UCD Payment Card Security Policy

1. Purpose

This policy has been created to assist the employees of University College Dublin ("the University") in understanding the importance of protecting credit/debit cardholder data and to inform employees on the new rules surrounding the safeguarding of this information.

This policy deals with the acceptable use and the controls required for receiving, processing and storing information in respect of all card receipts accepted and refunds made by the University. The University has three acceptance channels for card receipts and refunds made by the University; online payment systems, hand-help chip-and-pin terminals (customer present transactions) and telephone (customer not present transactions).

This document defines the University's payment card policy. As a merchant processing payment card data the University is required to comply with the Payment Card Industry Data Security Standard (PCI DSS) as defined by the Payment Card Industry Security Standards Council. This is a worldwide security standard created by the industry to combat fraud through increased controls around card data and its exposure to compromise. Compliance is monitored by the card providers (MasterCard, Visa, etc.) and organisations that fail to meet compliance requirements risk losing their ability to process card payments, being audited and/or fined and incur potential reputational damage.

It is important to note that the University is liable to substantial fines from its merchant service provider should it fail to comply with PCI DSS.

The University's approach to PCI compliance is to ensure that cardholder data is not stored, processed or transmitted over its IT network. This reduces the scope of PCI compliance and so controls the cost, difficulty and feasibility of implementing and maintaining the requisite PCI DSS controls.

Any UCD subsidiary, ancillary companies, core activities, commercial licence holder or third party commercial entity that wishes to use the UCD IT infrastructure must comply with this policy.

2. Definitions

- Payment Card – A card backed by an account holding funds belonging to the cardholder, or offering credit to the cardholder such as a debit or credit card.
- PCI DSS – The "Payment Card Industry Data Security Standard". See https://www.pcisecuritystandards.org/security standards/ for details.
- PAN – A "Primary Account Number" is a 14 or 16 digit number embossed on a debit or credit card and encoded in the card which identifies the issuer of the card and the account.
- PIN – A "Personal Identification Number" is a secret numeric password used to authenticate payment cards.

- CVC – A card verification Code provides extra security to credit and debit cards. On Visa and MasterCard it is the 3-digit number found on the signature bar on the back of the card.
- Cardholder Data – Payment card data including: Primary Account Number (PAN), Personal Identification Number (PIN), name of cardholder, expiration date and CVC.
- Cardholder Data Environment (CDE) – This includes all processes and technology as well as the people that store, process or transmit customer data or authentication data, including connected system components and any virtualization components (i.e., servers, applications etc.)
- PDQ Machine – A credit card swipe machine
- PED – PIN Entry Device
- Merchant Account – A Merchant Account is a type of bank account that allows businesses to accept payments by payment cards, typically debit or credit cards.
- Merchant Account Provider – Merchant Account Providers give businesses the ability to accept debit and credit cards in payment for goods and services.
- UCD Merchant Account Owner – UCD Staff Member who formally requests the merchant account and is responsible for the day-to-day operation of the account.
- Legacy data is data that is stored in physical or electronic format and is not currently used or managed.
- Payment Services Provider – Facilitating secure online payments.
- PCI Certification – Payment Card Industry card payment security standards certificate of compliance.
- Virtual Terminal – Facility to process cardholder information through an external payments service providers online facility via an authorised UCD staff members PC

3. Scope

PCI DSS requirements apply to all systems that store, process or transmit cardholder data or can impact the security of cardholder data. This policy is designed to enforce a zero CDE footprint on the University's IT infrastructure i.e. no cardholder data can be stored on any UCD computer system, or processed or transmitted over the UCD network. All e-commerce transactions and point of sale transactions must be isolated from the UCD network.

All units and staff must adhere to this policy to minimise the risk to both customers and the University.

All University card processing activities and related technologies must comply with PCI DSS and adhere to this policy. No activity may be conducted nor any technology employed that might obstruct compliance with PCI DSS standards.

