

**Payment Card Industry Data Security Standard – Compliance Policy**

IMPLEMENTATION DETAILS

Policy: PCIDSS-002 v3.2

Title: PCIDSS Compliance Policy

Change Control:
Change control added
Version - PCIDSS-001 changed to PCIDSS-002
Document Owner updated from Garry Robertson to John Bannaghan
Last Review Date updated
3.1- Reference to standard 3.0 updated to 3.2. High Level Overview updated.
5.1 - Hyperlinks updated

Document Owner – John Bannaghan Systems Accounting Section.

Last Review Date 28/4/2017

**1. Introduction**

1.1. All staff members who have roles which require access to cardholder data, or roles which make it possible to obtain access to cardholder data, have a responsibility to protect that data. This document lays out a set of requirements to which all University staff that may have access to cardholder data, must adhere to.

1.2. The University is required to comply with the Payment Card Industry Data Security Standard (PCI DSS), a worldwide information security standard defined and published by the Payment Card Industry Security Standards Council. The standard was created to help payment card industry organisations that process card payments prevent payment card fraud through increased controls around data and its exposure to compromise. The standard applies to all organisations that hold, process, or exchange cardholder information. Organisations that fail to meet the compliance requirements risk losing their ability to process card payments along with being fined. This standard is therefore part of the University’s Financial Regulations and the University must ensure that it’s business processes and technical systems conform with the PCI DSS standard.

1.3. Definitions

***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” (see above).

***Stripe / track data*** - Information stored in the magnetic strip or chip on a payment card.

***PAN*** - A “Primary Account Number” is a 14 or 16 digit number embossed on a debit or credit card and encoded in the card's 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 and service code.

***Sensitive Authentication Data*** - Full magnetic stripe data or equivalent on a chip, CAV2/CVC2/CVV2/CID or PINs/PIN blocks.

***Cardholder Data Environment (CDE)*** - Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.

***PDQ Machine*** – A credit card swipe machine.

***PED*** – PIN Entry Device.

***Qualified Security Assessor (QSA)*** – A person who has been certified by the PCI Security Standards Council to audit merchants for Payment Card Industry Data Security Standard (PCI DSS) compliance.

1.4. This document includes statements on:

* Scope
* PCI DSS outline
* PCI DSS compliance policy
* Authorisation and responsibilities
* Payment card processing
* Electronic cardholder data handling
* Paper cardholder data handling
* Retention of cardholder data
* Physical security of payment card processing equipment

**2. Scope**

2.1. Policy statements in this document apply to:

* All staff within the University involved in payment card processing or having access to cardholder data.
* All payment card processing arrangements across the University.
* All systems which store, process or transmit cardholder data.
* Both manual and IT-based payment card processing

**3. PCI DSS outline**

3.1. PCI DSS is a set of security standards introduced by VISA and Mastercard (endorsed by other card schemes) that applies across the card payment industry worldwide. It will help safeguard cardholder information, improve consumer confidence and reduce the risk of fraudulent transactions. These rules are compulsory for all organisations handling any aspects of card transactions and who have access to cardholder information.

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 (v3.2) are summarised under 6 headings and 12 requirements: Full PCI DSS details are available at <https://www.pcisecuritystandards.org/document_library>



**4. PCI DSS compliance policy**

4.1. All University card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS).

4.2. This policy document forms part of University of Edinburgh policy on card payments and directly meets the PCI DSS requirement to “Maintain a policy that addresses information security for all personnel”.

4.3. Card processing activities must be conducted as described herein and in accordance with the PCI DSS standards. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.

4.4. All relevant staff must be made aware of the importance of cardholder data security and must be aware of the requirements stated in this policy.

4.5. This policy shall be reviewed annually and updated as required to reflect changes to business objectives, to the risk environment or to PCI DSS.

(Note: Certain requirements stated in this policy are not part of the PCI DSS itself; however, are included to facilitate University PCI DSS compliance.)

**5. Authorisation and responsibilities**

5.1 All staff using Online Payment systems must comply with:-

Online Payment Policy [http://www.wiki.ed.ac.uk/display/Finance/Online+Payment+Policy](http://www.wiki.ed.ac.uk/display/Finance/Online%2BPayment%2BPolicy)

Information Security Policy
<http://www.ed.ac.uk/information-services/about/policies-and-regulations/security-policies/security-policy>

Fraud and Misappropriation Policy [https://www.wiki.ed.ac.uk/display/Finance/Fraud+and+Misappropriation+Policy](https://www.wiki.ed.ac.uk/display/Finance/Fraud%2Band%2BMisappropriation%2BPolicy)

Financial Systems Policy [https://www.wiki.ed.ac.uk/display/Finance/Financial+Systems+Policy](https://www.wiki.ed.ac.uk/display/Finance/Financial%2BSystems%2BPolicy)

5.2 Staff or departments must not plan, commission, use or modify any payment card processing procedures or systems without consultation with the Finance Department (Cash Office Manager). 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.

