University College Cork – National University of Ireland, Cork

Payment Card Security Policy

PCI DSS 2.0

Document Location

Finance Office Policies http://www.ucc.ie/en/policiesandprocedures/financeoffice/bc/

Revision History

Date of this revision: 18/11/13	**Date of next review: 01/11/14**

Version Number/Revision Number	**Revision Date**	**Summary of Changes**
1.0	20/03/2013	Initial draft using IS standard template
2.0	29/04/2013	Finance Office changes applied; plus some edits by JB
3.0	16/10/2013	Consolidated feedback from PCI Compliance Project Team
4.0	18/11/2013	Minor amendments (MMcS, DS, JB)

Approval

This document requires the following approvals:

Name	**Title**	**Date**
Diarmuid Collins	Bursar	December 2013
Michael Farrell	Corporate Secretary	December 2013
Gerard Culley	Director of IT Services	December 2013
UMTO	UMTO	December 2013

This policy shall be reviewed and updated on an annual basis.

Table of Contents

1. PURPOSE

This policy has been created to assist employees of University College Cork ("the University") in understanding the importance of protecting credit/debit cardholder data and to inform employees on the new rules surrounding safeguarding 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 cards receipts accepted and refunds made by the university: online payment systems, hand-held chip-and-pin card 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 and being audited and/or fined.

It is important to note that the University is liable to substantial fines from its merchant bank 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 limits the scope of PCI compliance and so controls the cost, difficulty and feasibility of implementing and maintaining the requisite PCI DSS controls.

Any UCC subsidiary companies that wish to use the UCC 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), 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 cardholder 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.
- Merchant Account Owner – UCC 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.

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 footprint CDE on the university's IT infrastructure i.e. no cardholder data can be stored on any UCC computer system, or processed or transmitted over the UCC network. All e-commerce transactions and point of sale transactions must be isolated from the UCC 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 UCC subsidiary, Campus Company, or third party commercial concerns operating on the UCC Campus must conform to this policy if they wish to use the UCC IT infrastructure.

4. SUPPORTING STANDARDS & PROCEDURES

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

- UCC Bank Account Procedures – http://www.ucc.ie/en/media/support/financeoffice/capital/BankAccountProcedures.pdf
- UCC Data Management Policy - http://www.ucc.ie/en/media/support/itpolicies/policies/DataManagementPolicy.pdf

5. PCI DSS COMPLIANCE POLICY

It is strictly 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 network or write down card details belonging to a payee. This includes occasions where the 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.

Policy for Cardholder Data Processed Online

It is recommended that any department wishing to take payments online where goods or services can be sold online must use a secure online payment facility. In this instance, contact must be made with IT Services to arrange the creation of a web site on the UCC network which will be fully PCI compliant. Should a department wish to use an alternative web design company or third party to host its online payment facility, sanction must be approved in advance by IT Services and the Treasury Section of the Finance Office. Departments must not arrange for e-commerce sites to be set up without prior approval. For all card details which are processed through an online system, no

card details must be retained by the University or by any third party hosting the web site on behalf of a UCC department.

Receiving payment by card when a customer is present

Where the customer is present at a card terminal, it is essential that 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 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 UCC e-commerce applications must employ **re-direct** integration with an external payment services provider (e.g. Realex). 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 UCC 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 UCC 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 merchant account owner.

6. Devices routinely used to process payment cards, such as tills, PDQs, and PEDs:

    a. must never be connected to the UCC 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 (e.g. through Realex) must operate without the need for entering PANs. Typically an order number will be used to refund to the card.

6. ROLES AND RESPONSIBILITIES

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

Heads of Colleges/Administrative Offices/Research Centres

Heads of Colleges and Administrative Offices are responsible for ensuring that this policy is adhered to and is confirmed in writing in the Annual Governance and Statement of Internal Control, and that no payment processes are in place or put in place without consultation with the Finance Office.

Heads of Schools/Departments/Research Units

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

Departmental Administrators

Departmental 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 Schools/Departments/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 this 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/Department/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.

IT Services

IT Services is responsible for ensuring that a secure network is maintained and that the IT infrastructure is consistent with and supports PCI controls. IT Services is responsible for arranging

and assessing any external and internal network security scans required for PCI DSS compliance. Initiation of the annual PCI Certification process will be undertaken by IT Services.

The Office of Corporate and Legal Affairs

The Office of Corporate and Legal Affairs (OCLA) is responsible for ensuring that contracts signed with external service providers which process cardholder data for UCC 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. The OCLA is also responsible for co-ordinating communications with external agencies and the public in the event of a breach.

7. 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 (Office of Corporate & Legal Affairs) 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.

8. FURTHER INFORMATION

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

The Finance Officer

University College Cork

Tel: 021-4903451

Email: MMcSweeney@fin.ucc.ie