PCI Card Handling Guidance Policy
SAQ C-VT
Contents

1  PCI DSS & Me  2
  1.1  What is PCI DSS?  2
  1.2  How does PCI DSS impact me?  2

2  What is Card Data?  3
  2.1  Cardholder Data & More  3
  2.2  Storing Card Data  4
    2.2.1  PDQ Machines  4
    2.2.2  Computers  5

3  Handling of Card Data within the University  5
  3.1  General Card Handling Practices  5
  3.2  Tampering  6
  3.3  Protection  6
    3.3.1  Firewalls  6
    3.3.2  Anti-virus  6
    3.3.3  Default Settings  7
    3.3.4  Configuration  7
    3.3.5  Encryption  8
    3.3.6  Transmission  8
    3.3.7  Risk Assessment  8
    3.3.8  Access Control  9
  3.4  Accepting Card Data  9
    3.4.1  Face to Face Payment  9
    3.4.2  MOTO – Mail Order Telephone Order  10
    3.4.3  Online  11
  3.5  Destruction  11
  3.6  Unsolicited Card Data  12

4  Documentation  13

5  Testing  14

6  Refunds  14

7  Compliance & Monitoring  15

8  Security Breach  15

9  Contacts  16
1 PCI DSS & Me

Think about the last time you made a credit or debit card purchase. Was it online? Was it in a shop? Was it at the garage? When you made that last purchase did you think about the security of your card data?
When you made your payment you trusted that your card data would be safe, protected by the retailer or merchant and the card companies.

The University of St Andrews takes hundreds of credit and debit card payments every day and has to protect the customer card data from loss or theft just like any other merchant big or small has too.

This document is intended as an introduction to the necessary practices for handling, processing, transmitting and managing of credit and debit card data.

1.1 What is PCI DSS?

PCI DSS is the Payment Card Industry Data Security Standard, a standard developed for protecting the customer’s credit and debit card information every time it is taken from the customer to make a purchase from the merchant.

The University is described as a “Merchant” by the PCI DSS and is contractually obliged to strictly follow the PCI DSS Standard whenever and/or wherever credit or debit card data is accepted, processed and/or stored by the University. Strict penalties are levied for not following the Standard and in the worst cases it can lead to the theft or loss of the customer’s credit or debit card data.

1.2 How does PCI DSS impact me?

If your role within the University requires that you are either directly or indirectly in contact with the customer’s credit or debit card data, it is essential that you follow the University’s policy, these guidelines and the PCI DSS Standard itself where it applies directly to your role or activities.

Your role is vital to the safekeeping of the customer’s credit or debit card data and contributes to the University’s overall PCI DSS operations.
2 What is Card Data?

Regardless of whether it is a credit card or a debit card, the data that the card holds is exactly the same. Card data is supplied by the customer to the merchant to make a payment. Card data is effectively the key to the customer’s account to withdraw the payment. The following is an introduction to card data.

2.1 Cardholder Data & More

The data that is held on the customer’s credit or debit card is either Cardholder Data (CHD) or Sensitive Authentication Data (SAD). The data can be either visually marked on the card or encoded in the chip or magnetic stripe. This is an overview of a typical credit card and the location of each type of cardholder data.

<table>
<thead>
<tr>
<th>Cardholder Data</th>
<th>Sensitive Authentication Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Account Number (PAN)</td>
<td>Full Track Data (from magnetic strip or chip)</td>
</tr>
<tr>
<td>Cardholder Name</td>
<td>CAV2/CVC2/CVV2/CID</td>
</tr>
<tr>
<td>Expiry Date</td>
<td>PIN data</td>
</tr>
<tr>
<td>Service Code</td>
<td></td>
</tr>
</tbody>
</table>

![Diagram of a typical credit card showing the location of each type of cardholder data.](image)
2.2 Storing Card Data

While all data on the card has to be protected, PCI DSS has slightly different rules about handling the two types.

- **Sensitive Authentication Data (SAD)** – Cannot be stored, transcribed or copied at any point.
- **Card Holder Data (CHD)** – Card Holder Data is not permitted to be stored under the University Policy.

