UNIVERSITY OF ABERDEEN

PAYMENT CARD SECURITY POLICY

1. Background

1.1. The University of Aberdeen accepts debit and credit card payments online, over the telephone (customer not present), and in person (face-to-face). Telephone and in person payments are processed on physical payment devices. In Campus Services these devices are integrated into their EPOS (electronic point of sales) system, in all other locations the devices are standalone (independent of systems). Virtual terminals where staff manually key payment card details into a website when processing the payment are not currently used by the University of Aberdeen.

1.2. The Payment Card Industry Data Security Standard (PCI-DSS) is a mandatory standard that all organisations accepting card payments must adhere to. The purpose of the standard is to reduce the risk of theft and fraud of sensitive cardholder data by providing a secure environment for customers to make payment. In the event of a data breach, failure to comply with the standard will result in higher fines and increased transaction charges and may result in removal of permission to accept card payments, and further investigation by other regulatory bodies such as OSCR and the ICO.

1.3. The University of Aberdeen must demonstrate its compliance with the standard by completing an annual self-assessment questionnaire (SAQ), or more frequently if there is any change to the payment card environment, for example introducing new methods of card payment or changing devices.

1.4. This policy assists the University of Aberdeen in complying with the legal requirements of the Payment Card Industry Data Security Standard. It will assist in reducing the risk and impact of a data breach, including subsequent fines and charges, and it ensures adequate safeguards are in place to protect sensitive cardholder data. Failure to comply with this policy may result in disciplinary action.

2. Responsibilities

2.1. The requirements of PCI-DSS compliance involves significant input and co-operation between both the Directorates of Finance and Digital and Information Services.

2.2. The Director of Digital and Information Services is responsible for ensuring the University of Aberdeen has a qualified Internal Security Assessor (ISA) and providing a secure internal network environment that adheres to all payment card security standards.

2.3. The Director of Finance is responsible for ensuring the University of Aberdeen is compliant with PCI-DSS.

2.4. Schools and Directorates with card payment devices (physical or virtual) are responsible for adhering to all policies relating to payment card acceptance including nominating a point of contact for queries or issues, advising Finance of all movements in devices, ensuring all staff with access to cardholder data or devices undertake the mandatory annual payment security training.

3. Accepting Card Payments

3.1. New or changes to existing card payment methods (virtual or physical) **must** be requested through and approved by the Treasury Team, Directorate of Finance.

3.2. Finance will maintain a register of all card payment methods and devices.

3.3. The need for payment card devices should be reduced by processing sales through the online store or by issuing a sales invoice. However, it is recognised in some instances there may be a genuine business requirement to accept card payments. In these instances, the School/Directorate must submit a written request by email to the Treasury Manager, Finance justifying the business requirement. If approved, Finance will work with the requesting area to obtain a suitable payment solution.

3.4. All Schools/Directorates accepting payment by card (in any format) must adhere to all policies and procedures detailed in this and other supporting documentation, failure to do so may result in the removal of the payment device and the area being unable to accept card payments.

3.5. Payment methods that are implemented without obtaining the appropriate permissions and/or do not meet the required standards will be removed from service.

4. Online Payments

4.1. All online payment acceptance methods **must** be requested through and approved by the Treasury Team, Directorate of Finance.

4.2. All third-party partners and payment service providers involved in the provision of online payment card services must evidence their PCI-DSS compliance when requested by University of Aberdeen Finance representatives or the ISA. Compliance must be requested and evidenced prior to the commencement of services, and on an annual basis for the duration of the services.

4.3. Finance is responsible for ensuring supporting compliance documentation is obtained from online partners and payment service providers on an annual basis.

4.4. Cardholder data accessed through online platforms must be obscured. This is to reduce the risk of theft of cardholder data and minimise the impact of the accompanying breach.

4.5. Only University staff with a genuine business need will be provided with a unique login to access online card payment data. Users must not share their log in details.

