**PCI DSS Awareness Module**

**Data Security Standards (PCI DSS) Requirements**

**Cardholder Data Received by Telephone**

Introduction

PCI DSS regulations are there to protect both electronic and manual cardholder data where a Primary Account Number (PAN) is stored or processed. PCI DSS was introduced so that Card Issuers can ensure that the level of protection a merchant employs is sufficient to remove the risk of a security breach.

A Security Breach, for instance where cardholder data which has been written down for a future payment attempt is intercepted by unauthorised personnel before processing, would result in compromising the security of the card data. This could have widespread consequences for the University, not only significant financial liabilities but a loss of reputation and a loss of customers. Card schemes may also remove the ability for the University to accept card payments.

The Finance Office recommends providing an online payment method where possible as it is the most secure payment channel. Where online payment is not an option this document will provide guidance and best practice procedures that need to be adhered to in order to process cardholder data received by telephone within PCI DSS requirements.

Processing the Telephone Order (TO)

Telephone orders can only be accepted from the cardholder, we are unable to process a request for payment by a third party. It is therefore imperative when processing a TO that the caller is asked to confirm that they are the cardholder, and if possible where customer information is held verification questions should be asked. For example, confirm their address or date of birth. Online payments and Cardholder Present Transactions provide greater security as the customer is able to authenticate that they are the cardholder.

When cardholder data is provided by telephone it should be input directly into the manual terminal or online payment page (only online sites approved by the Finance Office can be used) immediately by a trained member of staff.

The number of staff trained to take payments by telephone must be restricted to the number needed to facilitate the business function. Access to cardholder data displayed must be restricted to staff who require the card details to fulfil their role. These restrictions are in place to ensure the security of cardholder data by monitoring and controlling the members of staff who have access to unencrypted cardholder data.

It is important that cardholder data is not stored anywhere on the University’s network, such as a spreadsheet or other electronic file or system. This restriction is due to the unsecure nature of storing cardholder data electronically, leaving the cardholder data vulnerable to malicious activity and would be a breach of current procedures and PCI DSS compliance requirements.

Call recording systems are prohibited where TO are processed. Cardholder data must never be repeated back to the customer if you are in a public environment as this may be audible to others in close proximity. If the cardholder data needs to be clarified, request the customer to repeat the numbers for the processor to then confirm. Part of the PAN such as the last four digits may be stated to avoid confusion and to confirm the cardholder details.

If cardholder data is not able to be processed immediately due to system or payment failure it must not be written down for a future payment attempt. If an online payment facility is not available a call back or an attempt with an alternative card must always be offered to the customer. Where an online payment facility is available, this should be suggested to the customer for their convenience.

After the TO has been processed

If the payment has been processed through a PDQ machine a merchant copy receipt and a customer copy receipt will be produced. There are no specific storage requirements for either of these receipts as they contain only the first six and last four digits of the PAN. If a payment is processed through an Online Payment Page there will be no storage considerations.

Restricting access to areas where cardholder data is processed

It must be ensured all visitors are authorised and logged before entering areas where cardholder data is processed or stored. PCI DSS regulations stipulate:

*A visitor log is easy and inexpensive to maintain and will assist during a potential breach investigation in identifying physical access to a building or room and potential access to cardholder data. Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months*. [[1]](#footnote-1)

There must be a barrier between public areas and areas where cardholder data is processed to prevent unidentified visitors entering without authorisation. PCI DSS suggests the following precautions are implemented:

*All visitors must be given a physical token that expires (e.g. a name badge) that identifies them as not staff members*[[2]](#footnote-2)before entering areas where cardholder data is processed. *They must then surrender the physical token before leaving the facility or upon expiry.[[3]](#footnote-3)* These measures ensure staff are able to ‘*easily distinguish between onsite personnel and visitors in areas where cardholder data is accessible.’[[4]](#footnote-4)*

Glossary of Terms

PCI DSS Payment Card Industry Data Security Standards

PDQ Process Data Quickly

CVC Card Verification Code (3 digits on the back of the card)

PAN Primary Account Number

SAD Sensitive Authentication Data

Cardholder Data Consists of the SAD and the PAN/Cardholder name/Chip data/ Expiration date

Cardholder Present Transaction A transaction where the cardholder is present within the Merchant’s environment and is able to identify themselves by Chip and Pin.



1. *Navigating PCI DSS: Understanding the intent of the requirements* , Requirement 9.4, 2010,p.44 [↑](#footnote-ref-1)
2. *Navigating PCI DSS: Understanding the intent of the requirements* , Requirement 9.3.2, 2010,p.44 [↑](#footnote-ref-2)
3. *Navigating PCI DSS: Understanding the intent of the requirements* , Requirement 9.3.3, 2010,p.44 [↑](#footnote-ref-3)
4. *Navigating PCI DSS: Understanding the intent of the requirements* , Requirement 9.2, 2010,p.44 [↑](#footnote-ref-4)