Electronic Information Security: Payment Card Industry Data Security Standards (PCI-DSS) Procedures (Australia only)

Policy Statement

The Payment Card Industry Data Security Standards (PCI-DSS) are a set of guidelines developed by MasterCard, Visa, American Express, Discover and JCB International to assist merchants in preventing payment card fraud and to improve security around processing and storing payment card details. Any company processing, storing or transmitting the above branded payment card numbers must be PCI-DSS compliant or they risk losing the ability to process these payments.

TLC Learning is required to be compliant with the PCI-DSS. Non-compliance can result in fines to merchants of at least $10,000 per month and $500,000 per card brand (e.g. Visa, MasterCard) if there is a data breach.

PCI DSS Compliance

PCI compliance has been required since December 2010.

These procedures are designed to deal with situations where a company or individual provides their cardholder data to the Registered Training Organisation (RTO) for the purposes of paying an account (of any type).

Under PCI DSS requirements, TLC Learning is required to use, store and destroy cardholder data in a manner which protects the cardholder data from misuse or unauthorised transactions.

Responsibility - All Staff

Procedures

1. Companies and individuals must be prevented from providing any cardholder data via an email or VoIP facsimile.

   If such a request is received:

   - The email or VoIP fax should be replied to immediately with the credit card number deleted - stating that "TLC Learning does not accept payment card holder information via VoIP fax or email as it is not a secure method of transmitting cardholder data".
   - The email or fax is to be securely destroyed.

   Responsibility - All Staff

2. Minimal cardholder data is to be stored in hard copy format. There must be a legitimate business need to store cardholder data. Any cardholder data that is stored in hard copy must be stored in a highly secure and protected manner within a locked filing cabinet or safe within a locked office.

   Responsibility - All Staff

3. Cardholder data is not to be stored, processed, or transmitted on TLC Learning's computers in any form unless an exception has been approved by the eSolutions IT Security and risk manager. If cardholder data is stored, processed, or transmitted as electronic data, appropriate security measures must be utilised in accordance with PCI DSS. This may include but is not limited to:

   - Reducing the scope of PCI DSS compliance by segmenting the CDE network.
   - Segmenting payment card processing from the normal business use of workstations and using separate physical devices or virtual machines on a secure host.
   - Restricting access to the hosts that store cardholder data to systems that have a legitimate business need to access the data.
   - Separating duties of servers such that a web server in the CDE is not also running a database server.
   - Installing a state-of the art packet inspection firewall in the CDE and ensuring that the firewall has both ingress and egress rules.
   - Collecting logs from all devices in the CDE and shipping them to a centralised, backed up logging server.
   - Performing internal and external vulnerability scanning at least quarterly or when configurations change, and performing an internal and external penetration test at least annually. External scans will need to be performed by a PCI approved scanning vendor.
   - Ensuring that physical access to systems in the CDE is restricted to those individuals with a legitimate business need and all server consoles are locked or logged off.

   Responsibility - All Staff

4. All EFTPOS machines and other such devices used to collect cardholder data must be either on a tamper proof stand or stored securely (particularly when not in use, e.g. overnight). Tamper evident stickers across the seams of the EFTPOS terminals should also be used if available.

   Responsibility - All Staff

5. Only appropriate staff may have access to cardholder data, and appropriate training for such staff is to be conducted on an annual basis. All staff who handle cardholder data will be required to sign an acknowledgement of understanding and compliance with this policy.

   Responsibility - All Staff who handle cardholder data

6. Cardholder information is to be transferred securely. Therefore, no cardholder data is to be emailed or VoIP faxed either internally or externally between staff or learners (the only exception being if a direct line/analogue facsimile has been specifically installed for this purpose).

   Responsibility - All Staff

7. All service provides and third party vendors providing payment card related services for TLC Learning must be PCI DSS compliant.

   Responsibility - All Staff

8. Cardholder data is not be stored simply for chargeback purposes. Storing the first six and last four digits of a cardholder number, along with time, date, transaction identification and amount is adequate. Cardholder data is not to be retained for longer than six months after the date of processing the transaction.

   Responsibility - All Staff

9. When there is no need to retain hard copy cardholder data, the cardholder data must be destroyed using at least one of the following methods: cross cut shredding, incinerating, or pulping. (E.g. the portion of the form that contains the cardholder data can be cut out and shredded or the entire form can be shredded.)

   Responsibility - All Staff

10. Payment card security codes (CVV2, CVC2, CID etc.) are not to be stored or recorded under any circumstances once a transaction has been processed.

    Responsibility - All Staff

11. Definition of terms

PCI-DSS: Payment Card Industry Data Security Standard.
EFTPOS: Electronic Funds Transfer Point of Sale. Faculties and portfolios have machines that accept Visa, MasterCard, Amex and Diners Club payments.
Cardholder Data: PAN only or PAN plus either of the following: Cardholder name, Expiration data.
CDE (Cardholder Data Environment): The people, processes and technology that store, process or transmit cardholder data, or sensitive authentication data, including any connected system components.
CCV (Credit Card Verification): The 3-digit number on the signature panel of a Visa or MasterCard, or the 4-digit number on the front of the Amex Card (above the logo). These are referred to as CAV2, CVC2, CVV2, or CID depending on payment card brand. The following list provides the terms for each card brand.
CAV2: Card Authentication Value (JCB) on signature panel.
CVC2: Card Verification Code (MasterCard) on signature panel.
Firewall: Hardware and/or software technology that protects network resources. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.
PAN (Primary Account Number): Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
VoIP: Voice over Internet Protocol.
Analogue Fax: A fax received via an analogue line directly to a fax machine.
Payment Card: Any credit or debit card that bears the logo of Visa, MasterCard, American Express, Diners Club, Discover, JCB, China Union Pay.

12. Related/relevant legislative/policy frameworks

12.1 The Financial Viability Risk Assessment Requirements

12.2 National Vocational Education and Training Regulator Act 2011 (Cwt.)

12.3 PCI DSS requirements (Australia)

13. Related documents

13.1 Fees and Charges Policy and Procedure

13.2 Refund of Fees Policy and Procedure

13.3 Deferral/Withdrawal Policy and Procedure

13.4 Enrolment form