4.6. Third party online payment card platforms must only be accessed from secure University devices. Payment card sites must not be accessed through personal devices or publicly shared University devices.

5. Payment Card Devices

5.1. All payment card devices (virtual or physical) **must** be requested through and approved by the Treasury Team, Directorate of Finance.

5.2. Finance will maintain a register of all such devices including location, unique device identification numbers, model type and key contacts.

5.3. All third-party partners and payment service providers involved in the provision of payment card services using these devices, must evidence their PCI DSS compliance when requested by University of Aberdeen Finance representatives or the ISA. Compliance must be requested and evidenced prior to the commencement of services, and on an annual basis for the duration of the services.

5.4. Finance is responsible for ensuring supporting compliance documentation is obtained from all partners and payment service providers on an annual basis.

5.5. All payment card devices must have end to end encryption. End to end encryption means the payment data is transmitted to the payment service provider in an encrypted (unreadable) format. The payment service provider holds the decryption code to decipher the transmission and process the payment.

5.6. To reduce the risk of a data breach, payment card devices capable of storing or transmitting unencrypted data must not be used or connected to any system or network including WIFI.

5.7. Payment card devices must not be added to the University's network without prior consultation and authorisation from the Treasury Manager, Finance and Digital and Information Services. This includes devices using WIFI, blue tooth, GPRS, or any other transmission method.

5.8. Schools/Directorates will be notified in advance by Finance if device software or hardware updates are required, and from Digital and Information Services if updates are required for network connections points. Without advance notification from the appropriate Directorate, no individual is permitted to update or change a device or its network connection.

6. Payment Card Device Security

6.1. Physical card devices (PIN Entry Devices or PEDS or card terminals) must be located in a secure environment.

6.2. If the device is left unattended it must be appropriately secured or removed to a secured location e.g. in a locked office, safe or locked cupboard.

6.3. Any movement in location of a device must be notified to Finance in advance of the change. Finance will update the register of card payment devices.

6.4. Schools/Directorates may be requested by Finance to apply security updates to their devices, these updates must be applied immediately.

6.5. All devices must be inspected regularly, and as a minimum before the commencement of service. The purpose of inspecting devices is to identify signs of tampering at the earliest opportunity and so reduce the impact of fraud. Tampering may be in a physical form such as skimming devices or swapping of terminals, or a change in performance which may indicate the presence of malware.

6.6. Schools/Directorates are responsible for undertaking regular device inspections in accordance with the Card Payment Device Inspection Procedure.

6.7. An audit log of all device inspections must be maintained, and the audit log submitted to Finance on a monthly basis, or on request.

6.8. Finance will periodically undertake unannounced checks of audit logs.

6.9. If a School/Directorate fails to inspect their payment devices and/or submit the audit log, their payment device may be removed from service.

6.10. All discrepancies must be investigated, and the device disconnected and removed from service until the situation is resolved. All incidents must be reported to Finance as detailed in the Card Payment Device Inspection Procedure.

6.11. Devices must be returned to Finance when no longer required or at the end of contract.

6.12. Finance will dispose of payment devices in a secure and appropriately manner i.e. as directed by the service provider.

7. Payment Device Supervisor Cards

7.1. Due to the additional access granted by a payment device supervisor card, access to the card and PINs must be strictly limited to those with a genuine business need and appropriate responsibility.

7.2. Supervisor cards must be always be kept secure and must not be stored with the payment device.

8. Cardholder Not Present Payment Acceptance

8.1. Customer requests to pay by card over the telephone should be discouraged. Customers should be requested to make payment online or by an alternative means as detailed on the University's web pages.

8.2. Schools/Directorates must obtain written permission from Finance prior to accepting over the telephone cardholder not present payments (or refunds). All other telephone payments or refund requests must be referred to the Income & Credit Control Team, Finance for processing.

8.3. Finance (or other approved area) will process the telephone payment and destroy any noted cardholder details by cross shredding immediately. This is applicable if the payment is successful or declined.

