**Payment Card Industry Data Security Standards (PCI DSS):**

**Information for Managers**

**Introduction**

This document is intended for managers and supervisors of teams which handle cardholder data, or who manage an online or other automated / electronic payment stream. The purpose of this document is to give those responsible an understanding of the security implications of handling card data to ensure their teams and processes are operating according to University policy and industry standards.

As an organisation which processes card payments, we have an obligation to our customers to protect them from data theft and card fraud. In doing so, we also protect the University from the results of a data breach, which among others is likely to involve bad publicity, loss of reputation and financial sanctions. This is achieved by adherence to the security standards, which minimises the risk of card data loss, either by physical theft of hard copy data or by theft of electronic data through cyber-crime.

**What is PCI DSS?**

PCI DSS is a set of security requirements developed by the five card brands: VISA, Mastercard, AMEX, JCB and Discover. Their aim was to put together a common set of security principles.

PCI DSS relates to the Primary Account Number (PAN) and the Sensitive Authentication Data (SAD). The PAN is the 16 digit number on the front of a card. If we store this in any format, it must be protected from unauthorised access. The SAD refers to the Card Verification Code (CVC), which is the 3-digit code on the back of the card used to confirm payment. It also refers to the data contained in the magnetic stripe and the Chip. The SAD must never be stored after the payment has been authorised and University policy is also to never store any magnetic stripe or Chip data.

All members of staff who have visibility of cardholder data need to be aware of PCI DSS, the processes they are required to follow and how they can reduce the risk of card data theft and fraud.

PCI DSS consists of 12 requirements, which are grouped into categories:

**Build and Maintain a Secure Network**

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

**Protect Cardholder Data**

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

**Maintain a Vulnerability Management Program**

Requirement 5: Use and regularly update anti-virus software or programs

Requirement 6: Develop and maintain secure systems and applications

**Implement Strong Access Control Measures**

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

**Regularly Monitor and Test Networks**

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

**Maintain an Information Security Policy**

Requirement 12: Maintain a policy that addresses information security for all personnel[[1]](#footnote-1)

Each requirement is broken down further into individual points for action.

These requirements are referred to throughout this document, as relevant to you. Items that individual managers are responsible for and need to take action on will be highlighted later.

**Why is PCI DSS important to the University?**

Compliance with PCI DSS is a requirement of our contract with our acquirer, Worldpay, as well as other software and service providers. We need to be compliant in order to take card payments. Being compliant minimises the risk of data theft and provides a secure payment environment for our customers.

The consequences of a security breach resulting in customer card data being accessed by an unauthorised party can be wide-ranging:

* Inconvenience and distress to our customers – card data theft and fraud can be very distressing, and take time to resolve.
* Financial sanctions – the University could be fined if we lose card data.
* Reclassification for compliance – the University could be assessed as a high risk, level 1 merchant. We would need to have external verification of our security, which would be expensive and time consuming for the University.
* Lose card processing facility – the University could have its ability to take card payments removed. This would cause a significant increase in workload and costs, and would lead to loss of business.
* Reputational damage – this could be the most damaging consequence of all, as data security breaches can get a lot of publicity that could deter students from choosing our University as well as our partners and other companies being willing to work with us.

Complying with PCI DSS requirements and University policy does not guarantee that a security breach will not occur, but it reduces the risk and our liability.

**What does PCI DSS apply to?**

**Processing, transmission and storage of the Primary Account Number (PAN)** – this is the long number on the front of the card. What does this mean to you?

* **Processing:** how the PAN is collected and what we do with it whilst still in our possession up to putting the transaction through. This is something you need to be aware of and will be covered below.
* **Transmission:** how we connect to the acquiring bank. This will be managed by the Finance Office or IT Services on set up.
* **Storage:** what we need to do if the PAN is stored. The PAN should not be stored after the payment has been processed. If the PAN is stored, or you feel this would be of benefit, please contact us to discuss this immediately.

There are a number of ways you might come into contact with the PAN:

* You may obtain this from customers over the phone or by post, when you take Cardholder Not Present transactions.
* When taking a face-to-face transaction, the PAN is printed on the customer’s card.

**CVC** – the authorisation number on the back of the card. This is used during cardholder not present transactions. This is Sensitive Authentication Data (SAD) and must never be stored after the payment has been authorised.