In particular, each merchant account owner is responsible for ensuring that this policy is fully adhered to. Any staff member handling cardholder data must also comply.

Any UCD subsidiary, Campus Company, or third part commercial concerns operating on the UCD Campus must conform to this policy if they wish to use the UCD IT infrastructure.

4. Supporting Standards & Procedures

This policy should be read in conjunction with the following University policies and Users should ensure compliance with these policies in addition to this policy:

http://www.ucd.ie/dataprotection/policy.htm

https://www.ucd.ie/foi/recordk/rmpolicy.html

http://www.ucd.ie/itservices/aboutus/acceptableusepolicy/

5. PCI DSS Compliance Policy

It is prohibited to send cardholder data by email, store such data via electronic methods (i.e. excel spreadsheets, word documents, access databases), transmit cardholder data over the University networks or write down card details belonging to a payer. This includes occasions where e-commerce systems may be unavailable and in such instances, students/customers should be contacted when the system returns to live mode.

Receiving payment by card when a customer is not present

Under no circumstances should card details be taken by email, fax, or by post or on an order form. Should a customer send in any card details by post or by fax, these should be shredded immediately. Emails should be deleted immediately.

Cardholder data processed over the phone

Receiving payment by card when a customer is not present (other than online) is discouraged, however, it is recognised that customers may sometimes wish to make payments over the phone. Where the order taker must take details over the phone, he/she must have immediate access to a card terminal. In such circumstances, the order taker must enter the card transaction directly into the card terminal. Under no circumstances should any customer details be written on a piece of paper or entered into a computer. If a transaction is successfully processed, a merchant copy should be stored within the till drawer or cash box for the duration of the working day. At the end of the business day

these receipts should be filed in a secure filing cabinet. The customer copy must be sent to the customer. If the transaction is declined, the customer should be advised immediately.

Cardholder Data Processed Online

It is essential that any department wishing to take online payments ensures that card details are not processed on the University IT network or retained by the University or any third party on behalf of a UCD School/Unit. In this instance, contact must be made with IT services to arrange the creation of a website on the UCD network which will be fully PCI compliant. Should a School/Unit wish to use an alternative web design company or third party to host its online payment facility, proof of PCI Compliance must be submitted to the Finance Office for approval. School/Units must not arrange for e-commerce sites to be set up without prior approval. All University hosted e-commerce websites or applications must be managed by an external IT company with sufficient skills to secure e-commerce sites. The site must also employ payment re-direct integration with an approved external payment provider to ensure that card holder information is not processed on the University network. This means that the cardholder information is entered by the customer on the external service providers IT system.

All outsourced e-commerce solutions (when using a UCD merchant account) must meet PCI DSS standards. This requires that the external provider must have PCI certification and contracts must explicitly include this requirement. The PCI status of these providers must be forwarded the Finance Office prior to the e-commerce application becoming operational. The use of a *'Virtual Terminal'* for processing payments over the University network is prohibited and not to be used by any University School/Unit.

Receiving payment by card when a customer is present

When the customer is present at a card terminal, it is essential that the customers enter their PIN number into the card terminal unobserved. The customer's PIN and other card details must not be written down, electronically copied or otherwise obtained or recorded. If a transaction is successfully processed, a merchant copy should be stored within the till drawer or cash box for the duration of the working day. At the end of the business day these receipts (PAN rendered unreadable) should be filed in a secure filing cabinet. The customer copy must be given to the customer.

Specifically,

1. The storage of cardholder information in electronic files, (including Excel, Word, databases, etc.) is expressly forbidden. This includes PAN, PIN, CVC, expiry dates, etc.

2. Any legacy payment card data should be reported to the Finance Office and arrangements made for its deletion (or quarantine).

3. All UCD e-commerce applications must employ re-direct integration with an external payment services provider. This means that the cardholder information is entered by the

customer on the external service provider's IT system. The cardholder data must not be transmitted back to the UCD e-commerce application.