8.4. Cardholder details must not be requested or accepted from customers in any other format e.g. by email, text, social media, paper form. This includes requesting details to allow refunds to be processed.

8.5. If cardholder details are received, the details must not be forwarded (including replies to emails, etc), all sources of the data must be deleted immediately, and the customer contacted and advised not to submit payment card details in this format.

8.6. With the exception of merchant copies of receipts retained by Finance, full cardholder data must not be stored or retained in any format including electronically or on paper.

8.7. The following sensitive authentication cardholder data must never be stored in any format:

- The contents of the payment card magnetic stripe (track data)
- The CVV/CVC/CID – the 3 or 4 digit number on the signature panel on the reverse of the payment card
- The PIN or the encrypted PIN Block.

9. Payment Card Receipts

9.1. The default setting for the University (merchant) copy of the payment card receipt contains sensitive cardholder data i.e. the full card number or PAN (primary authentication number).

9.2. Finance will ensure PANs are obscured unless the requesting School/Directorate demonstrates a genuine business need to retain the information for future refunds.

9.3. All receipts, regardless of whether the PAN is displayed in full or not, must be treated as sensitive data and be stored in a secure location. Only individuals with a genuine business need should be granted access to the receipts.

9.4. Where the PAN has been obscured, receipts must be disposed of through confidential waste either in a restricted access confidential waste bin or dedicated pick up. All confidential waste is cross shredded.

9.5. Receipts on which the PAN is obscured must be disposed of no later than one month after the date of sale.

9.6. Receipts that display the full PAN must be sent securely to the Income & Credit Control Team, Finance. Finance will retain these receipts for no longer than 1 year, or less, if there is no business requirement to retain them.

9.7. Receipts on which the full PAN is displayed must be disposed of securely in a sealed confidential waste bag. The confidential waste bag must be stored securely in a restricted location until collection.

9.8. Cardholder data must not be used for any other purpose than that intended i.e. payment acceptance and related refunds.

10. Refund Processing

10.1. For Anti Money Laundering purposes payment card refunds must, wherever possible, be processed to the original payment card.

10.2. Online Store refunds will be processed through the Online Store. In instances where a School or Directorate has a regular requirement to process refunds, access to this functionality will be granted, all other online store refunds will be processed by Finance.

10.3. Refunds of online payments of sales invoices will be processed by Finance using the payment service provider's portal.

10.4. Over the counter purchases e.g. catering or retail sales, processed on a physical payment device (pin entry device) may be refunded by the School/Directorate to the original payment card.

10.5. Refunds of invoices where payment has been processed on a physical payment device (pin entry device) should be referred to Finance unless prior permission has been granted for the School/Directorate to process this type of transaction. To ensure the customer account is accurate and the audit trail complete, refunds of customer sales invoices must be processed and matched to a credit note in the Finance System.

10.6. In instances where the refund cannot be processed to the original payment card because the card has expired or the allowable refund period has passed (online payments only), the customer must be contacted, and new refund details obtained.

10.7. The refund must be paid to the original payee. Finance will apply appropriate checks to verify the identity of the original payee and ensure the refund is returned to them.

11. Staff Training

11.1. All staff are responsible for adhering to the University of Aberdeen's policies regarding payment acceptance and security.

11.2. Staff with access to the cardholder data must undertake mandatory annual Payment Acceptance training. This includes:

- All staff who accept card payments, even if infrequently
- All staff located in the area where a payment card device is located
- All staff who support payment processing in any format e.g. process or store merchant copies of receipts on which full card numbers are displayed, IT staff

11.3. Finance is responsible for providing access to appropriate Payment Card Security Training.

11.4. Training will include, but is not limited to, understanding the importance of payment card data security, device security, and the incident response plan.

11.5. The School/Directorate is responsible for identifying and ensuring all relevant staff undertake the Payment Card Security Training.

