PAYMENT CARD INDUSTRY DATA SECURITY STANDARD POLICY AND PROCEDURE

CONTENTS

1 PURPOSE

1.1 This policy and procedure is designed to deal with situations where a company or individual provides their cardholder data to CQUniversity, for the purposes of making payment to the University. This policy and procedure also applies to any owned subsidiaries and all entities within CQUniversity.

2 SCOPE

2.1 This policy and procedure applies to CQUniversity as a corporate entity, CQUniversity Council, including members, staff of CQUniversity and controlled entities.

3 POLICY STATEMENT

3.1 The Payment Card Industry Security Standard (PCI DSS) is 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.

3.2 CQUniversity is required to be compliant with the PCI DSS in order to accept credit card payments in any capacity. Compliance is overseen by the relevant acquiring banking institution and enforced by the Payment card brand (e.g. Visa, Mastercard, etc). Failure to comply with the PCI DSS may result in substantial fines and penalties.

3.3 The requirements of the Standard, and therefore this policy and procedure, are based on six goals and 12 requirements:

- Build and maintain a secure network

- Requirement 1: install and maintain a firewall configuration to protect cardholder data
- Requirement 2: do not use vendor-supplied defaults for system passwords and other security parameters

- Protect cardholder data
  - Requirement 3: protect stored cardholder data
  - Requirement 4: encrypt transmission of cardholder data across open, public networks
- Maintain a vulnerability management program
  - Requirement 5: use and regularly update anti-virus software
  - Requirement 6: develop and maintain secure systems and applications
- Implement strong access control measures
  - Requirement 7: restrict access to cardholder data by business need-to-know
  - Requirement 8: assign a unique ID to each person with computer access
  - Requirement 9: restrict physical access to cardholder data
- Regularly monitor and test networks
  - Requirement 10: track and monitor all access to network resources and cardholder data
  - Requirement 11: regularly test security systems and processes
- Maintain an information security policy
  - Requirement 12: maintain a policy that addresses information security

3.4 Non-compliance can bring about suspension of merchant accounts, fines/penalties from the payment card industry and providers. Substantial fines can apply to the following:

- per data security breach
- per day for non-compliance with published standards
- liability for all fraud losses incurred from compromised account numbers
- liability for the cost of re-issuing cards associated with the compromise, and
- suspension of merchant accounts resulting in the inability to accept credit card payments.

4 PROCEDURE

4.1 Under PCI DSS requirements, CQUniversity is required to use, receive, transmit, store and destroy cardholder data in a manner which protects the cardholder data from misuse or unauthorised transactions. CQUniversity is required to comply with all requirements specified in the PCI DSS to achieve and maintain compliance.

Build and maintain a secure network

4.2 CQUniversity is required to build and maintain a secure network for receiving, transmitting and storing cardholder data. This includes installing and maintaining appropriate firewall configuration to protect cardholder data.

4.3 All staff must adhere to the Information and Communications Technology Passwords Procedure.

Protect cardholder data

Receiving payment card information

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

4.5 If such a request is received the transmission will be blocked and an appropriate response will be returned to the customer.

Transmitting payment card information

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

Storing payment card information

4.7 Minimal cardholder data will 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.

4.8 Cardholder data will not to 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 sufficient. Cardholder data will not be retained for longer than six months after the date of processing the transaction.

4.9 Cardholder data will not be stored, processed, or transmitted on CQUniversity computers in any form. However, 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 cardholder data environment (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 stateful 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.

4.10 Cardholder data must not be stored in any customer relationship management, document management or records management system (e.g. TRIM).

Destroying hard copy payment card information

4.11 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.)

Removing/modifying electronic payment card information

4.12 In the event that cardholder data is identified as being stored in an unsecure environment, it must be removed. Data must be removed by purging or truncation methods in accordance with the PCI DSS. Only the Information and Technology Directorate (IaTD) will be permitted to delete data. An IaTD Technology and Services Assistance Centre (TaSAC) case must be logged to delete data. IaTD will liaise with the relevant Finance and Planning Division staff in relation to deleting or modifying the cardholder data.

Card authentication or verification codes

4.13 Credit card verification (CCV) codes (CVV2, CVC2, CID etc) will not be stored or recorded under any circumstances once a transaction has been processed.

Maintain a vulnerability management program

4.14 CQUniversity is required to use and regularly update anti-virus software on all systems commonly affected by malware. This includes adhering to the PCI DSS scan requirements by performing vulnerability scans of internet-facing environments of merchants and service providers.