*As a general rule, if you don’t need the data, don’t accept it, don’t store it and it cannot be lost or stolen.*

2.2.1 PDQ Machines

- Settings should be checked to ensure that the full PAN is not displayed on terminal or on receipts. Only the first six or last four digits of the PAN are permitted to be displayed.

- If a transaction is successful, the merchant copy should be stored securely and the customer copy given to the customer. These receipts must be treated as confidential documents and should be marked accordingly.

- Merchant copies of PDQ receipts must be kept for a rolling year of 12 months, for audit purposes. Merchant copies that have been held for 13 months or more can therefore be destroyed by confidential shredding. The receipts should be filed chronologically and in a secure environment. A secure environment is defined as:
  - Within a safe
  - Within a cash box
  - Within a locked drawer
  - All of these should be stored in a locked room, where a log of access to the stored receipts must be maintained.

- Merchant copies should be stored within the till drawer or cash box for the duration of the working day and the customer copy must be given to the customer.

- If the transaction is declined the customer should be advised immediately. The option of paying with a different card should be offered. The customer copy stating that the payment was declined should be sent to the customer and the merchant copy should be stored within the till drawer or cash box for the duration of the working day.

- The PDQ machine transaction slips must be reconciled to the PDQ Z report at the end of business each day. The merchant copies should be retained securely within the School/Unit and the excel spreadsheet should be emailed to accrec@st-andrews.ac.uk to allow the income to be processed to your cost centre.

- When not in use, devices should be protected from physical access by those not authorised to use the equipment. This can be in a locked room or drawer. Only named staff/roles should have access to the device.
2.2.2 Computers

- Storage of card details on PCs in any format (email, access databases, excel spreadsheets, data sticks etc.) breaches the Security Standard Regulations which effectively makes the University non-compliant and could result in large fines from Visa and MasterCard. The most common method that fraudsters use to obtain card details is by hacking into computers that store card information.

3 Handling of card data within the University

This section covers procedures for all methods by which staff may come into contact with card data.

3.1 General card handling practices

For all staff involved in accepting, managing and/or processing card data.

- To request a first PDQ machine for your Unit, please contact the nominated person in section 7 to discuss your requirements. If a PDQ machine is later replaced, staff should notify Finance immediately to ensure that the University’s master list is kept up-to-date.

- Staff must not request transmission of any payment card information from customers via email, text, social networking or other end-user messaging technologies.

- Staff must not send cardholder data via email, or other end-user messaging technologies (such as SMS, social networking, skype) whether or not the messaging system is encrypted.

- Payment card information, including full PAN numbers, must not be displayed or made visible to anyone except authorised staff. For example, payment equipment such as tills must not show the full PAN. (The first six and last four digits are the maximum number of digits that may be displayed.)

- Staff must not store any payment card information in an electronic/digital format, whether or not encrypted, on any computers or storage devices whether by scanning, keying, photographing or any other means. Note: This applies to all types of payment card data including PAN, PIN, three-digit security codes and full track data. This requirement limits the University’s scope so controls the cost, difficulty and feasibility of implementing and maintaining the PCI DSS controls that apply to storing card data necessary for compliance.

- Customers (including students) must not be specifically directed to the University’s IT equipment to provide online payment solutions. If a customer wishes to use the University’s IT infrastructure to make an online payment, then it is their choice and not mandated by the University.

- Staff roles should be reviewed regularly to ensure that only staff who require access to system components and/or cardholder data are able to access it. Access should be limited to the minimum required to enable that staff member to carry out their duties effectively. Individual Unit policies should state clearly those members of staff...
who require access and the level of this access, either by referring to staff members by name or by their job classification.

3.2 Tampering

All payment devices that are used by the University for accepting card payments should be inspected daily to ensure that the device has not been tampered with, substituted and/or compromised in any way. Devices should be checked on any occasion that they have been left unattended. This could be at the start of the day, at a change of shift, at a change of staff member or after an evacuation, such as for a fire alarm. A record should be kept including details of inspections carried out.