**Card terminals** – these should be stored securely, so that they cannot be tampered with. Your team members should be able to identify if changes are made to the terminal.

**How to apply PCI DSS in your outlet**

**Third-party processes**

Third party processes may be used to collect cardholder present transactions (e.g. via self-service machines), or cardholder not present transactions (e.g. online payments). As the payments are collected and processed by a third party, the University does not transmit, process or store cardholder data. This can be good news for our PCI DSS compliance. Our relationship with our service providers is addressed by PCI DSS requirement 12.8 and is managed by the Finance Office.

The following points must be addressed for the University to be compliant:

* The University is required to maintain a list of our service providers. This is maintained by the PCI DSS team.
* 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 DSS team
* There must be a written agreement between the University and each service provider that acknowledges that the service provider is responsible for the security of cardholder data the service provider possesses. This should be included in the contract or agreement between the University and the service provider. All financial agreements are authorised by the Finance Office and therefore this is managed by the PCI DSS team.
* There must be an established process for engaging service providers. This is managed by Procurement & Finance Accounting team
* All service providers must be PCI DSS compliant. This is monitored annually by the PCI DSS team.
* All service providers should be listed on the VISA Merchant Agents list or provide a certificate of proof of compliance for PCI-DSS (this is a condition of our contract with Worldpay) this is monitored by the PCI DSS team.

In order to fulfil these requirements, any department who wishes to engage a third party service provider to collect payments **must** inform the PCI DSS team in the planning stages, so that we can ensure the above requirements are met, and the nature of the service will not compromise our PCI DSS compliance. Procurement must be involved at an early stage to ensure the correct process is followed.

Any department planning changes to an existing service which is run by a third party must inform the PCI DSS team in the planning stage, so that we can ensure that the changes do not affect our compliance.

All third party payment services must be installed to the provider’s specifications, and must be used in accordance with their terms and conditions. If these are not followed it is possible the service will not be PCI DSS compliant.

**Processes within departments**

The following points are taken from the PCI DSS requirements and will be relevant to departments processing cardholder present (Chip and Pin) and cardholder not present (telephone) transactions. Further information and guidance are given for your information and action as required.

Due to the diverse nature of the business conducted at the University, this document cannot address every situation – its purpose is to provide a guidance document for managers, to enable them to ensure their processes and procedures are compliant. If you need more specific advice, or would like to confirm your understanding, please contact the PCI DSS team (details at the end of this document).

**Requirement 3 - Do not store sensitive authentication data after authorisation (even if encrypted).**

Sensitive authentication data (SAD) refers to the card verification code (CVC), the magnetic strip data, the PIN or the PIN block.

The CVC must only be obtained from the customer where there is a business need to do so (for example to process a Cardholder Not Present transaction and entered directly into the card terminal or virtual keypad.

**Requirement 4 - Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).**

Unprotected PANs (Primary Account Number) must never be sent by email, instant message or end-user other messaging technologies, either internally or externally. University policy goes further than this, to state that **PANs, even if protected, must never be sent by email or other end-user messaging technology**.

Customers must never be instructed to send their card details to the University by email or other end-user messaging technology, this message should be available to customers, for example on any website providing payment options or paper documents if sent. Where a customer sends their card details unsolicited the transaction must not be processed. The card details should be deleted as soon as possible and within the same day they are discovered. If you need to keep the email for your records, for example if it contains an order request, the email must be edited to remove the card details. In addition, the message should not be forwarded internally or externally. The customer must be contacted to explain that we cannot accept card details by email for security reasons and payment must be requested via an approved payment method.

Points for attention:

* Local procedures must state that PANs must never be sent by email or other end-user messaging technology.
* The procedures must state the process of what to do if a PAN is received by email or other end-user messaging technology.

**Requirement 9 - Secure all media containing cardholder data.**

All media (e.g. paper receipts) which contain cardholder data must be secured. Paper records of cardholder data must be locked in a designated area or container (e.g. locked filing cabinet).

No cardholder data should be stored electronically, whether this is contained within a spreadsheet or other electronic document.

Paper records of cardholder data must only be kept as long as is required for business or legal reasons. After the storage period has elapsed, the paper records must be destroyed by cross-shredding, or by disposal via the Confidential Waste Service. If the Confidential Waste Service is used, the documents must be handled according to the Confidential Waste Protocol, which specifies that unsealed bags must not be left in areas where unauthorised personnel might have access to them (e.g. cleaners). They must be sealed and stored in a secured room until they are collected.

