Face to Face and MOTO Card Payment Security Policy

Document Owner: Matt Roach (ITCS)

Date: 13/02/20

Version: 5.1

This document defines the University's security policy on the receipt of payments via payment cards via face to face and MOTO (mail order/telephone order) payment channels, and is based on the following principles:

- **Only approved payment channels may be used for receipt of card payments**
- **Receipt of payments must be compliant with the requirements of the PCI DSS**
- **Specifically, all use must satisfy the SAQ P2PE-HW (for network connections) or SAQ B (for mobile connections)**
- **Many general information security policies also apply as well as more stringent requirements for this particular use of data and equipment**

IMPORTANT: If you are planning on accepting payments by payment card, you must first speak with Finance to ensure that you only set up systems and processes compliant with this policy.

Version history

Version	Date	Note
0.1	17/6/15	First draft
0.2	7/7/15	Updated after review by ISD/FIN
0.3	20/8/15	Approved at IT Security project board meeting
1.0	4/9/15	Approved by ISSC Chair
1.1	24/09/15	Updated to align with E-commerce security policy
2.0	20/10/15	Approved by ISSC
2.1	19/2/16	Updated to include requirements for SAQ B and to change the focus from the device used to the payment channels
3.0	26/2/16	Approved by ISSC Chair
3.1	12/5/16	Updated to include requirements as defined by PCI DSS v3.2
4.0	14/6/16	Approved by ISSC
4.1	30/3/17	Reviewed
5.0	13/6/17	Approved by ISSC
5.1	13/02/20	Reviewed – replaced ISD with ITCS

Introduction

Payments taken from payment cards are subject to the Payment Card Industry's Data Security Standard (PCI DSS). Where the payment is taken via the use of a PIN entry device (PED), the PED used must satisfy a subset of the requirements in the PCI DSS. These requirements concern the acquisition and maintenance of the devices as well as their operation in the handling of payment card data.

Requirements are placed on the operators of the PEDs as well as those overseeing their use and with responsibility for their installation and maintenance.

To satisfy the PCI DSS, all requirements must be met and documentation showing how they have been met must be generated in the course of their operation and management. Failure to meet the requirements of the PCI DSS may lead to the University being prevented from taking card payments, or fined, or both.

This policy applies to card payments taken for Face to Face (card-present) and MOTO (mail order/telephone order) (card-not-present) transactions via hardware payment terminals (PIN entry devices). Alternatively, the University may take payments via an e-commerce payment channel using a third party website. The use of websites must satisfy the University's E-commerce security policy.

Scope

This policy applies to:

- All Face to Face and MOTO payment card transactions
- All those parties with responsibility for taking payments by payment card for Face to Face and MOTO transactions. This includes and is not limited to IT staff, FIN staff, and staff in departments operating PEDs and their managers/supervisors
- The acquisition, installation, configuration, operation, maintenance, management and decommissioning of PEDs used for taking card payments
- All PEDs attached to the UEA data network, as well as those operated outside the UEA data network making a data connection via a mobile network SIM
- Companies totally owned by the University of East Anglia and its subsidiaries

SAQ B is defined by the Payment Card Industry to apply to:

- Merchants who process cardholder data only via imprint machines or standalone, dial-out terminals, and who do not store cardholder data on any computer system.
- Merchants handling both Face to Face (card-present) and MOTO (card-not-present) payment channels.

SAQ P2PE-HW is defined by the Payment Card Industry to apply to:

- Merchants who process cardholder data only via hardware payment terminals included in a validated and PCI-listed Point-to-Point Encryption (P2PE) solution.
- Merchants who do not have access to cardholder data on any computer system and enter account data via hardware payment terminals from a PCI SSC-approved P2PE solution.
- Merchants handling both Face to Face (card-present) and MOTO (card-not-present) payment channels. For example, cardholder data may be received on paper or over an analogue phone line, then keyed into a validated P2PE hardware device to process the payment.

Definitions

The following definitions apply to this policy:

- **Card verification code or value**. The three-digit or four-digit card verification code or value printed on the front of the payment card or the signature panel (CVV2, CVC2, CID, CAV2 data).
- **CHD**. Cardholder data. This includes the primary account number (PAN), cardholder name, expiration date, and service code.
- **DSS**. Data Security Standard.