The type of inspection will vary based on the type of payment device being used. For further guidance on how to spot signs of tampering and how to prevent it taking place, please see the University's Physical Inspection Checklist.

3.3 Protection

The Cardholder Data Environment (CDE) should be protected from both internal and external attacks to ensure that the data is secure.

3.3.1 Firewalls

- Firewall and router configurations should restrict connections between untrusted networks and any system in the cardholder data environment.
- Both inbound and outbound traffic should be restricted to that which is necessary for the environment. All other traffic should be specifically denied access to the environment.
- Any outbound traffic from the environment to the internet should be explicitly authorised.
- Only established connections should be permitted into the network.
- Personal firewall software should be installed and active on any portable computing devices (both University and staff owned) that connect to the internet when outside the network (such as laptops) and that are also used to access the CDE. This software should be configured to specific settings and not alterable by users of these devices.

3.3.2 Anti-virus

- Anti-virus software should be deployed on all systems commonly affected by malicious software.
- Anti-virus software must be capable of detecting, removing and protecting against all known types of malicious software, such as viruses, Trojans, worms, spyware, adware and rootkits.
- Periodic evaluations should be performed to identify and evaluate evolving malware threats in order to confirm whether those systems considered to not be commonly affected by malicious software continue as such.
- All anti-virus software and definitions should be kept up-to-date.
• Automatic updates and periodic scans should be enable and performed.

• All anti-virus mechanisms should generate audit logs and those logs should be retained for at least 1 year with at least the most recent 3 months available for analysis.

• All anti-virus mechanisms should be actively running and unable to be disables or altered by users.

3.3.3 Default Settings

• Vendor-supplied defaults must always be changed before a system is installed on the network. This applies to ALL default passwords.

• Any unnecessary default accounts should be removed or disabled before a system is installed on the network.

• For wireless environments connected to the cardholder data environment or transmitting cardholder data, all wireless vendor defaults should be changed as follows:

  o Encryption keys should be changed from default at installation and changed any time anyone with knowledge of the keys leaves the University or changes position.

  o Default SNMP community strings on wireless devices should be changed on installation.

  o Default passwords/passphrases on access points should be changed at installation.

  o Firmware on wireless devices should be regularly updated to support strong encryption for authentication and transmission over wireless networks.

  o Other security-related wireless vendor defaults should be changed on installation.

3.3.4 Configuration

• Standards should include enabling only necessary services, protocols, daemons, etc., as required for the function of the system.

• Where virtualisation technologies are used, only one primary function should be implemented per virtual system component or device.
3.3.5 Encryption

- All non-console access should be encrypted with strong cryptography and a strong encryption method in place before the administrator's password is requested.

- System services and parameter files should be configured to prevent the use of insecure remote login commands such as Telnet.

- Administrator access to web-based management interfaces should be encrypted with strong cryptography.

3.3.6 Transmission

- Cardholder data sent across open, public networks must be protected through the use of strong cryptography or security protocols (e.g., IPSEC, TLS). Only trusted keys and/or certificates can be accepted. Security protocols must be implemented to use only secure configurations, and to not support insecure versions or configurations. The proper encryption strength must be implemented for the encryption methodology in use (check vendor recommendation/best practices). For TLS implementations HTTPS must appear as part of the URL, and cardholder data may only be entered when HTTPS appears in the URL.

- Wireless/WiFi networks must not be used for transmitting cardholder data or connected to the cardholder data environment.

- Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user messaging technologies include email, instant messaging and chat.

3.3.7 Risk Assessment

Processes must be in place to identify potential security vulnerabilities that include:

- Using reputable outside sources for vulnerability assessments.

- Assigning a risk ranking to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a high risk to the environment. In addition to the risk ranking, vulnerabilities may be considered critical if they pose an imminent threat to the environment, impact critical systems and/or would result in a potential compromise if not addressed.

These processes must be reviewed regularly to ensure that they take into account changes in business activity and technology.

