

**PCI DSS Policy**

|  |  |
| --- | --- |
| Author & Title: | Claudia McLean, Chief Accountant & Head of Financial Services |
| Responsible Director: | Sue Beecroft, Executive Director of Finance & Resources |
| Last Update: | October 2022 |
| Review Date: | March 2021 |
| Next Review Due: | October 2023 |
| Version:  | 4 |

**Index**

|  |  |  |
| --- | --- | --- |
| **Section** | **Contents** | **Page** |
| **1** | **Introduction and policy statement** | **3** |
| **2** | **Security breach of data** | **3** |
| **3** | **On-line payments** | **3** |
| **4** | **Card processing terminals** | **4** |
| **5** | **Storage** | **6** |
| **6** | **Refunds** | **7** |
| **7** | **Compliance and monitoring** | **7** |
| **8** | **Training** | **8** |
| **9** | **Points of contact** | **8** |
| **10** | **Glossary of terms and key** | **9** |
| **11** | **Appendix** | **9** |

**1.**

**Introduction**

1.1

**The Payment Card Industry Data Security Standard** (PCI DSS) is a worldwide information security standard, created to help organisations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. It applies to all organisations which receive process, store and pass cardholder information.

The University is liable to fines from its merchant bank should it fail to comply with PCI DSS.

This policy is required to ensure compliance with Point 12 of the Standard. For full details please see Appendix in Section 11.

This policy is mandatory to all staff. Failure to comply with this procedure may result in disciplinary action. Budget Managers are responsible for ensuring staff awareness of the policy and that it is adhered to and should also be aware of the ***financial regulations*** which can be found at:

<https://www.hope.ac.uk/gateway/staff/stafffinance/financeformspoliciesandprocedures/>

**2.**

**Security Breach of Data**

2.1

In the event of there being a security breach of data, Staff must contact the appropriate member of Finance Staff – See Point 9. The Finance member of Staff must then contact parties listed below and ensure that card processing is discontinued immediately

WPM –Telephone 0344 264 1580

Worldpay – Fisglobal.com

Worldpay – Relationship Executive: Carl Graham

Tel: 0330 333 5153

Email: carl.graham@fisglobal.com

**3.**

**Online payments**

3.1

In the first instance customers should make payment for goods and services online by using the Online Store and Online Payment Pathway facilities provided by the University. This is the preferred method and best practice for taking payments. For further information please contact the nominated person at Point 9.

3.2

On completion of a successful payment the online system being used will automatically generate an email payment confirmation to the customer. This is the only Finance confirmation document that will be received by the customer for the payment.

3.3

If a customer’s payment has been unsuccessful or declined, the customer in the first instance should contact their card provider.

3.4

If a customer faces difficulty in making a payment then staff assistance can be provided. The customer should be assisted at the time of the enquiry, whether this is in person or via the telephone. If the payment problem cannot be resolved, then the customer should provide a number to be called back on at a suitable time.

3.5

Card details must **NEVER** be written down by any member of staff for a future payment attempt.

3.6

For all card details which are processed through an online system, no card details are retained by the University. There is no University access to full card details as this information is stored on an external encrypted PSP (Payment Services Provider) server.

**4.**

**Card Processing Terminals – PDQ (Payment Data Quickly)**

**4.1**

**Obtaining a PDQ Machine**

4.1.1

To request a PDQ machine for your Department, please contact the nominated person at Point 9 to discuss your requirements. A business case and value for money evaluation will be undertaken prior to approval.

4.1.2

The set up your PDQ machine will be overseen by a nominated person at Point 9, to ensure the instructions provided by our Merchant bank (WorldPay/fisglobal) are complied with.

***Note: Upon installation the default password should be changed immediately and must be changed 12 months thereafter.***

**4.2**

**Use of PDQ Machine**

4.2.1

PDQ payments should be processed for customer present transactions only. If the customer is not present then the Online Store or other online payment pathway facilities should be used for the payment. The only exception to this is student finance who can take payments over the telephone and will immediately input the card details into the WPM pay now system using the virtual keypad.

**4.3**

**Customer Present With Card**

4.3.1

When the customer is present the card payment should be processed through the PDQ machine according to the machine instructions.

4.3.2

If the transaction is successfully processed, the merchant copy should be stored securely (see Section 5) and the customer copy given to the customer if requested. The retained copy **must not** display the full 16 digit PAN (Permanent Account Number).

4.3.3

If the transaction is declined, the customer should be advised immediately. The option of paying with a different card should be offered. The customer copy stating that the payment was declined should be given to the customer and the merchant copy should be stored securely (see Section 5).

