**PCI DSS Awareness Module – face to face transactions only**

You are required to complete this course if you process face-to-face card payments as part of your job. If you carry out any other tasks involving cardholder data, e.g. taking payment over the telephone or archiving of cardholder data, you must complete the full PCI DSS Awareness Module which covers a wider range of activities. Please ask your manager if you are unsure if this is the right module for you.

When we process or store cardholder data, we have a responsibility to protect our customers from theft and fraud by ensuring that we use and store their data in a secure way. This course will introduce you to the PCI DSS requirements, explain why they are so important, and give some examples of how they might be applied to your working practices.

**What is PCI DSS?**

PCI DSS stands for “Payment Card Industry Data Security Standards”. PCI DSS is a set of 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. The purpose of PCI DSS is to ensure that businesses are reducing the risk of card data theft and fraud and therefore providing a secure environment for their customers to make payment.

Any team member who comes into contact with cardholder data needs to be aware of PCI DSS, and how they as an individual can reduce the risk of cardholder data theft and fraud.

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

If we process, transmit or store cardholder data, we have a responsibility to secure it and protect our customers from fraud. Because it is considered so important, compliance with PCI DSS is a requirement of our contract with our acquirer, WorldPay, as well as other software and service providers. Being compliant shows, we have worked to reduce the risk of data theft and to provide 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 upsetting, and take time to resolve
* Financial sanctions – the University could be fined if card data is lost.
* We could be assessed as a high-risk merchant. We would need to have external verification of our security, which would be expensive and time consuming for the University.
* The University could have its ability to take card payments removed. This would cause increased workload, and could lead to loss of business.
* Reputational damage – data security breaches can get a lot of publicity, and the trust our customers have in us could be severely damaged.

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

**What does PCI DSS relate to?**

**Primary Account Number (PAN)** – this is the long number on the front of the card. If we do not handle or store the PAN, then PCI DSS does not apply. It should therefore only be handled or stored where there is a business need to do so. The only way you will come into contact with the PAN is on the customer’s card – if you do have access to a customer’s PAN in any other way, you should complete the full PCI DSS Awareness Module.

**CVC** – the authorisation number on the back of the card. This is Sensitive Authentication Data (SAD) and must never be stored after the payment has been authorised. You will never have any reason to ask for or record this number, as it is not required for face-to-face transactions.

**Card terminals** – these should be stored securely so they cannot be tampered with.

As a team member who takes card payments, you have a responsibility to carry out your work according to procedures and University policy regarding PCI DSS. By doing this you are protecting your customer’s data from theft, protecting the University from the consequences of a data security breach, and protecting yourself in the event of a breach.

If you are concerned that a process may not be secure, and may put cardholder data at risk, you have an obligation to report this to your manager or the PCI DSS Team.

**How does PCI DSS relate to what I do?**

The following examples highlight some of the ways you should take PCI DSS into account when dealing with card data. The list does not cover all situations, and some of the scenarios might not be relevant or appropriate to you. If you are unsure how to apply PCI DSS to your processes, please seek advice from your manager.

Remember, the best defence against cardholder data theft is not to store it – if we do not have it, it cannot be stolen from us.

**Payments made in person**

Team members should not need to handle the customer’s card. Once you have entered the amount, the customer should put their card in the terminal for chip and pin transactions, or pass their card over the terminal for contactless transactions. If you do not handle the card, you do not come into contact with the card holder data.

One way in which criminals can obtain card data is by tampering with the card terminals so that the cardholder data can be collected as the payment is being processed. This is called skimming. It is therefore important to ensure that terminals are not tampered with. Portable terminals must be kept out of reach of customers and the public, and stored securely out of hours. You should be able to recognise if a terminal has been tampered with - you may have a reference photo of your terminal, so you can compare the terminal to the photo and identify any changes. If you think your terminal may have been tampered with, stop using it and alert your manager immediately.

If your terminal prints the full Primary Account Number (PAN) on the merchant copy of the receipt, you must bring this to your manager’s attention or contact the PCI DSS team immediately.

C:\Documents and Settings\townseev\Local Settings\Temporary Internet Files\Content.IE5\2L5FPJUZ\MC900237996[1].wmf

Merchant copies of till receipts that display the full PAN must be securely stored at all times in a designated, locked place with restricted access. They must not be left out on a counter. This must only be a temporary situation until the terminal has been updated to NOT show the full PAN

**What should I do if I suspect someone has gained unauthorised access to card data?**

If you believe that an unauthorised person has gained access to cardholder data that the University holds (e.g. if there has been a break in to an area where cardholder data is stored, or you believe a terminal has been tampered with) you must inform your line manager and the PCI DSS Team at once. If a card terminal may have been tampered with, stop using that terminal and unplug it, but do not change anything; then contact PCI DSS Team immediately.

If you have any questions about PCI DSS, please speak to your manager for guidance. Any further queries should be referred to the PCI DSS Team.

**PCI DSS Contacts**

**The PCI DSS team, contact details can be found in the PCI DSS Policy**