Once vulnerabilities are known, relevant staff must ensure that all affected system components are protected by installing vendor-supplied security patches. Any critical security patches must be installed within 1 month of their release.
3.3.8 Access Control

System Access:

- All users should be assigned a unique ID before being allowed to access system components or cardholder data. In addition, one or more of the following methods must be employed to authenticate all users:
  - Something you know, such as a password or passphrase
  - Something you have, such as a token device or smart card
  - Something you are, such as biometric

- User password parameters should be configured to require passwords/passphrases meet the following requirements:
  - A minimum password length of at least seven characters.
  - Contain both numeric and alphabetic characters.
  - Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.

- All non-console administrative access and all remote access to the CDE should be secured using multi-factor authentication.

- Multi-factor authentication should be incorporated for all non-console access into the CDE for staff with administrative access.

- Generic user IDs and accounts should not be used for system administration activities or any other critical functions.

- Access for any terminated users must be either deactivated or removed immediately.

Physical Access to CDE and media:

- All media containing cardholder data (including computers, removable electronic media, paper receipts, paper reports) should be physically secured.

- If any kind of media is to be moved, strict controls must be in place to ensure that the media is classified so that the sensitivity of the data can be determined. Media should be sent by secured courier or by another delivery method that can be easily tracked. Management approval must also be obtained prior to moving the media.

3.4 Accepting card data

This section outlines the various ways that card payments can be made across the University.

3.4.1 Face to Face Payment

Face to Face payments may be defined as:

*Any transaction where a customer presents their card to make a payment in person. The payment point is attended by a member of staff responsible for processing payments. Also known as a customer present transaction.*

General guidance for Face to Face payment processing and protection of devices:
• Face to Face payment should be done by staff authorised to do so as part of their duties.

• Physical payment devices must be protected from physical access out-of-hours by those not authorised to use the equipment or authorised to be in the area. (Small devices such as PDQs must be locked away and larger devices such as tills must be in rooms with restricted access when not in use.)

• Physical payment devices must be subjected to visual inspection each day or before use. Equipment, cabling and connections should be inspected for signs of tampering. The working area in the vicinity of the equipment should be checked for any suspicious devices.

• When a payment is being made, the customer should enter their card in the payment device. Staff should not handle the customer’s card unless they have the specific permission of the customer to do so. In which case at no point should the customer’s card be out of sight of the customer.

• If staff become aware of individuals near the payment devices with active video recording devices, such as phone cameras or wearable cameras such as Google Glass, Body cameras (common with security officers) and or Go-Pro’s. The staff member should request the owner to turn off the camera for the duration they are in the vicinity of the payment area.

At all times if the staff member suspects the device or card data has been compromised, it must be reported immediately to pcidss@st-andrews.ac.uk.

3.4.2 MOTO – Mail Order Telephone Order

A Moto Payment maybe defined as:

“A customer not present payment, where the customer has entrusted the staff member with their card data to take on behalf of the customer only the payment for which the card data has been provided for”

When taking payment by the telephone:

• Staff must not use VOIP (Voice over Internet Protocol).

• Staff should ensure the telephone system being used does not have voice mail or voice recording which may be used to record customer card data.

• Staff should enter supplied card data directly into the payment device while on the call and at no point record it electronically.

• Staff should not read the card number back to the customer to validate the number. If in doubt the customer should be asked to read the card number again.

If card data is being received by post

• Process the card data immediately after opening the envelope, destroy the letter/form or document immediately after using a cross shredder.
• If it is not possible to immediately process the card data on receipt, securely store the data in a lockable data storage facility. Clearly record the number of items being stored, who has supplied the data and when - this record should be used to cross check the items being stored. This should only be required in exceptional circumstances.

At all times if the staff member suspects the device or card data has been compromised, it must be reported immediately to pcidss@st-andrews.ac.uk

3.4.3 Online

An online payment may be defined as:

“A payment made directly by the customer using an internet provided payment method”.

Online payments are made directly by the customer using internet payment services provided by the University, such as the Online Payment Services. Staff members at no point will be involved in accepting payments via this method.

