Dublin Institute of Technology

Payment Card Security Policy

Version 1.0
## Document Location

http://www.dit.ie/aadlt/ictservices/security/itsecuritypolicies/

## Revision History

<table>
<thead>
<tr>
<th>Version Number/Revision Number</th>
<th>Revision Date</th>
<th>Summary of Changes</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Oct 2017</td>
<td>Initial draft</td>
<td>E Dunne, R Dunne</td>
</tr>
<tr>
<td>0.2</td>
<td>Feb 2018</td>
<td>Updates and corrections</td>
<td>E Dunne, R Dunne</td>
</tr>
</tbody>
</table>

## Approval

This document requires the following approvals:

<table>
<thead>
<tr>
<th>Name of approval body</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLT Campus Development sub-committee</td>
<td>27 Feb 2018</td>
</tr>
</tbody>
</table>
1. TABLE OF CONTENTS

1. TABLE OF CONTENTS ................................................................................................................. 3
2. PURPOSE ........................................................................................................................................ 4
3. DEFINITIONS .................................................................................................................................. 4
4. SCOPE ........................................................................................................................................... 5
5. SUPPORTING STANDARDS & PROCEDURES.............................................................................. 5
6. POLICY STATEMENTS ....................................................................................................................... 6
7. ROLES AND RESPONSIBILITIES ................................................................................................. 7
6. BREACH OF THIS POLICY ............................................................................................................. 8
7. FURTHER INFORMATION ................................................................................................................. 8
2. PURPOSE

This policy has been created to assist staff of the Dublin Institute of Technology (“the Institute”) in understanding the importance of protecting payment card data, and to describe the 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 Institute. DIT has three acceptance channels for cards receipts accepted, and refunds made by the Institute: online payment systems, hand-held chip-and-pin card terminals (customer present transactions), and telephone (customer not present transactions).

This document defines the Institute’s payment card policy. As a merchant processing payment card data, DIT 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.

It is important to note that DIT could be liable to substantial fines and/or compensation claims should it fail to comply with PCI DSS.

The Institute’s approach to PCI compliance is to ensure that cardholder data is not stored, processed or transmitted over its ICT infrastructure. This limits the scope of both PCI compliance, and any associated cost and effort in implementing and maintaining the requisite PCI DSS controls.

3. 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” which applies to any payment card/device bearing the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard, or Visa
- **Customer** – The recipient of an invoice by the Institute, including students, who wishes to make payment using a payment card covered under PCI DSS
- **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: 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.
- **PED** – PIN Entry Device, or card terminal
- **Payment Processor** - Sometimes referred to as “payment gateway” or “payment service provider (PSP)”.

DIT Payment Card Security Policy
Entity engaged by a merchant or other entity to handle payment card transactions on their behalf

- **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 Owner** – Authorised DIT Staff Member who formally requests the merchant account, and is responsible for the day-to-day operation of the account
- **Virtual Payment Terminal** - A virtual payment terminal provides web-based access to a third party website to authorise payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card

### 4. 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 Institute’s ICT infrastructure i.e. no cardholder data can be stored on any DIT computer system, or processed on the DIT network. All point of sale transactions involving card terminals must be isolated from the DIT network.

All DIT staff must adhere to this policy to minimise the risk to both customers and the Institute.

All card processing activities conducted on behalf of DIT 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.

Any DIT affiliate, Hothouse client company, or third party commercial concerns operating on the DIT Campus must conform to this policy if they wish to use the DIT ICT infrastructure.

### 5. SUPPORTING STANDARDS & PROCEDURES

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

- **Fraud Policy and Response Plan** - [http://dit.ie/intranet/media/intranet/finance/policiesandprocedures/FR.1%20Fraud%20Policy%20Approved%20by%20GB_2.pdf](http://dit.ie/intranet/media/intranet/finance/policiesandprocedures/FR.1%20Fraud%20Policy%20Approved%20by%20GB_2.pdf)
  - Information Handling
  - Cryptography
  - Password Standard
6. POLICY STATEMENTS

It is strictly prohibited to send cardholder data by email, photo, or text message, or to store such data via electronic methods (i.e. spreadsheets, documents, databases), transmit cardholder data over the DIT network, or write down card details belonging to a customer. This includes occasions where the e-commerce systems may be unavailable and in such instances, 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, text message, 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 or other electronic messages should be deleted immediately.