Secure systems

4.15 All critical systems must have the most recently released software patches to prevent exploitation. The University will apply patches to less-critical systems as soon as possible, based on a risk-based vulnerability management program. Secure coding practices for developing applications, change control procedures and other secure software development practices should always be followed:

- ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Deploy critical patches within a month of release
- establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. Risk rankings should be based on industry best practices and guidelines
- develop software applications (internal and external, and including web-based administrative access) in accordance with PCI DSS and based on industry best practices. Ensure all public-facing web applications are protected against known attacks, either by performing code vulnerability reviews at least annually or by installing a web application firewall in front of public-facing web applications
- follow change control processes and procedures for all changes to system components
- select third party cloud providers that comply and support Australia PCI legislation and standards
- develop applications based on secure coding guidelines and review custom application code to identify coding vulnerabilities. Follow up-to-date industry best practices to identify and manage vulnerabilities.

Implement strong access control measures

4.16 CQUniversity must ensure access to cardholder data is restricted by the use of physical and/or technical control measures.

Securing devices

4.17 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 be used.

Handling payment card information

4.18 Only appropriate staff may have access to cardholder data, and appropriate training for such staff will 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 and procedure.

Service providers and third party vendors

4.19 All service providers and third party vendors providing payment card related services for CQUniversity must be PCI DSS compliant. The Finance and Planning Division will request appropriate certification from all service providers and third party vendors and maintain sufficient records.

Regularly monitor and test networks

4.20 To prevent exploitation of data and systems, CQUniversity must regularly monitor and test networks to find and fix vulnerabilities. System components, processes, and custom software should be tested frequently to

ensure security is maintained over time. Testing of security controls is especially important for any environmental changes such as deploying new software or changing system configurations.

Maintain an information security policy

4.21 CQUniversity is required to maintain a policy in relation to information security, and has an Information Security Management Policy.

5 RESPONSIBILITIES

Compliance, monitoring and review

5.1 The Deputy Vice-Chancellor (Finance and Planning) is responsible for monitoring, reviewing and ensuring compliance with this policy and procedure.

5.2 The Finance and Planning Division and IaTD, in conjunction with key business areas, will progressively implement the policy and procedure to ensure full compliance is achieved.

5.3 CQUniversity will comply with all guidelines and requirements set by the PCI Security Standards Council. Compliance will be monitored by the Finance and Planning Division and IaTD, and the relevant acquiring banking institutions that provide CQUniversity with the ability to accept credit or debit card payments

Reporting

5.4 Annual verification of compliance must be supplied to any banking institution that provides CQUniversity with the means to accept the abovementioned card payments.

Records management

5.5 The Finance Operations Manager is responsible for ensuring all record management requirements are met.

5.6 Staff must maintain all records relevant to administering this policy and procedure in a recognised University recordkeeping system.

6 DEFINITIONS

6.1 Terms not defined in this document may be in the University glossary.

Terms and definitions

Cardholder: the customer to whom the payment card has been issued to.

Cardholder data: all personally identifiable data associated with the cardholder. Primary account number (PAN) only or PAN plus either of the following: cardholder name, expiration data.

Cardholder data environment (CDE): The people, processes and technology that store, process or transmit cardholder data, or sensitive authentication data, including any connected system components.

Cloud service providers: includes any SaaS (Software as a Service) or PaaS (Platform as a Service) the University engages to provide card holder services.

Credit card verification (CCV): 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.

EFTPOS: Electronic Funds Transfer Point of Sale. Faculties and portfolios have machines that accept Visa, MasterCard, Amex and Diners Club payments.

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.

Payment card: any credit or debit card that bears the logo of Visa, Mastercard, American Express, Diners Club, Discover, JCB, China Union Pay.

Primary account number (PAN): unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

Sensitive authentication data: security related information pertaining to the verification of identity. This information is used to authenticate cardholders. Information includes; card validation codes/values, full magnetic stripe data, or personal identification number (PIN)), appearing in plain-text or otherwise unprotected form.

Server: a muti-user computer, which provides some service for other computer connected to it via a network. The most common examples are department/collegiate file servers, web servers, mail servers and database servers.

VoIP: Voice over Internet Protocol.

VoIP fax: a fax received via the CQUniversity VoIP server to a fax machine or email address.

7 RELATED LEGISLATION AND DOCUMENTS

Information Privacy Act 2009 (Qld)

Information Security Management Policy

Payment Card Industry Data Breach Containment Policy and Procedure

Payment Card Industry Data Security Standard

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cwlth)

Risk Management Policy and Procedure (FMPM)

8 FEEDBACK

8.1 University staff and students may provide feedback about this document by emailing policy@cqu.edu.au.

9 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Council
Advisory Committee to Approval Authority	Audit, Risk and Finance Committee
Administrator	Deputy Vice-Chancellor (Finance and Planning)
Next Review Date	8/11/2021

Approval and Amendment History	Details
Original Approval Authority and Date	Council 29/04/2015
Amendment Authority and Date	Updated titles and template – Deputy Vice-Chancellor (Finance and Planning) 15/03/2017; Administrator Approved – Deputy Vice-Chancellor (Finance and Planning) 8/11/2018.
Notes	