Card Payment Procedures

Issued July 2017

Contents

1. Introduction

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 staff of the University who may have access to cardholder data must adhere.

As an organisation which processes cardholder data, the University is obliged to comply with the Payment Card Industry Data Security Standard (PCI-DSS).

2. What is PCI-DSS? (Payment Card Industry Data Security Standards)

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards introduced by VISA, Mastercard and other payment brands that applies across the card payment industry worldwide. It helps safeguard cardholder information, improve customer confidence and reduce the risk of fraudulent transactions. These rules are compulsory for all organisations handling any aspect of card transactions who have access to cardholder data.

There are 12 requirements to PCI-DSS, these include:

Control Objectives	Requirements
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 program	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 data 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 test 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 for all personnel

More information on PCI DSS can be located at https://www.pcisecuritystandards.org/.

Card Payment Data

Card payment data consists of 2 main sets of data that must be protected by the University at all times. These include:

<table>
<tr><th colspan="2">Card Payment Data</th></tr>
<tr><th>Cardholder Data</th><th>Sensitive Authentication Data (SAD)</th></tr>
<tr><td>Primary Account Number (PAN) i.e. the 16 digit number on the front of the card</td><td>Full Magnetic Stripe Data/Chip Data</td></tr>
<tr><td>Cardholder Name</td><td>CAV2/CVC2/CVV2/CID i.e. the last 3 digits on the signature strip on the back of the card</td></tr>
<tr><td>Expiration Date</td><td rowspan="2">Pin Numbers</td></tr>
<tr><td>Service Code</td></tr>
<tr><td colspan="2">PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If the PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply.</td></tr>
</table>

3. Purposes of Procedures

These procedures deal with the acceptable use and the controls required for receiving, processing and storing information in respect to all card data and covers all electronic and manual handling methods, including:

Card Present transactions	Card not present transactions
Face to Face (Chip and pin)	Internet
Face to Face Contactless	Telephone

These procedures cover the security of cardholder data and must be distributed to all University staff who process credit card transactions. The procedures shall be reviewed annually and updated as needed to reflect changes to business objectives, to the risk environment or to PCI-DSS.

4. Ethics and Acceptable Use Policies

These procedures are subject to the appropriate University regulations and policies. Of particular relevance are:-

- University Policy 12 – Business Ethics and Fraud (http://www.bath.ac.uk/finance/regulations/policies.html#up12)

- IT Security Policy (http://www.bath.ac.uk/bucs/aboutbucs/policies-guidelines/policies-it-security.html)

All users must read and abide by the main Information Security Policy. An employee's failure to comply with the policy set forth in this document may result in disciplinary action up to and including the termination of employment.

In order to ensure compliance, the key areas that need to be addressed and implemented by University staff who undertake card transactions are:

- Access to payment card transactions and data must be restricted to only those members of staff who need access as part of their role.

- Staff should be aware of the importance and confidentiality of card payment data and under no circumstances should credit card numbers be stored or transmitted electronically, this includes e-mailing, instant messaging, chat and scanning of paper copies.

- It is strictly prohibited to send, receive, process and store card details by Unapproved University Methods.

Card payment data **MUST NOT** be written down. This includes when taking payments over the phone. If for some reason the payment cannot be input immediately the caller's contact details should be taken and a call-back arranged.

5. University Approved Card Payment Methods and Services

Card data must only be received and processed by the University approved methods and services. These are:

Payment Method	Card Transaction	Mandatory Controls	Storage of Card Data
Customer NOT Present	**Online via University approved solution**	Payment via online system should generate an e-mail payment confirmation to the customer.	No Data is held by the approved University PCI-DSS compliant supplier
		If a customer's payment has been unsuccessful or declined, the customer should contact their card provider in the first instance.	
		If a customer faces difficult in making a payment then staff assistance can be provided.	
		If the payment problem cannot be resolved, the customer should be offered an alternative payment method.	
	Telephone	Where card details are provided during a telephone call, these must be processed directly into the PDQ terminal at that time. The card details must not be written down.	No Data is held by the approved University PCI-DSS compliant supplier
		When card details are being provided during a telephone call, these must not be repeated back to the customer in such a way that it can be intercepted by third parties.	
		If it is not possible to process the card details directly into the PDQ terminal immediately then a call back must be offered.	