- **Imprint machine**. A device for taking a copy of payment card details from the card by use of carbon paper.
- **P2PE-HW**. Point to point encryption hardware. This type of PED creates a secure communication channel direct from the device to the acquiring bank system through the host (University) data network in order to protect the information conveyed including the customer's PAN.
- **PAN**. Primary Account Number. The customer's card number.
- **Payment card**. The PCI DSS defines payment card to be any payment card bearing the logo of one of the founding members of the PCI SSC (Security Standards Council), namely, American Express, Discover, JCB, MasterCard or Visa.
- **Payment card processing entities**. All those bodies involved in the processing of a payment made by payment card. This includes the merchant (UEA in this case), processors, acquirers, issuers, and service providers.
- **PCI**. Payment Card Industry.
- **PED**. PIN entry device.
- **PIN**. Personal identification number.
- **PTS**. PIN transaction security.
- **SAQ**. Self-Assessment Questionnaire.
- **Sensitive authentication data**. This includes the full track data (magnetic stripe data or equivalent on a chip), card verification code or value, and PINs/PIN blocks.
- **Service provider**. Any third party organisation which processes CHD on behalf of the University, e.g. a document retention company that stores paper documents that include CHD. PCI DSS Requirements also apply to the service provider to ensure continued protection of the data. Processing includes transmitting, retrieving, storing, and destroying.

Aims

The aims of this policy are to ensure that the University:

- Only uses approved and compliant methods for accepting card payments via face to face and MOTO payment channels.
- Meets the requirements of the PCI DSS as they apply to the use of PIN entry devices (PEDs) processing payments by card as defined by SAQs B and P2PE-HW.

Policy statements - general

The University will only use payment channels which are PCI compliant. For e-commerce transactions, it will aim to achieve PCI compliance under SAQ A-EP, and for Face to Face and MOTO transactions – SAQ B and SAQ P2PE-HW.

- All payment channels for the receipt of CHD via face to face or MOTO transactions must first be approved. Approval is provided by Finance. Finance will maintain a list of approved payment channels.
- Only approved and certified PCI DSS compliance PIN entry devices are to be connected to the University data network and must comply with P2PE standards. SIM based PEDs must comply with PTS certification.
- All devices must be registered with the Finance and authorised by FIN before they are connected to the network. ITCS will provide advice on the technical compliance of devices (it.servicedesk@uea.ac.uk).
- The only systems that store, process, or transmit account data are the Point of Interaction (POI) devices approved for use with the validated and PCI-listed P2PE and PTS SIM (mobile phone) solutions.

- No other receipt or transmission of cardholder data via electronic means is permitted.
- The University will retain only paper reports and receipts with CHD for a maximum of one day, and these documents must not be received electronically.
- Where use of any network-connected device for processing card payments for Face to Face and MOTO transactions does not meet the requirements of SAQ B or SAQ P2PE-HW, explicit authorisation to accept the risks of non-compliance (including the University receiving unlimited fines and the removal of its ability to accept payments by card) must be obtained from the Director of Finance and Planning. Otherwise, the devices must not be used.
- CHD must not be received via any postal service. The University is not able to process mail orders.
- Telephone orders may only be received over analogue phone lines. VOIP phones (connected to the data network) must not be used for receipt of CHD.
- Face to Face and MOTO transactions must not be processed by operators using a web terminal running an e-commerce solution. All transactions must be processed through use of an approved and compliant PED.
- Imprint machines must not be used. All transactions must be processed through use of an approved and compliant PED.
- All service providers used to process CHD on behalf of the University (i.e. take card payments) must be certified PCI compliant.
- Any devices which are found to have been installed or operated in contravention to this policy will be disconnected from the network, and will be subject to an investigation.

Commented [RS(1]: As discussed at security project board 8/9/17. RW says this does not apply to UEA purchase cards. This is a known risk. (It is unclear where this is recorded.)

Policy statements – PCI DSS requirements

Where a policy statement relates directly to a requirement of the PCI DSS, the relevant requirement reference is provided.

Protect stored cardholder data [Req 3]

CHD must be held securely, kept no longer than needed, and only secure disposal methods are to be used for its destruction.