• On completion of a successful payment the online system being used will automatically generate an email payment confirmation to the customer. This is the only Finance confirmation document that will be received by the customer for the payment.

• If a customer’s payment has been unsuccessful or declined, the customer in the first instance should contact their card provider. The most common reason for a declined transaction is the card provider suspecting that the transaction may be fraudulent.

• If a customer faces difficulty in making a payment then staff assistance can be provided. The customer should be assisted at the time of the enquiry, whether this is in person or via the telephone. If the problem cannot be resolved, then the customer should provide a number to be called back on at a suitable time.

• Staff must not direct customers at any point to IT equipment owned, supplied or managed by the University to make an online payment.

• Any problems the customer experiences with the online payment systems should be reported immediately to onlinepayments@st-andrews.ac.uk.

If a staff member has reason to believe an online payment system has been compromised, it should be reported to pcidss@st-andrews.ac.uk immediately.

3.5 Destruction

As and when card data needs to be destroyed, it must destroyed in such a way that it cannot be reconstituted and the original data restored.

For physical paper copies of data:

• All paper based card data must be cross shredded, pulped or incinerated.
• Paper based card data must not be stored for recycling without first being cross shredded.

• If paper based card data needs to be stored prior to destruction, it must be securely stored in a lockable storage cabinet or container. A record of the items being stored must be kept and used to confirm prior to destruction that the items are present.

• If there is reason to suspect that paper based card data has been lost, stolen or compromised, this should be reported immediately to your line manager who can then refer to pcidss@st-andrews.ac.uk if necessary.

Digital Destruction

In the advent that data is discovered in a digital format, it must be destroyed and deleted in such a way that it cannot be restored using forensic or data recovery tools.

Digital data may occur on computers, backup tapes, hard drives, memory sticks, optical media (DVD/CD’s).

• On discovery of a digital copy of card data, this should be reported to the PCI team ASAP to arrange secure destruction. Do not email, or copy the file. Note the filename, location and any dates associated with the file.

• Do not presume this file is a one off – establish the source of the data file and confirm if the file has been automatically or manually created.

• Do not delete the file using the standard deletion functionality. The following options are available:
  o Overwriting - Using appropriate compliant multi-pass software or hardware to overwrite digital media with zero’s or generic patterns, which render the data irrecoverable.
  o Degaussing – Using appropriate compliant degaussing (or demagnetizing equipment) to erase Magnetic Media.
  o Physical Destruction – Using appropriate compliant methods for physically destroying media.
    ▪ Optical media may be shredded or be passed through a grinder;
    ▪ Magnetic media may be melted or pulverized after being degaussed or overwritten.
    ▪ Solid State Drives (including memory sticks) in their nature of storage can result in data remaining. As such solid drives may be melted or pulverized after an attempt at degaussing or overwriting.

• Validate all back up media has not retained traces of the digital files containing card data.

3.6 Unsolicited card data

There will be exceptional times that card data may be provided by the customer either deliberately or accidentally. These are considered to be unsolicited card data incidents, the following describes the actions to take to try and reduce these occurrences.
Email

- If you deal with payments, invoicing customers / students, please include a footer which says “do not send credit card details via email”
- On receipt of unsolicited email with card data, do not reply or forward the email – delete the email and delete it from the deleted folder. If the email requires a response, the card information provided should not be contained within the reply.
- Email the customer using a fresh email and inform them that the University doesn’t accept card data via email.

Voice mail:

- Where possible deactivate voice mail in teams that take payments. If voicemail is required, then as part of the voice mail message state that the customer must not leave card data as a voice mail message. If card data is discovered on a voice mail message – contact the PCI team to arrange secure destruction.

For lost credit and debit cards:

- If a customer’s credit/debit card has been left behind or discovered, secure the card until the earliest opportunity that the card can be destroyed.
- If the customer returns to collect the card before destruction – validate the customer’s identity before returning the card.

