse.ac.uk.

Any card data on LSE systems must be reported to the Cyber Security and Risk Team via dts.cyber.security.and.risk@lse.ac.uk immediately upon discovery.

- Copying and printing of existing card data is expressly forbidden.

Handling 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, in lockable storage where access must be restricted, 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.
    - A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.

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.

PCI-DSS Cardholder Data Management

This section provides the minimum mandatory requirements that need to be applied to all data created, transmitted, stored or managed by LSE within the Cardholder Data Environment (CDE); be that data in hard (e.g. paper) or soft (e.g. logical) formats. Any third party that uses or accesses any of LSE's data within the CDE, either physically or logically must also comply with this policy.

Revenue Protection Correspondence

- This refers to all correspondence relating to charge-backs, revenue protection and fraud prevention. These will typically be paper copies and must be destroyed by cross-cut shredding once they have met their retention period.

Information Systems and Physical Location Documentation

- All documentation relating to Information Systems within the PCI DSS CDE, including network diagrams, firewall access, system configuration, system passwords and backup documentation must be held securely with privileged access.

Physical Security

Device Checking

An up-to-date list of Point of Interaction (POI) devices is maintained including

- Make and model of the device
- Location of the device
- Device serial number or other methods of unique identification
- The Point-of-interaction (POI) devices 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 device surface, 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 PCI DSS poster provides a summary of what to look for while inspecting a device; the poster can be requested from dts.cyber.security.and.risk@lse.ac.uk
- The business area is advised to maintain a device checking log; the template can be requested from dts.cyber.security.and.risk@lse.ac.uk
- 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

Device update

Firmware and Operating System updates must be applied timely, based on the instructions of the device provider.

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.

Entry control

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

PCI-DSS Cardholder Data Environment (CDE) Security

This section outlines controls that need to be applied to the Cardholder Data Environment (CDE) to meet the PCI DSS. System Owners are responsible to implement these.

User Access Management

Access is assigned to users based on ‘need to know’ and ‘least privilege’.

All users are assigned a unique ID before access to system components or cardholder data is allowed*

Shared account should be avoided but only used as necessary on an exception basis provided:

- Business justification for use is documented and explicitly approved by the Cyber Security and Risk team
- Individual user identity is confirmed before access to an account is granted
- Every action taken is attributable to an individual user

Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects must be subject to appropriate approval. Access for terminated users is immediately revoked.

Authentication must meet the School’s Password Policy and MFA policy. If MFA is not used the password shall be changed every 90 days.

Remote administrative access into the CDE must have MFA implemented and is encrypted using strong cryptography.

* [note – this does not apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals)]

Secure configuration

Any default password provided by the vendor that’s present at the system components of the CDE must be changed. Vendor default account must be removed or disabled.

Where payment is authorised via Virtual Terminals, the system security parameters must be configured appropriately for all components that are connecting to the CDE; only necessary services, protocols, daemons, and functions of the system components are enabled. Any exception must have business justification which is properly documented with additional security features in place to mitigate the risk.

Security of Virtual Terminals

The virtual payment terminal solution (VT) must be PCI DSS-compliant and only accessed via a computing device that is isolated in a single location and not connected to other locations or systems. Security controls must be implemented on such devices.

Ingress and egress traffic to and from the CDE must be restricted to that is only necessary with all other traffic explicitly denied.

No wireless environment shall be connected to the CDE.

An anti-malware solution is deployed on all system components and is kept current via automatic updates. Periodic or real-time scans must be carried out. Audit logs for the anti-malware solution are enabled and retained for at least 12 months, with at least the most recent three months immediately available for analysis.

Technical controls must in place to prevent end users from disabling or altering the anti-malware mechanisms.

Vulnerability Management

The Cyber Security and Risk team shall keep updated with new security vulnerabilities that are identified using industry-recognised sources for security vulnerability information, including alerts from international and national Computer Emergency Response Teams (CERTs)

All system components are protected from known vulnerabilities by installing applicable security patch/updates following the School's Patch Management Policy

For LSE hosted e-commerce website*, external vulnerability scans are performed at least once every three months by PCI SSC Approved Scanning Vendor (ASV) with rescans as necessary following changes to fix any noted vulnerabilities

For Virtual Terminals system security configuration should be independently assessed on an annual basis.

*[Note - This refers to the card-not-present transactions through public facing website where card payment feature is outsourced to the third-party service provider (TPSP)]

Integrity check

For LSE hosted e-commerce site, or an LSE customised third party hosted site, integrity checks should be carried out on the page that provides the URL of the TPSP's payment page, to:

- Confirm that each script is authorised
- To assure the integrity of each script

An inventory of all scripts shall be maintained with written justification as to why each is necessary.

Third-Party Due Diligence

The business areas handling card details must maintain an updated list of TPSPs with 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 mechanism 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 School's Information Security Policy and the Incident Response Plan.

Acceptable Use

- The information system facilities of LSE are provided for business purposes and use of these facilities must be authorised in accordance with the '**Conditions of Use of IT Facilities**' and the **Access Control Policy**.

- It is mandatory for all users of systems and equipment within LSE's cardholder data environment to adhere to the terms of 'Conditions of Use' and the Access Control Policy.
- Employees and other users who deliberately breach the terms of this policy will be subject to disciplinary action up to and including summary dismissal. Serious offenders are liable for prosecution under the Computer Misuse Act 1990.
- Every user is responsible for the proper use of the equipment they have been assigned and must comply with LSE's policies and all applicable laws.
- Any IT Systems equipment not belonging to LSE should not be installed on the LSE network within the cardholder data environment, unless permitted, with the authorisation of the Head of *Information Security*. Any such equipment must adhere to the standards within this document.

Responsibilities

All users within the cardholder data environment include all permanent (direct hire), temporary and contract staff who use LSE computer systems. All users must use the IT systems, information and equipment in accordance with LSE security policies and procedures. Users are responsible for:

- Familiarising themselves with and adhering to the policies and procedures applicable to their area of responsibility;
- Protecting LSE equipment issued to them against unauthorised access and damage;
- Using LSE equipment for business purposes only;
- Protecting LSE and customer information against unauthorised access and loss;
- Not disclosing their passwords or sharing user accounts;
- Ensuring that LSE IT systems and facilities (e.g. email or Internet) are used in accordance with the 'Conditions of Use of IT Facilities at LSE';
- Clearing desks of all sensitive material and logging off or locking workstations at the end of the day and when leaving their desk;
- Not removing equipment, information or any other LSE property from the organisation's premises without authorisation;
- Not connecting personal equipment to LSE networks within the cardholder data environment (CDE);
- Not installing, copying or modifying any software on LSE equipment without authorisation;
- Immediately reporting security incidents to the Cyber Security and Risk Team (dts.cyber.security.and.risk@lse.ac.uk).
-

Business managers of areas that are handling the cardholder data, or Systems owners of the CDE, are responsible to implement and maintain procedural and technical controls to ensure this Policy is met. The School's PCI DSS Compliance Group plays the audit and assurance role to ensure the business managers have implemented such controls.

Review schedule

IT Services reference: ISM-PY-120

Updated: 31/08/22 by Jia Fu, Head of Information Security

Version: 1.6

Review interval	Next review due by	Next review start
Annually	Aug 2023	July 2023

External document references

Title	Version	Date	Author
Information Security Policy	3.21	01/06/20	Jethro Perkins
Information Classification Standard	4.3	03/12/18	Jethro Perkins
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 annually for all staff handling credit card data, and managers of these staff.	