Customer Present	**PDQ/EPOS** **Face-to-face transaction including contactless**	For contactless payments ensure the customer checks the value of the transaction before swiping their contactless card or device over the PDQ/EPOS terminal.	ONLY merchant receipts held in secure physical storage with PAN truncated and disposed of as confidential waste
		When the customer is present the card should be processed through the PDQ/EPOS terminal according to the on-screen instructions. Only the customer should handle their card unless you have to check a signature.	
		If the transaction is successfully processed, the merchant copy should be securely stored and the customer copy given to the customer.	
		If the transaction is declined, the customer should be advised immediately.	
		The customer copy stating that the payment was declined should be given to the customer and the merchant copy should be stored securely.	
		The option of paying with a different card should be offered.	

Approved PDQ terminals and Third Party Suppliers

The University provides card payment processing terminals (PDQ's) and online systems' which are approved and PCI-DSS compliant.

The terminals in use have been selected to ensure that appropriate controls are in place to minimise risk, for example, the number of PAN digits that appear on till receipts is limited to just the last four digits on both the customer and merchant copies. Only PDQ terminals provided by the University's approved supplier should be used. Any queries about obtaining, upgrading or returning a PDQ terminal should be directed to cashiers@bath.ac.uk. The till receipts should be retained for at least 6 months, to enable chargebacks. They should not in any case be held for longer than 2 years.

The online systems' ensure that the relevant card payment data is securely processed and stored via approved payment service providers. The University also has an approved Online Store for all other goods and services. WPM is the approved provider and the system is PCI-DSS compliant and should be used for all such payments.

The use of any other online system or payment service provider will require:

1. Due diligence checks to be performed to ensure the prospective provider is PCI-DSS compliant.
2. Business case detailing why WPM is not suitable.
3. Formal approval by the Director of Finance.

The authorisation of alternative providers will only be granted in exceptional circumstances and in the first instance the WPM option will be explored.

6. Unapproved Card Payment Methods

The following are unapproved methods of payment and should not be used:

- Post/Written
- E-mail
- Fax
- Voicemail/Recordings

Accepting cardholder data via the above methods exposes the University to non-compliance with the PCI-DSS. This may result in fines, reputational risk if there is a data breach and ultimately potential withdrawal of the facility to take payments by credit and debit cards.

Under no circumstances should the non-approved payment methods be used without a formal University review.

7. Storage of Card Payment Data

In the event that storage is required for operational, regulative and legislative requirements, ONLY the data below can be stored:

- Truncated Primary Account Number (PAN) – First 6 or last 4 digits only
- Cardholder Name
- Service Code
- Expiration Date

The approved methods are designed to securely store the relevant data for legislative requirements.

Below are only a few examples of further controls required and must be active at all times with the appropriate technology in place:

- Masking to ensure ONLY the first 6 or last 4 digits of the PAN can be seen (relevant to displaying on computer screens/receipts/voicemail)
- Truncation, hashing and encryption via transmission and storage databases
- Segregation away from other data sources on a designated secure server
- Technical hardening and further controls of all aspects of systems, network and services used to process, store and transmit card payment data
- Technical vulnerability and penetration testing of services on a regular basis

8. Third Party Approved Suppliers

Any third party appointed to manage cardholder data on behalf of the University must be an approved and trusted University supplier.

The third party must be audited on an annual basis and PCI-DSS certification must be evidenced.

The Finance Office will maintain a central list of service providers who store, process, or transmit cardholder data.

9. Security Management and Incident Response Plan

The areas which credit card data is processed or held is referred to as the Card Data Environment (CDE)

General Security Responsibilities

- All users within the CDE must familiarise themselves and follow the policies and procedures applicable to their area of responsibility
- All users within the CDE must only carry out their designated role,
- All users must not disclose their passwords or share accounts
- All users within the CDE must take appropriate steps to secure devices and data from unauthorised access and protect them from damage
- Only university supplied equipment should be used in connection to credit card processing, no personal devices should be used or connected to the systems
- Users must not install, copy or modify any software or devices in the CDE without authorisation.
- Computers, devices and technologies used for card processing should only be used for official university business
- All users must immediately report security incidents to their line-manager who will co-ordinate with relevant teams within the university

The line manager must ensure that at least one of these roles are informed to co-ordinate a response

- IT Security Manager
- Treasury Accountant

Who will inform the Director of Finance, Data Protection Officer, the university acquirer, relevant payment service providers, relevant third party hosting providers and the Information Commissioner's Office (where appropriate).

In the event of a breach or security incident the university will take prompt action and follow an approved incident plan, the plan includes steps in line with recommended best practice to:

1. Preserve evidence
2. Provide an initial investigation report and inform acquirer
3. Procure approved external forensic capability if needed
4. Assess all exposed accounts
5. Provide a final investigation report