**4.4**

**By Telephone**

4.4.1

Where card details are provided during a telephone call, these must be processed directly into the PDQ, Online Store, other online payment facilities at that time and **must not** be written down or noted anywhere.

4.4.2

When card details are being provided in a telephone call these **must not** be repeated back to the customer in such a way as to be audible to third parties.

4.4.3

If it is not possible to submit the card details immediately then a call back must be requested or offered. Please refer to Point 3.5.

**4.5**

**Card Details Received In Writing**

4.5.1

Some customers may provide their card payment information in writing for processing i.e. in a letter, email or by booking form. Customers should be deterred from providing the information in this manner as it is not secure and there is no guarantee that these details have not been intercepted prior to being received by the University.

4.5.2

When details have been received by email or other end-user messaging technology they **must** **not** be processed. The card details should be deleted as soon as possible (from the in-box and the deleted mail folder) and within the same day they are discovered. If the email requires a response, the card information provided **should not** be contained within the reply.

**4.6**

**PDQ Records**

4.6.1

If the transaction is successfully processed, the merchant copy should be stored within the till drawer or cash box for the duration of the working day.

4.6.2

If the transaction is declined, the customer should be advised immediately. The option of paying with a different card should be offered. The customer copy stating that the payment was declined should be given to the customer and the merchant copy should be stored within the till drawer or cash box for the duration of the working day. When storing merchant copy receipts these must be treated as a confidential document and should be marked accordingly.

4.6.3

The PDQ machine transaction slips are to be sorted into card type and must be reconciled to the PDQ Z report at the end of business each day.

4.6.4

Merchant copies of PDQ receipts must be kept for a length of time which reflects good commercial practice, audit and refund requirements. The length of time which they are kept is detailed in the signed procedure document which each department has produced. For Chargeback and PCIDSS requirements, Worldpay require that all customers retain copies of receipts for at least 18 months from the transaction date. However, for operational purposes and the volume of transactions the Catering Department will retain their receipts for a shorter period of time. Worldpay do not have a policy regarding the timescales of how long a refund can take place after the original sale date.  Although they always would advise to issue a refund onto the same card that the sale was taken. Confidential shredding should always be used when destroying merchant copies.

4.6.5

If the 16 Digit PAN number is displayed on any retained merchant copy receipts then you **must** contact the nominated person in point 9 to instruct the changes of the parameters on the PDQ machine. The University does not allow the full 16 digits to be displayed.

**5.**

**Storage**

5.1

Storage of card details on PC’s in any format (email, access databases, excel spreadsheets, pen drives, etc.) breaches the Security Standard Regulations and effectively makes the University non-compliant. This could result in significant fines from ICO (Information Commissioners Office), Visa and MasterCard. In addition, the University may be barred from accepting cards or the fees may be increased by the Merchant bank to process cards. The most common method of fraudsters obtaining card details is by hacking into computers which stores cardholder information. As well as non-compliance under PCI DSS the University may not be complying with GDPR and therefore subject to additional fines under GDPR regulation.

5.2

Safe and secure storage of merchant copies is defined as:

* Within a safe or
* Within a locked Cash Box or
* Within a locked drawer

5.3

Merchant copies of PDQ receipts must be retained by the University within each relevant department for the time stipulated in the departmental procedure document for audit purposes. Merchant copies that have been held for the stipulated time can therefore be destroyed by confidential shredding. The merchant copy receipts are to be filed chronologically and stored in a secure environment as detailed in Point 5.2.

**6.**

**Refunds**

**Online Refunds**

6.1.1

The refund must be approved by an authorised signatory for the cost centre and then passed to the appropriate administrator in point 9 for the relevant payment pathway. The appropriate system is accessed and the refund is processed back to the source card from which the original transaction was authorised.

6.1.2

If a transaction is older than 180 days (6months), a refund cannot be processed on to the source card for the original transaction. This is due to security measures implemented by the Payment Service Provider (PSP). In this instance the customer should be contacted for alternative details for the refund to be processed by BACS.

**PDQ Refunds**

6.2.1

PDQ refunds require to be authorised on the PDQ machine using a “Supervisor Card”. This card must be kept securely by an authorised signatory.

6.2.2

The refund must be approved by an authorised signatory for the cost centre. The refund should then be processed through the PDQ machine back onto the source card from which the original transaction was authorised.

6.2.3

If the source card is unavailable for the refund to be processed then the customer should be contacted for alternative details for the refund to be processed by BACS. A refund must never be processed onto a card that is not the source transaction card.

**7.**

**Compliance and Monitoring**

7.1

All card processing activities of the University must comply with the PCI DSS. No activity or technology may obstruct compliance with the PCI DSS.