4 Documentation

- An Information Security Policy must be established, published and distributed to all relevant staff. The policy must be reviewed at least annually and any time there is a change in the environment. The updated policy should then be distributed to relevant staff. The policy should clearly define information security responsibilities for all staff.
- An incident response plan must be in place to be implemented in the event of a system breach.
- Usage policies must be in place for critical technologies. This can include remote access and wireless technologies, laptops, tablets, removable electronic media, email usage and internet usage. Policies should contain the following:
  - Explicit approval by authorised parties to use the technologies.
  - A list of all such devices and staff that have access.
  - Acceptable uses of the technologies.
- Where external service providers are used, policies and procedures should be maintained and implemented to manage those providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:
  - A list of service providers must be maintained, including a description of service(s) provided.
  - A written agreement should be implemented and maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service provider possesses or otherwise stores.
processes or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s CDE.

- A process should be in place for engaging service providers, including proper due diligence being carried out prior to engagement.
- A review of service provider’s PCI DSS compliance status should be carried out at least annually.
- A record should be kept about which PCI DSS requirements are managed by each service provider and which requirements are managed by the University.

5 Testing

Scanning and Penetration Testing

- Where segmentation is used to isolate the CDE from other networks, penetration testing procedures should be defined to test all segmentation methods, to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE.

- Penetration testing should be performed at least annually and after any changes to segmentation controls/methods. The testing should cover all segmentation controls/methods in use and verify that each is operational and effective.

- Penetration testing must be performed by a qualified internal resource or a qualified external third party. This person does not need to be an ASV.

6 Refunds

- Online Refunds

  - The refund must be approved by an authorised signatory for the cost centre and then emailed to the Cash Office in Finance. The appropriate system is accessed and the refund processed back to the source card from which the original transaction was authorised.

  - If a transaction is older than 18 months, a refund cannot be processed on to the source card for the original transaction. This is due to security measures implemented by the Payment Service Provider (PSP).

- PDQ Refunds

  - PDQ refunds require to be authorised on the PDQ machine using a “Supervisor Card”. This card must be kept securely by an authorised signatory.
The refund should then be processed through the PDQ machine back onto the source card from which the original transaction was authorised.

If the source card is unavailable for the refund to be processed then the customer should be contacted for alternative details for the refund to be processed by BACS. A refund must never be processed onto a card that is not the source transaction card.

7 Compliance & Monitoring

- All card processing activities of the University must comply with PCI DSS. No activity or technology may obstruct compliance with PCI DSS.

- All Schools/Units must adhere to this policy to minimise the risk to both customers and the University. Failure to comply will render the University liable for fines and may also result in Visa and/or MasterCard preventing transactions from being processed by the University.

- A third party company is under contract to monitor University compliance with PCI DSS through annual Self-Assessment Questionnaire (SAQ) reviews.

- Through meetings with Supervisors and relevant staff the Finance Operations Manager will conduct a regular review that identifies threats and vulnerabilities and results in a formal risk assessment.

- The University may screen potential employees to minimise the risk of attacks from internal sources.

- The University will contractually require all third parties with access to cardholder data to adhere to PCI DSS requirements. These contracts will clearly define information security responsibilities for contractors.

- If you have difficulties implementing or complying with any aspect of this policy, you should contact the appropriate member of University staff in section 7 below.

8 Security Breach

In the event that a member of staff suspects that there may have been a security breach, they should report this immediately to an appropriate member of Finance Staff using the contact details in section 9. The Finance member of staff must ensure that card processing is discontinued immediately and contact the appropriate external party in section 7.
9  Contacts

Internal

- Eric Gillespie – Finance (all general enquiries) ext. 2455 erg@st-andrews.ac.uk
- Joanna Gardner – Finance, Online Payment Services ext. 2476 onlinepayments@st-andrews.ac.uk
- Cash Office – Finance ext. 2587 cashoffice@st-andrews.ac.uk
- Financial Accounts – Finance ext. 2519 accrec@st-andrews.ac.uk
- PCI Team pcidss@st-andrews.ac.uk

External

- WPM – 0844 264 1581
- Barclays Helpline (PDQs) – 0844 811 6666
- Realex – 00353 1702 2000