LIVERPOOL
HOPE
UNIVERSITY
1844

Liverpool Hope University

PCI DSS Policy

Date	Revision/Amendment Details & Reason	Author
26th March 2015	Updates	G. Donelan
23rd June 2015	Audit Committee	
7th July 2015	University Council	

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 and other irregularities including fraud policy' which can be found at:

https://www.hope.ac.uk/media/liverpoolhope/contentassets/documents/policiesandprocedures/media,23814,en.pdf

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 01444 250985

Barclays (PDQ's) – Telephone 01604 256939

Worldpay – PaymentSecurity@worldpay.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. The most common reason for a declined transaction is the card provider suspecting the transaction may be fraudulent.

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 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 server.

4. Card Processing Terminals – PDQ

4.1 Obtaining a PDQ Machine

4.1.1 To request a PDQ machine for your Unit, please contact the nominated person at Point 9 to discuss your requirements.

4.1.2 To set up your PDQ machine please follow the instructions that are provided by our Merchant bank and are included with your PDQ terminal.

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 should be used for the payment. The only exception to this is Student Finance who can take payments over the telephone but the card information is immediately deposited in the shredder container.

4.3 Customer Present With Card

4.3.1 When the customer is present the card 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.

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 or Online Store at that time and must not be written down or noted anywhere. The only exception to this is noted in point 4.2.1

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. by fax, 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.

4.5.3 If card details provided on a booking form or other form of letter, when the payment has been successfully authorised, the original document showing the full card details must be cross cut shredded.

4.5.4 In a situation where it is not possible to process the transaction immediately then the details must be stored in a secure environment such as a locked drawer or cabinet. This is only to be actioned in exceptional circumstances.

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. The customer copy must be sent to the customer.

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 sent 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 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 because of volume of transactions both Catering and the Sports Hall retain their receipts for a shorter period. Worldpay do not have a policy regarding the timescales of how long a refund can take place after the original sale date. However, they always would advise to issue a refund onto the same card that the sale was taken from. Confidential shredding should always be used when destroying merchant copies

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 and could result in hefty fines from Visa and MasterCard. The most common method of fraudsters obtaining card details is by hacking into computers which stores cardholder information.

5.2 Safe and secure storage is defined as:

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

All of these should be stored in a locked room, where a log of access to the stored receipts must be maintained.

5.3 Merchant copies of PDQ receipts must be retained by the University within each relevant Unit 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

6.1 **Online Refunds**

6.1.1 The refund must be approved by an authorised signatory for the cost centre and then passed to the Administrator 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 (6 months), 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.

6.2 **PDQ Refunds**

6.2.1 PDQ refunds are required 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.

7.5 The University may screen potential employees to minimize the risk of attacks from internal sources.

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.

8. Training

8.1 Staff Induction - New members of staff are requested to familiarise themselves with the Financial Regulations policy, Data Protection policy where reference is made to PCI DSS.

8.2 It is the duty of the Budget Manager 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/ Policies and Procedures section of the university website.

8.3 External training – Budget Managers, 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/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 Ann Rimmer Ext 3280 rimmera@hope.ac.uk

9.3 Cash office Finance Ext 3339 lynchm@hope.ac.uk

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

9.5 Procurement Manager Sheila Smith Ext 3157 smiths1@hope.ac.uk

10. Glossary of Terms and Key

Glossary

PCI DSS - Payment Card Industry Data Security Standards

PSP - Payment Service Provider

SAQ - Self-Assessment Questionnaire

PDQ - Process Data Quickly

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
- CB

PSP'S

- Worldpay

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**

Build and maintain a secure network

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

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open public networks

Maintain a vulnerability management programme

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement strong access control measures

7. Restrict access to cardholder by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly monitor and rest networks

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

Maintain an information security policy

12. Maintain a policy that addresses information security