7.2

All Units must adhere to this Policy to minimise the risk to both Customers and the University. Failure to comply will render the University liable for fines and may also result in Visa and/or MasterCard preventing transactions from being processed by the University.

7.3

A third party company is under contract to monitor University compliance with PCI DSS through annual Self-Assessment Questionnaire (SAQ) reviews.

7.4

Through regular meetings with Supervisors and relevant staff the PCI working group will conduct regular checks that identifies threats, and vulnerabilities, and results in a formal risk assessment.

7.6

The University will contractually require all third parties with access to cardholder data to adhere to PCI DSS requirements. These contracts will clearly define information security responsibilities for contractors.

7.7

If you have difficulties implementing or complying with any aspect of this policy, you should contact the appropriate member of University staff – see Point 9.

7.8

The University must ensure the sharing of information from a Personnel perspective for example, when an employee leaves or changes their role within the University. Access to specific areas is controlled.

7.9

The purchase of any equipment from a third party to be used for the processing of card information should only be purchased with the approval of the PCI team (Point 9).

**8.**

**Training**

8.1

Staff Induction **-** New members of staff are requested to familiarise themselves with the Financial Regulations.

8.2

It is the duty of the Budget Holders to ensure that all their staff that has contact with credit/debit card details are trained and made aware of PCI DSS. Training material is located within the Staff Finance/ Finance Forms Policies and Procedures section of the university website.

<https://www.hope.ac.uk/gateway/staff/stafffinance/financeformspoliciesandprocedures/>

8.3

External training – Budget Holders, Staff in Supervisory roles and others may be requested to complete the Foundation training provided by the PCI DSS SIG. There may be a requirement in some departments for Staff to also attend the Practitioner training provided by the SIG.

8.4

Internal training – This training is for all Staff and accessible via the Staff Finance/ Finance Forms Policies and Procedures section of the university website.

**9.**

**POINTS OF CONTACT**

9.1

**PCI Working Group**

Mark Pringle Ext 3487 pringlm@hope.ac.uk

Ann Rimmer Ext 3280 rimmera@hope.ac.uk

Claudia McLean Ext 3237 mcleanc@hope.ac.uk

9.2

Online Store and Online Payment Pathways Ann Rimmer Ext 3280 rimmera@hope.ac.uk or Jamie Maguire Ext 3833 maguirej@hope.ac.uk

9.3

Student Finance Office (Paynow) Ext 3339 lynchm@hope.ac.uk

9.4

Financial Accounts Claudia Mclean Ext 3237 mcleanc@hope.ac.uk

9.5

Procurement Manager Vacant Post

9.6 PCI University Champions

Catherine Barrett Ext 3551 barretc1@hope.ac.uk

Sue Jolley Ext 3244 jolleys2@hope.ac.uk

Michelle Loftus Ext 2162 loftusm@hope.ac.uk

Michelle Lynch Ext 3221 lynchm@hope.ac.uk

9.6 PDQ Machines

Ann Rimmer Ext 3280 rimmera@hope.ac.uk

10.

**GLOSSARY OF TERMS AND KEY**

**Glossary**

PCI DSS - Payment Card Industry Data Security Standards

PSP - Payment Service Provider

PAN – Permanent Account Number

SAQ - Self-Assessment Questionnaire

PDQ - Process Data Quickly (Tills, hand held terminals and car parking machines)

CVV - Card Verification Value (3 digit code on back of card)

CVC - Card Verification Code (3 digit code on back of card)

**Cards Not Accepted**

* American Express
* Diners
* JCB

**PSP**

* Worldpay/Fisglobal

**11.**

**Appendix**

In January 2005 Mastercard and visa combined their security standards to create a joint standard. It is endorsed by American Express, JCB and Diners

If a business stores, processes or transmits card data it needs to meet the 12 requirements set out in the programme. More information can be found at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

**Build and maintain a secure network and systems**

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor supplied defaults for system passwords and other security parameters

**Protect cardholder data**

1. Protect stored cardholder data
2. Encrypt transmission of cardholder data across open public networks

**Maintain a vulnerability management programme**

1. Protect all systems against malware and regularly update anti-virus software or programs
2. Develop and maintain secure systems and applications

**Implement strong access control measures**

1. Restrict access to cardholder by business need to know
2. Identify and authenticate access to system components
3. Restrict physical access to cardholder data

**Regularly monitor and test networks**

1. Track and monitor all access to network resources and cardholder data
2. Regularly test security systems and processes

**Maintain an information security policy**

1. Maintain a policy that addresses information security for all personnel