11.6. If a School/Directorate fails to ensure all relevant staff undertake the annual training, the payment device may be removed, and the area will not be permitted to accept card payments.

11.7. Staff who are unable to undertake the mandatory training due to long term absence e.g. maternity leave or sick leave, must undertake the training on their return to work and prior to accepting payment by card or accessing areas with cardholder data.

12. Incident Response

12.1. The Directorate of Finance will maintain the Incident Response plan.

12.2. In the event that an incident is identified e.g. a payment device is suspected of being tampered with, the School/Directorate must remove the device from service immediately and unplug it from networks and/or systems.

12.3. The nominated individual identified on the Payment Card Device Inspection Procedure should be contacted immediately.

12.4. The nominated individual will investigate the matter, if satisfied the device has not been tampered with it can be returned to service.

12.5. If there is any concern over the security or integrity of the device, it must not be returned to service.

12.6. All incidents must be logged and reported to Finance who will undertake further investigations if required.

12.7. If the nominated individual and their delegated substitute are both absent the device must be removed from service and the incident reported to Finance immediately.

12.8. Finance is responsible for reporting data breaches to the appropriate third parties.

12.9. The Incident Response Plan will be tested annually.

13. Information Security

13.1. It is University of Aberdeen policy to maintain a level of payment security that meets or exceeds the requirements of the PCI DSS standard.

13.2. Payment security activities and controls will be subject to both internal and external audits as required for PCI DSS compliance.

13.3. Firewalls are required to control the transmission of data between the cardholder data environment, trusted internal networks and untrusted external networks.

13.4. Network devices and systems will have default passwords changed, security configuration assessed, and unnecessary default services and accounts removed prior to deployment.

13.5. Cardholder data storage will be kept to a minimum and be securely encrypted when in transit across a network and at rest.

13.6. Where possible, all systems used within the cardholder data environment will be protected against malware with anti-virus software that updates automatically and cannot be removed or disabled by users. The effectiveness of the malware controls should be reviewed on at least an annual basis.

13.7. Internal and external vulnerability scans and remediation activities will be performed in line with the University of Aberdeen vulnerability management procedure.

13.8. If required, a quarterly external vulnerability scan will be performed by an Approved Scanning Vendor (ASV) certified by the Payment Card Industry Security Standards Council (PCI SSC).

13.9. Internal and external penetration tests will be carried out at least once a year.

13.10. Cardholder data will only be accessible to personnel who have a legitimate business reason because of a job or activity they are authorised to undertake.

13.11. Individuals who handle or have access to cardholder data will be identifiable and authenticated in compliance with the University of Aberdeen Authentication Policy.

13.12. Information security related logs will be kept for at least 1 year with a minimum of three months immediately available.

13.13. Cardholder data will be retained for the minimum time possible in line with business need and be destroyed immediately after usage, or when retention period has expired.

13.14. A cyber incident response procedure that is suitable for responding to potential incidents that may impact the confidentiality, integrity or availability of cardholder data will be maintained and tested at least annually.

14. Review

This policy is reviewed on at least an annual basis to ensure it:

- Remains fit for purpose.
- Reflects changes in technologies and requirements.
- Is aligned to industry best practice.
- Supports continued regulatory, contractual, and legal compliance.

15. Supporting Policies, Procedures and Documentation

- Authentication Policy
- Cyber Incident Response Plan
- Incident Response Plan
- Card Payment Device Inspection Procedure
- Card Payment Device Inspection Log
- Payment Card Training

Document Control

Version	Date	Action
1.0	Dec 2021	Approved – Information Governance Committee Approved – Senior Management Team

Title	Payment Card Security Policy
Author / Creator	Shiona Denton
Owner	Finance
Date published/approved	December 2021
Version	1.0
Reviewed	
Date of next review	December 2022
Audience	All staff involved in the processing of credit/debit card payments and staff who support the processing of credit/debit card payments.