

**PCI DSS Training**

**THE FOLLOWING TRAINING MODULE SHOULD BE COMPLETED BY ALL SU STAFF THAT:**

* Process Payments
* Have direct contact with payment card transactions
* Oversee, manage, reconcile, or work with payment card transactions

**WHEN DOES IT NEED TO BE TAKEN?**

* For employees currently handling cardholder information, at least annually.
* For new employees or current employees taking over cardholder duties, upon hire and annually thereafter.



**WHY DO YOU NEED TO KNOW ABOUT PCI COMPLIANCE?**

1. We all use our debit or credit cards on a regular basis, such as paying for coffee or buying something on-line. It is such an everyday occurrence that many of us give very little thought to handing over our credit or debit card to complete strangers or entering our card data into a website. We do this in good faith, expecting that our information will be protected. Yet, each year millions of people are affected by credit card theft.
2. Each day students, staff, customers, and visitors use their cards to make payments to us, with the expectation that we will keep their information safe and secure. So, we have all have a responsibility to make ourselves aware of and abide by policy and the designated card handling procedures.
3. It is very important that all credit card information be safeguarded. All business units, departments, schools, and sections that collect credit card payments must ensure all staff members adhere to these standards.



**SO, WHAT ARE THE ‘PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS’ (PCI DSS)?**

The PCI DSS standards were developed and agreed upon by VISA, MasterCard, American Express, Discover, and JCB.

The main purpose of PCI DSS is to protect cardholder data by requiring mandatory data security standards for any merchant that processes, stores, or transmits cardholder data.

By properly following the twelve elements of the PCI DSS, the University and the SU can reduce the risks of payment card fraud, hacking, and other sources that result in compromised data. The standards apply to all forms of payment card acceptance: mail, phone, fax, point-of-sale, and online.

**The 12 ELEMENTS OF PCI DSS REQUIREMENTS are**:



**SO, WHAT DOES THIS MEAN FOR THE SU?**

It is our responsibility to prevent and detect fraud, we have an obligation to others to keep their card information safe when processing credit card payments.

**We must:**

* Identify and evaluate all credit card acceptance activities.
* Develop policies/procedures for payment card acceptance-please refer to **IT usage** **data** policy.
* Ensure that credit/debit card activities comply with established procedures.

**WHAT DOES THIS MEAN FOR STAFF?**

We rely on all staff to protect student and customer account information, including credit card account number, expiration dates, security codes, pins, and any other personal information. When handling such sensitive information, handle it like it was cash or your own card data.

Strictly follow and adhere to the department’s payment processing procedures.

All persons involved in taking card payments must complete an Annual PCI training review.

**Make yourself aware of potential risks and take action to stop them:**

* Only allow authorised staff to access work areas, tills and card reading devices.
* Never leave computers, tills or card reading devices unattended.
* Secure card reading devices when not in use e.g., locked away in a cabinet overnight.
* Do not write down card data or leave card details on view to others.
* Safely and securely dispose of any card holder data that is no longer required (using a cross-cut shredder), it must not be stored on paper or electronically. Your card reading device has been configured to only show the last 4 digits of the 16-digit card number on receipts, this is okay to retain. No other card data (expiry date or CVC) may be retained.
* Do not store any card data on paper or electronically once the payment has been processed.
* Regularly inspect card reading devices to guard against substitution or tampering.
* Never accept credit card numbers in an email, text, voicemail, or instant message. DO NOT process the transaction. Send an email back to the individual without the credit card information included and state that the University will not process any credit card number received through email.; make surer to delete the original email and seek the assistance of the IT Manager to have the email removed from servers.
* If you are taking credit/debit card information over the phone, process the payment whilst the customer is on the line. Any documents that contain card information must be shredded immediately upon processing the payment.
* When it is deemed necessary, check the signature on the card and verify it against the signed receipt. If card is not signed, ask cardholder to present a valid photo ID and compare signatures and name, including the one on the sales receipt. Remember: Visa cards begin with a 4, MasterCard starts with a 5, Discover starts with a 6, and AMEX starts with a “34” or “37”. Do not accept a credit card with a number that does not correspond to the credit card type.
* Where possible, segregate duties so that persons taking payments or issuing refunds do not reconcile takings.
* Inspect card reading devices daily, to check for signs of substitution or tampering. Check makes, model and serial number against the daily check sheet to ensure that they match. If the device exhibits signs of tampering (e.g., scratches around screw holes, missing labels, damaged seals, misaligned key, difficulty reading mag strip or entering pin codes etc.) or starts to operate differently, stop using it immediately and report it to management.



**CONSEQUENCES OF NONCOMPLIANCE CAN INCLUDE:**

Failure to comply with card security requirements can result in significant and detrimental outcomes:

* Even a small data breach could easily cost the SU hundreds of thousands (£) in direct costs alone.
* Loss of funds by card holder(s), which the SU will be expected to reimburse.
* Setting up notifications to card holders, hotlines, credit monitoring etc.
* Loss of income from the fraudulent purchase made.
* There will also be many indirect costs such as conducting a forensic investigation, updating and/or replacing compromised equipment, litigation by card holders for lost funds and inconvenience.
* A data breach will be investigated by the Information Commissioner (a Government agency), with the risk of criminal prosecution and financial penalties arising.
* Negative publicity eroding the trust the SU has with its stakeholders.
* The termination of our ability to accept card payments.

**WHAT ACTION MUST YOU TAKE IF YOU NOTICE SOMETHING?**

As soon as you notice something is amiss, you must notify your Line Manager immediately. They in turn will notify the SU IT and Finance Team, who will work with them to investigate the matter.

* Lost or stolen:

o Password,

o ID,

o Keys,

o Laptop,

o Portable storage device, or

o Credit Card Terminal.

* Filing cabinets, credit card terminals or locks that have been tampered with or have changed without notification.
* Computers holding virtual terminals are infected with virus or malicious software.
* Unannounced visits by engineers to inspect or replace card reading devices.
* Anything you feel is suspicious.
* If you recognise procedures/ regulations not being followed contact your Line manager.

**REMEMBER: YOU ARE THE FIRST LINE OF DEFENCE AGAINST FRAUD**