5.3 The Finance Department is responsible for managing PCI DSS compliance across the University and may remove any payment card processing activity causing unacceptable risk.

5.4 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.)

5.5 The Finance Department along with Heads of College/Schools/Departments are jointly responsible for making all relevant staff aware of the importance of cardholder data security strategy and the requirements stated in this policy. Line managers are responsible for ensuring that all new and existing staff receive documentation and basic training in PCI DSS requirements.

5.6 Departments/Areas working in a card payment environment, must nominate a locally responsible person to maintain PCI DSS records/compliance for that area.

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

5.8 The Finance Department is responsible for ensuring that Central Finance system service providers dealing with cardholder information are PCI DSS compliant.

5.9 A list of all staff currently authorised to use devices to process payment cards, such as tills, PEDs, PDQ machines etc. must be maintained by the department responsible for providing that service and a copy submitted to the Finance Department (Cash Office Manager) who will maintain a central register of authorised users.

5.10 The Finance Department will maintain a wiki page listing all locally responsible PCI DSS contacts and a list of all authorised PDQ users.

**6. Payment card processing**

6.1. Staff must not request or agree to accept transmission of any payment card information from University customers via email or other end-user messaging technologies. Any cardholder data received in this way should be deleted immediately.

6.2. Staff must not ask for 3D Secure or Verified by Visa codes, when processing through an online interface.

6.3. Any electronically stored legacy payment card data, or data stored in error, must be deleted.

6.4. 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 tills must not show or print details of the full PAN. (The first six and last four digits are the maximum number of digits that may be displayed.)

6.5. Full credit card numbers may only be viewed by authorised staff with a need to see them as part of their duties.

**7. Electronic cardholder data handling**

7.1. 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. Note: This applies to all types of payment card data including PAN, PIN, three-digit security codes and full track data.

7.2. Staff must not transfer cardholder data via email, or other end-user messaging technologies, whether or not encrypted.

7.3. Systems which are specifically designed and deployed to transfer cardholder data electronically such as tills, PEDs and PDQs and outsourced e-commerce solutions must do so in a way that meets PCI DSS compliance requirements. When planning and deploying such systems, the Finance Department will work with departments, IT Services, system vendors and QSAs as appropriate to achieve and maintain PCI DSS compliance.

7.4. Computers being used by University staff to access outsourced e-commerce solutions, such as WPM on behalf of customers must automatically run updating anti-virus software.

**8. Paper cardholder data handling**

8.1. The aim should be to reduce and preferably eliminate the need for cardholder data to be held in paper form. Processes should be regularly reviewed to determine whether online payment processes can be implemented to replace paper-based procedures.

8.2. Sensitive card authentication data must not be recorded on paper.

8.3. Cardholder data stored on paper, which must exclude sensitive authentication data, must be:

* In a locked cabinet whenever not in use or supervised. Offices housing such cabinets must also be locked when not occupied.
* Destroyed when no longer required by secure onsite cross-cut shredding, incineration or pulping. (Paper records holding unwanted payment card information must be locked away until destroyed.) (also see 9.2 below.)
* Marked to distinguish it from other paperwork. Departments may use their own classification and marking system for cardholder data paperwork. A suitable solution would, for example, be to use distinctively coloured stationery.

8.4. Where it is necessary to transfer paper cardholder data within the site: The only acceptable method is delivery by hand during office hours. The internal mail system must not be used.

8.5. Incoming mail containing cardholder data from outside the University may be received through the internal mail system. Where there is the expectation that mail may contain card data, two members of staff should be involved in the mail opening process. However, regard should be had to Section 8.1 with a view to eliminating the need for paper-based processes.

8.6. There should not be any requirement for cardholder data to be sent via an external postal service. However, if in exceptional circumstances a need should arise, approval must be first obtained from the Director of Finance.

8.7. A record must be kept detailing any transfer of payment card data within the University and by external postal service should a need arise. Management approval is required prior to the transfer.

**9. Retention of cardholder data**

9.1. Cardholder data, excluding any sensitive authentication data, may be retained if there is a business need, only as paper records.

9.2. Except in exceptional circumstances and with explicit approval of the Finance Department, retained cardholder data for any financial year (August-July) must be destroyed by the end of the following January.

**10. Physical security of payment card processing equipment**

10.1. Devices used to process payment cards, such as tills, 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. (Small devices such as PDQs must be locked away and larger devices such as tills must be in rooms with restricted access when not in use.)
* Be subjected to routine visual inspection, preferably each day or before use. Equipment, cabling 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.

10.2. Out-of-hours visitors to areas giving access to payment equipment must be supervised and details of such visits must be logged.

Failure to comply with University Policy may lead to disciplinary action.