4. Cardholder data must not be sent via email or other end-user messaging technologies (e.g. instant messaging chat), whether or not it is encrypted.

5. All outsourced e-commerce solutions (when using a UCD merchant account) must meet PCI DSS standards. This requires that the external provider must have PCI certification and contracts must explicitly include this requirement. The PCI status of these providers must be reviewed annually by the School/Unit merchant account owner.

6. Devices routinely used to process payment cards, such as tills, PDGs, and PEDs:
   a. Must never be connected to the UCD network,
   b. Must themselves carry PCI DSS certification,
   c. Must be adequately safeguarded against loss or theft,
   d. Must only be used by staff authorised to do so as part of their duties, and
   e. Must be protected from physical access and misuse out-of-hours.

7. Staff must not request transmission of any cardholder data via email or other end-user messaging technologies. If such data arrives unsolicited then it should be deleted, and under no circumstances should it be redirected elsewhere (even back to the sender).

8. Online refunds, through external payment service providers must operate without the need for entering PANs. Typically, an order number will be used to refund to the card via the chosen e-commerce solution. Other refund acceptance channels may also be chosen at the discretion of the School/Unit.

7. Roles and Responsibilities

The key responsibilities in connection with the policy for cardholder data security are as follows:

College Principals/Administrative Offices/Research Centres

College Principals and Administrative Offices are responsible for ensuring that this policy is adhered to and that no payment processes are in place or put in place without consultation with the Finance Office.

Heads of Schools/Units / Research Institutes

Heads of Schools/Units /Research Institutes are responsible for ensuring that this policy is adhered to, in particular in relation to receiving, transmitting, processing and storing cardholder data.

School/Unit Administrators

School/Unit Administrators must ensure, where cards are accepted for payment of goods and services that cardholder data is received and processed is in accordance with this policy.

Internal Audit

The Internal Audit function is responsible for checking that School/Units / Research Units are complying with PCI policy and where they become aware of any instance of non-compliance will advise the Finance Office.

Finance Office

The Finance Office has responsibility for ensuring that card data security policy is communicated to all relevant parties. Where the Finance Office becomes aware that the PCI policy is not being adhered to it will remove payment card processing functionality from that School/Unit / Research Unit. Regular review, of the policy, procedures, and internal and external regulations will be the joint responsibility of the Finance Office and IT Services.

Initiation of the annual PCI Certification process will be undertaken by the UCD Finance Office.

IT Services

IT Services will assist with external and internal network security scans required for PCI DSS Compliance.

The Legal Office

The Legal Office is responsible for ensuring that contracts reviewed by them which are to be entered into with external parties which process cardholder data for UCD merchant accounts include an acknowledgement that the service providers are responsible for the security of the cardholder data that they possess and are formally PCI certified.

8. Breach of this Policy

Any suspected or actual security incidents involving cardholder data should be reported immediately to the Finance Office (see contact details below). No one should communicate with anyone outside of their supervisor(s) or the Finance Office about any details or generalities surrounding any suspected or actual incident.

The Finance Officer will immediately notify the Information Compliance Officer (The Legal Office) of any data security breach involving personal data.

Any staff member in breach of this policy will be subject to disciplinary action up to and including dismissal in accordance with the University's disciplinary procedures for staff.

9. Further Information

If you have any queries in relation to this policy, please contact:

The Finance Officer

University College Dublin

10. Policy Revision History

Version	Date	Description	Author
1.0	24/04/2017	Policy created	UCD Bursar's Office
1.1	19/05/2017	Policy amended with recommended updates	UCD Internal Audit
	02/06/2017	Policy reviewed	UCD IT Services (MSU)
1.2	06/06/2017	'Card Data Processed Online' section amended	UCD IT Services
1.3	11/07/2017	Policy reviewed with recommended updates	UCD Legal Office
1.4	12/07/2017	Policy reviewed with recommended updates	UCD Finance Systems
1.5	25/09/2018	UCD UMT Approval 25th September 2018	UCD Bursar's Office