Cardholder data should not be distributed outside of the originating department. Where there is a business need to do so, the data must be hand delivered or sent by a secure delivery method that can be tracked. If you are requested to send cardholder data outside the University, you must contact the PCI DSS team for advice before sending.

Points for attention:

* Cardholder data must be treated as Confidential under the Information Classification Standard.
* Local procedures must describe all the ways in which cardholder data is stored, how it is secured.
* Local procedures must describe procedures for transferring cardholder data between storage locations (if appropriate), stating this must only be done with the required authority.

**Requirement 12 - Security Awareness**

All departments are required to adhere to the PCI DSS procedures, which are reviewed annually. If a security breach is suspected, this must be reported to the PCI DSS team immediately.

All team members who have any visibility of card data must complete the PCI DSS Awareness module provided by the PCI DSS team. These activities should form part of the induction for new team members and must be renewed every year, as applicable.

Any change in payment processes, including new developments, must be approved by the PCI DSS team or Finance Accounting team***.*** To minimise the effect on any timeframe for changes please contact the PCI DSS team during the planning stages, before tender and discussions with suppliers, so that any impact on the University’s PCI DSS compliance can be assessed.

Points for attention:

* Managers must ensure that all team members who handle card data complete the relevant PCI DSS Awareness module as part of their induction, and annually thereafter.
* Managers planning new payment processes, or changes to existing ones, must contact the PCI DSS team at the planning stage.

**What are your additional responsibilities as a manager of staff who process card payments and handle card data?**

As a manager of a team which handles cardholder data, you are responsible for ensuring that your team operates in a compliant manner. This includes the following areas:

**Empower your team**

Team members should be encouraged to share ideas and good practice, and to bring any concerns regarding processes to your attention for review or for you to seek advice.

**Card payment terminals (or PDQ Devices)**

These must be kept secure from tampering as skimming devices can be added to them which copies card data, allowing the data to be stolen and a breach to occur. PDQ devices must be kept out of reach of the public when not in use, and stored securely out of hours. Team members need to be able to identify if a device has been tampered with. A suggestion to implement this is to have a reference photo, allowing the device to be checked against the photo at the beginning or end of each shift.

The Terminal ID should be checked regularly to ensure that the terminal has not been swapped. Criminals target the terminals to gather cardholder data or to commit fraud, by collecting the University’s income.

**Encourage online payments**

This may be via the Online Store; www.store.hope.ac.uk or other online pathways. Using online payments reduces the scope as University staff do not have access to cardholder data. For information on the Online payments please email [maguirj@hope.ac.uk](mailto:maguirj@hope.ac.uk) or rimmera@hope.ac.uk.

**Please note** that customers must never be directed to use a University computer to make payment, unless agreed by the PCI DSS team. These PCs are not set up or monitored in accordance with PCI DSS and therefore could be tampered with to copy cardholder data entered. If we direct customers to use these PCs we would be responsible for the cardholder data. Any advice given must only state that services are available online, which can be stated as the preferred choice, but leaving the customer to make their own choice on where and how they wish to use this service.

**What to do if you suspect a security breach, i.e. potential or actual unauthorised access to card data**

Contact the PCI DSS team immediately where:

* You believe an unauthorised person has gained access to and/or stolen cardholder data held by the University (e.g. if an inventory identifies missing cardholder data, if there has been a break-in to an area where cardholder data is stored or if you believe a terminal has been tampered with).
* If a terminal is suspected to have been tampered with, stop using that terminal and unplug it, but do not change anything.

**What to do in case of any queries**

Information relating to PCI DSS can be found at the URL below

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

**Contacts**:

PCI DSS team:

Mark Pringle Ext 3487 [pringlm@hope.ac.uk](mailto:pringlm@hope.ac.uk)

Ann Rimmer Ext 3280 [rimmera@hope.ac.uk](mailto:rimmera@hope.ac.uk)

Claudia McLean Ext 3237 [mcleanc@hope.ac.uk](mailto:mcleanc@hope.ac.uk)

Finance Accounting team: Email [finance@hope.ac.uk](mailto:finance@hope.ac.uk)

1. Navigating PCI DSS: Understanding the Intent of the Requirements, v2.0 [↑](#footnote-ref-1)