Cardholder Data Processed over the phone

Receiving payment by card when a customer is not present (other than online) is not considered ideal. However, it is recognised that customers may wish to make payments over the phone. In such circumstances, the DIT agent must enter the card transaction immediately into a card terminal or VPT, and not repeat the card details back to the customer. Under no circumstances should any customer details be written on a piece of paper or entered into a computer (other than through the VPT). 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

A department wishing to accept payments for goods or services must have the prior approval of Corporate Services for the use a secure online payment facility. Where said department wishes to utilise the DIT infrastructure for the creation of an on-line payment facility, they must contact ICT Services to review the security arrangements. For all card details, which are processed through an online system, no card details must be retained by the Institute, or by any third party hosting the web site on behalf of a DIT department.

Receiving payment by card when a customer is present

Where the customer is present at a card terminal, the department receiving the payment must ensure that customers have sufficient privacy to enter their PIN 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 spreadsheets, images, documents, databases, etc.) is expressly forbidden. This includes PAN, PIN, CVC, expiry dates, etc.
2. Any legacy payment card data should be reported to the Head of Finance and arrangements made for its deletion (or quarantine)

3. All DIT e-commerce applications must employ re-direct integration with a DIT-approved 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 DIT e-commerce application

4. All outsourced e-commerce solutions (when using a DIT 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

5. Devices routinely used to process payment cards, such as card terminals, point of sale systems:
   a. must never be connected to the DIT network
   b. must themselves carry PCI DSS certification
   c. must be adequately safeguarded against loss, theft, or tampering
   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 while not attended

6. Staff must not transmit nor 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).

7. Any refund must be approved by the appropriate Merchant Account Owner. The refund should be processed back to the source card from which the original transaction was authorised without the need for entering PANs. If there has been a delay since payment, it may not be possible to make the refund due to security measures implemented by the Payment Processor. In this instance, the customer should be contacted by Corporate Services for alternative details for the refund to be processed

8. Any records of transactions should be held for no longer than the period specified in the appropriate record retention schedule

7. ROLES AND RESPONSIBILITIES

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

**Senior Leadership Team (SLT)**
- To ensure that this policy is adhered to, and is confirmed in writing in the Annual Governance Statement, and the Statement on Internal Control
- That no payment processes are in place or put in place without consultation with Corporate Services

**Merchant Account Owners**
- To ensure that where cards are accepted for payment of goods and services, that cardholder data is received and processed is in accordance with this policy
- To provide training for all staff with responsibility for processing payment cards
Internal Audit

- To ensure that Schools/Departments/Research Units are complying with DIT policy on PCI DSS, and where they become aware of any instance of non-compliance, to advise Corporate Services

Corporate Services

- To ensure this card data security policy is communicated to all relevant parties
- To review and approve requests for payment facilities
- To remove payment card processing functionality from any department that does not adhere to this policy
- To undertake regular reviews of the policy and associated procedures under the joint responsibility of the Head of Finance and the Chief Information Officer
- To ensure completion of the annual PCI certification process
- To coordinate communications with external agencies, including the Office of the Data Protection Commissioner, and the public in the event of a data breach.

ICT Services

- To ensure that a secure network is maintained and that the ICT infrastructure is consistent with and supports PCI controls
- To arrange for and assess any external and internal network security scans required for PCI DSS compliance

6. BREACH OF THIS POLICY

Any suspected or actual security incidents involving cardholder data should be reported immediately by telephone to the DIT Support Desk (01 402 3123). No one should communicate with anyone outside of their supervisor(s) or the Head of Finance about any details or generalities surrounding any suspected or actual incident.

The Head of Finance, the Chief Information Officer, or their designated appointees will immediately notify the Information Governance Officer of any data security breach involving personal data, to facilitate any external reporting within the required timelines.

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

7. FURTHER INFORMATION

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

The IT Compliance Officer, ICT Services, Dublin Institute of Technology
Tel: 01-402 3453 / Email: eoin.dunne@dit.ie

For further information on PCI DSS, please visit: https://www.pcisecuritystandards.org/