PAYMENT CARD DATA SECURITY POLICY AND PROCEDURE

CONTENTS

1 PURPOSE

1.1 This policy and procedure outlines how CQUniversity will manage company or individual cardholder data provided to CQUniversity for the purposes of making payment to the University.

2 SCOPE

2.1 This policy and procedure apply to:

- CQUniversity as a corporate entity
- Council
- employees, and
- controlled entities.

3 POLICY STATEMENT

3.1 The Payment Card Industry Data Security Standard (PCI DSS) is a set of guidelines to assist merchants in preventing payment card fraud and improve security around processing and storing payment card details. The University must comply with the PCI DSS in order to accept credit card payments. 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.

3.2 The requirements of the PCI DSS, 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.

3.3 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, the University must use, receive, transmit, store and destroy cardholder data in a manner which protects the cardholder data from misuse or unauthorised transactions. The University must comply with all requirements specified in the PCI DSS to maintain compliance.

Build and maintain a secure network

4.2 The University will 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 employees must adhere to the Information and Communications Technology Passwords Procedure.

Protect cardholder data

Receiving payment card information

4.4 Companies and individuals must not provide cardholder data via an email or voice over internet protocol (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 will be emailed or VoIP faxed either internally or externally between employees or customers.

Storing payment card information

4.7 If cardholder data must be retained (i.e. for refund or chargeback purposes), it will be stored in a truncated format - the first six and last four digits of a cardholder number - and will not be kept for longer than six months after the transaction date.

4.8 Cardholder data will not be stored, processed, or transmitted on University computers in any form. 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, and
- 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.

4.9 Cardholder data must not be stored in any customer relationship management, document management or records management system (e.g. Content Manager or StudyLink).

Hard copy payment card information

4.10 Hard copies of customer cardholder data must not be requested, accepted or stored.

Removing/modifying electronic payment card information

4.11 Any untruncated cardholder data identified must be removed by purging or truncation methods in accordance with the PCI DSS. The Digital Services Directorate will liaise with the Finance Directorate in relation to requests to delete data. A Technology and Services Assistance Centre (TaSAC) case must be logged for the appropriate action to be taken.

Card authentication or verification codes

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

Maintain a vulnerability management program

4.13 The University will 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

4.14 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, 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 Australian PCI DSS legislation and standards, and
- 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

4.15 The University must ensure access to cardholder data is restricted by using physical and/or technical control measures.

Securing devices

4.16 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). Confirmation that terminals are regularly checked for evidence of tampering must be declared on the bi-monthly Cash float and EFTPOS terminal audits.

Handling payment card information

4.17 Cashiers must receive appropriate cashiering training which incorporates PCI DSS compliance prior to receiving access to the cashiering or receipting systems. PCI DSS compliance should be clearly documented in training material and operational procedures.

Service providers and third-party vendors

4.18 Service providers and third-party vendors providing payment card related services for the University must be PCI DSS compliant. The Finance Directorate will request appropriate certification from service providers and third party vendors and maintain sufficient records.

Regularly monitor and test networks

4.19 To prevent exploitation of data and systems, the University must regularly monitor and test networks to find and fix vulnerabilities. System components, processes, and custom software will 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

4.20 The University maintains a Cybersecurity Management Policy which is based on the international standard for security management systems (i.e. ISO 27001).

5 RESPONSIBILITIES

Compliance, monitoring and review

5.1 The Chief Operating Officer is responsible for implementing, monitoring, reviewing and ensuring compliance with this policy and procedure.

5.2 The Finance and Digital Services Directorates will ensure full compliance is maintained.

5.3 The University will comply with all guidelines and requirements set by the PCI Security Standards Council. Compliance will be monitored by the Finance and Digital Services Directorates, and the relevant acquiring banking institutions that provide the University 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 the University with the means to accept the abovementioned card payments.

Records management

5.5 Employees must manage records in accordance with the Records Management Policy and Procedure. This includes retaining these records in a recognised University recordkeeping information system.

5.6 University records must be retained for the minimum periods specified in the relevant Retention and Disposal Schedule. Before disposing of any records, approval must be sought from the Records and Privacy Team (email records@cqu.edu.au).

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: personally identifiable data associated with the cardholder. This includes the Primary Account Number (PAN) only, or PAN plus the cardholder name or 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.

VoIP: Voice over Internet Protocol.

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

7 RELATED LEGISLATION AND DOCUMENTS

Cybersecurity Management Policy

Information and Communications Technology Passwords Procedure

Information Privacy Act 2009 (Qld)

Payment Card Industry Data Breach Containment Policy and Procedure

Payment Card Industry Data Security Standard

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

8 FEEDBACK

8.1 Feedback about this document can be emailed to policy@cqu.edu.au.

9 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Council
Delegated Approval Authority	Audit, Risk and Finance Committee
Advisory Committee	N/A
Required Consultation	N/A
Administrator	Chief Operating Officer
Next Review Date	07/06/2024

Approval and Amendment History	Details
Original Approval Authority and Date	Council 29/04/2015
Amendment Authority and Date	Deputy Vice-Chancellor (Finance and Planning) 15/03/2017; Deputy Vice-Chancellor (Finance and Planning) 8/11/2018; Vice-President (Student and Corporate Services) 07/06/2021; Editorial amendment 03/01/2023.
Notes	This document was formerly known as the Payment Card Industry Data Security Standard Policy and Procedure (last approved 08/11/2018).