- CHD must not be stored electronically.
- If CHD is stored as physical (paper) records, the following policy statements relating to Requirement 3 then apply.
- The amount of CHD stored and the duration of its storage must be limited to only that required to satisfy all legal, regulatory and business requirements for data retention. UEA policy is to hold CHD on paper for no longer than one day. [Req 3.1]
- CHD must be securely deleted when no longer needed for legal, regulatory or business reasons. [Req 3.1]
- Retention period for CHD must be recorded in the appropriate departmental Records Retention Schedule (RRS) in accordance with the University's Records Management policy detailing the retention period and supporting reasons for retention. [Req 3.1]
- There must be a quarterly process in place to identify and securely delete stored CHD that exceeds the defined retention period. [Req 3.1]
- If sensitive authentication data is held, after authorisation all data must be deleted and rendered unrecoverable. [Req 3.2]
- Sensitive authentication data must not be stored after authorisation, including:
    - Full contents of any track (full track, track 1, track 2, magnetic stripe data) [Req 3.2.1]
    - Card verification code or value (CVV2, CVC2, CID, CAV2) [Req 3.2.2]
    - Personal identification number (PIN) [Req 3.2.3]

Commented [RS(2]: As discussed at security project board 8/9/17. RW says this does not apply to purchase cards and that this is a known risk. (It is unclear where this risk is recorded or how it is managed.)

    - Encrypted PIN block
- When displayed, the PAN must be masked so that at most only the first six and the last four digits are visible. Only personnel with a legitimate business need can see more than the first six and last four digits. [Req 3.3]
- Security policies and operational procedures for protecting stored CHD must be documented, in use, and known to affected parties. [Req 3.7]

Encrypt transmission of cardholder data [Req 4]

Sensitive cardholder data must not be transmitted or shared via insecure technologies.

- CHD including PANs are classed as CONFIDENTIAL information and must be handled in accordance with the University's Information Classification and Data Management policy
- Use of approved and certified PIN entry devices ensures secure encrypted transmission of CHD to the acquiring bank system.
- Encrypted and unencrypted PANs must not be sent via any end-user messaging technology including email, instant messaging, fax, chat or forum sessions. [Req 4.2]

Restrict physical access to cardholder data – held on paper records [Req 9]

All physical media including paper holding copies of CHD must be held and destroyed securely.

- All paper media containing CHD must be physically secured to prevent any access by unauthorised personnel, e.g. by storing them in a locked drawer, cabinet or safe. [Req 9.5]
- Internal or external distribution of any media must be strictly controlled [Req 9.6]:
    - Classify media to determine the sensitivity of the data [Req 9.6.1]
    - Send media via secured courier or other delivery method to enable tracking [Req 9.6.2]
    - Management must approve any movement of media from a secured area [Req 9.6.3]
- The storage and accessibility of media must be strictly controlled. [Req 9.7]
- All paper media containing CHD must be securely destroyed when no longer needed, and no longer than one day after creation. [Req 9.8.1]
- Storage containers used for holding paper media containing CHD awaiting destruction must be securely locked. [Req 9.8.1]

Restrict physical access to cardholder data – devices capturing data [Req 9]

All devices collecting CHD (such as PEDs) must be secured and protected against tampering or unauthorised substitution.

- There must be an up-to-date and accurate list of all devices that capture payment card data. The list must contain make, model, location, and serial number for the device. [Req 9.9.1]
- The list of devices must be updated when devices are added, relocated, replaced or decommissioned. [Req 9.9.1]
- Devices that capture payment card data must be regularly checked to ensure that they have not been tampered with or substituted. [Req 9.9.2]
- All staff operating devices that capture payment card data must be trained to be aware of suspicious behaviour and report tampering or substitution of devices. Training should include: verifying identity of individuals claiming to be service engineers; verifying any attempt to install, replace or return devices; being aware of suspicious behaviour around devices; and reporting any indication of suspicious behaviour or signs of tampering. [Req 9.9.3]

- Security policies and operational procedures for restricting physical access to CHD must be documented, in use, and known to affected parties. [Req 9.10]

Maintain a policy that addresses information security [Req 12]

Policies and procedures must be in place to address the requirements for the security of the University's cardholder data environment especially around the use of third party service providers.

- Policies covering use of critical technologies must be created, and proper use of those technologies must be defined. Critical technologies include: laptops, tablets, wireless access, remote access, removable media, email and internet. [Req 12.3]
- Usage policies must require:
    - Explicit approval by authorised individuals [Req 12.3.1]
    - A list of all devices and personnel with access [Req 12.3.3]
    - Acceptable uses of those technologies [Req 12.3.5]
- A security incident response and escalation procedure must be created. [Req 12.5.3, 12.10.1]
- A formal security awareness programme must be implemented to ensure that all personnel are aware of the CHD security policy and procedures and the importance of maintaining the security of CHD. [Req 12.6]
- A current and accurate list of approved service providers must be maintained including contact details for all personnel and a description of the services provided. [Req 12.8.1]
- For any services engaged with service providers that may affect or have a relationship or function associated with cardholder data environment, there must be a written agreement which includes an acknowledgement by the service providers of their responsibility for securing the CHD they possess, process or transmit. [Req 12.8.2]
- Due diligence must be exercised before engaging with any service providers that may affect or have a relationship or function associated with the University's cardholder data environment. [Req 12.8.3]
- Service providers' compliance with PCI DSS will be monitored and checked at least annually. [Req 12.8.4]
- Any agreement with a service provider must make clear which PCI DSS requirements are to be managed by the service provider, and which will be the responsibility of the University. [Req 12.8.5]

