Payment Card Industry Data Security Standards (PCI DSS)
Information for Managers

What is PCI DSS?

PCI DSS are 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 providing a secure environment for their customers to make payment by reducing risk of card data theft and fraud

PCI DSS is all about the Primary Account Number (PAN). This 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. A lot of the requirements of PCI DSS are specific to IT Services. However, all members of staff need to be aware of PCI DSS, and how they as an individual can reduce the risk of card data theft and fraud.

The 12 requirements of PCI DSS:

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]

Why is PCI DSS important to the University?

Compliance with PCI DSS is a requirement of our contract with our acquirer, Global Payments, as well as other software and service providers. We need to be compliant in order to take card payments. Being compliant shows we have worked to reduce the risk of data theft and 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 distressing, and take time to resolve
- Financial: lost income – the University may lose money due to fraudulent transactions
- Financial: sanctions – the University could be fined if card data is lost.
- We 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.
- The University could have its ability to take card payments removed. This would cause increased workload, and could lead to loss of business

[1] *Navigating PCI DSS: Understanding the Intent of the Requirements, v2.0*

- Reputational damage – this could be the most damaging consequence of all, as data security breaches tend to get a lot of publicity.

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

If you would like to know more about PCI DSS, you can visit the PCI Security Standards website: www.pcisecuritystandards.org/

What does PCI DSS apply to?

Primary Account Number (PAN) – this is the long number on the front of the card. If you need to retain this, it should be securely stored in a designated lockable place at all times. There are a number of ways you might come into contact with the PAN:

- You may obtain this from customers over the phone, fax 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.
- Old merchant copies of receipts will have the PAN printed on them. After the switchover to Global Payments, the terminals will not print this data therefore the merchant copies do not come under PCI DSS. However it is good practice to store them securely.

CVC – the authorisation number on the back of the card. This is Sensitive Authentication Data (SAD) and must never be stored with the PAN.

PDQ terminals – these should be stored securely, so that they cannot be tampered with. You should be able to identify if changes are made to the terminal. We suggest having a reference photo of the terminal, which can be compared to the terminal to confirm that no unauthorised changes have been made, i.e. the addition of skimming equipment.

What are the main considerations?

- The best defence against cardholder data theft is not to store it – if we do not keep it, it cannot be stolen from us. Where possible, you should limit the amount of cardholder data you store. If you do not store the PAN, PCI DSS does not apply.
- If you have a business need to store card data:
    - Ensure the appropriate people are aware of what you are storing and why
    - Do not store card data electronically. If you currently have card data stored electronically, please contact Paul Simpson (details below).
    - Physical storage of card data – Card data should be securely stored in a locked location, with access to the key recorded. Card data should be stored for 6 years plus current financial year. When the card data no longer needs to be stored, it should be securely destroyed e.g. by cross shredding
- Paper forms requesting card details must be approved by Finance, and must be handled and processed in accordance with PCI DSS requirements.
- If details are received by email, they must not be processed or forwarded on – the email should be deleted and the customer contacted to request details via a secure method
- Online payments should be encouraged e.g. online shop, as University and individual staff members do not have access to card holder data at any time, therefore they are not in scope for PCI DSS
- If a student asks where they can pay online, you can direct them to the designated payment PCs in the Student Fees Enquiry and Income Counter. These PCs are specifically set up to be secure PCs for taking payments. Other computers on campus are not set up to be secure for payments, so customers must not be directed to them to make payment.

What are your responsibilities as a manager of staff who take card payments?

- To ensure that all staff who take card payments receive the appropriate training yearly
- To ensure that PCI DSS forms part of the induction process for new staff
- To ensure that cardholder data is not stored electronically
- To ensure that your procedures are up to date and are PCI DSS compliant
    - Postal forms – where these are accepted, ensure the data is protected throughout the process, from when the details are requested from the customer to the processing of the payment and the disposal or storage of the paperwork. Note, customers should be advised that these must not be returned by email
    - Telephone transactions – if a terminal is not available and it is not possible to call the customer back, to determine if your staff are permitted to write card details down, and if so, to ensure that correct procedures are followed
- To inform Paul Simpson of any change in systems relating to payments in the planning stage, before tender or speaking with companies
    - All 3rd parties must be PCI DSS or PA DSS compliant. This must be included in contracts.
- To investigate staff concerns regarding the security of your processes, referring these to the Finance Office or IT Services where appropriate

What to do if you suspect a security breach, i.e. potential or actual 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 should inform your line manager and Paul Simpson (details below), at once. If a terminal may have been affected, stop using that terminal and unplug it, but do not change anything.

PCI DSS Contacts

Finance Office: Paul Simpson, p.m.simpson@bham.ac.uk, 0121 414 7188

IT Services: David Deighton, d.deighton@bham.ac.uk, 0121 414 4748