Responsibilities

Within this policy, the following individuals or groups have the following responsibilities [Req 12.4]:

Responsibility	**Owner**
Authorise installation of certified PEDs	FIN
Approve payment channels staff are allowed to use	FIN
Sign off on risks associated with use of non-compliant systems or suppliers in a payment channel	Director of Finance and Planning
Advise on the technical compliance of PEDs	ITCS
Install authorised PEDs	ITCS IT support
Advise on retention period including business justification for cardholder data	FIN
Add cardholder data to department RRS and ensure documented procedures exist supporting the RRS, covering a quarterly review of records, and the secure deletion of CHD at the end of the retention period	Departments using PEDs

Responsibility	Owner
Provide process for secure destruction of CHD	ITCS
Conduct checks to ensure card verification code is not stored, and that PANs are masked	Departments using PEDs
Create procedures to ensure operators do not store card verification codes, and full PANs are only viewed by authorised staff and never transmitted unencrypted via end-user messaging technologies	Departments using PEDs
Create procedures for the secure storage of physical media holding CHD	Departments using PEDs
Create and maintain list of PEDs and their authorised users including changes such as adding, relocating, replacing and decommissioning devices	FIN cashiers office
Organise and record the outcome of routine checks of PEDs to ensure they have not been tampered with or substituted	Departments using PEDs
Internal audit of compliance with this policy	ITCS
Offer training for PED operators covering tampering, substitution, suspicious behaviour, and verifying the identity of service engineers. Keep records of course completions and ensure only trained staff are allowed to operate PEDs	Departments using PEDs
Deliver general security awareness training for all staff operating PEDs covering the importance of securing CHD	ITCS
Create and maintain incident response plan	ITCS
Conduct due diligence checks, approval and selection of service providers and their regular review	ITCS
Ensure security policies are documented, in use, and known	ITCS
Draft agreements and manage relationship with approved service providers on a daily basis	Departments using PEDs
Maintain a list of approved service providers	FIN

References

This Face to Face and MOTO Card Payment Security policy is supported within the context of the following pieces of legislation, professional standards, and University documents:

- E-commerce security policy. https://portal.uea.ac.uk/documents/6207125/7103513/E-commerce+security+policy/
- General information security policy. https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies/information-security/gisp. In particular,
    - GISP3 – Physical and environmental security
    - GISP11 – Information classification
    - GISP14 – Incident monitoring and reporting
    - GISP16 – Legal and regulatory compliance
    - GISP17 – IT and information asset management
    - GISP18 – Encryption use and key material handling
    - GISP19 – Personnel security
    - GISP22 – Working with third parties
- Records management policy. https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies/records-management

- Information classification and data management policy https://portal.uea.ac.uk/documents/6207125/6857482/Information+classification+policy.pdf/
- PCI DSS Requirements v3.2. https://www.pcisecuritystandards.org/security_standards/pcidss_agreement.php?association=pcidss
- PCI SAQ B v3.2. https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-B.pdf
- PCI SAQ P2PE-HW v3.2. https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-P2PE.pdf
- PCI DSS Glossary v3.2. https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf

Breaches

Any breaches of this policy must be reported at the earliest opportunity to ITCS via misuse@uea.ac.uk. ITCS will lead on an investigation in consultation with FIN and the affected department. Serious breaches will be referred to HRD as matters to be deal with under staff disciplinary procedures.

Review

The Face to Face and MOTO security policy will be reviewed every 12 months or sooner as necessary by the ITCS Strategy, Policy and Compliance team to ensure it remains current in the light of relevant legislation, organisational procedures, contractual obligations or changes to the environment or updates to PCI requirements [Req 12.1.1]. Changes will be agreed with the Director of Information Services, and authorisation and quality assurance will be provided by the Information Strategy and Services Committee (ISSC).