PAYMENT CARD DATA BREACH POLICY AND PROCEDURE

CONTENTS

1 PURPOSE

1.1 This policy and procedure outlines how CQUniversity will manage payment card (credit or debit) data breaches.

2 SCOPE

2.1 This policy and procedure applies to cardholder data breaches, including those of an accidental or malicious nature, and:

- 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 global set of guidelines to assist merchants in preventing payment card fraud and improve security around processing and storing payment card details. The University must be complaint with the PCI DSS 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 University has an obligation under the *Information Privacy Act 2009* (Qld) to take reasonable steps to protect personal information from misuse, loss or other unauthorised access, use, modification or disclosure. This includes customer's credit and debit card information. The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cwlth) legislates mandatory breach notifications for all data breaches that impact privacy. If a PCI DSS related data breach occurs that impacts privacy the Privacy Policy and Procedure also applies.

3.3 The Chief Operating Officer will take all risks into consideration and consult with expert advisors to swiftly contain the breach, protect credit and debit card data, minimise the financial impact and negative publicity for the University.

3.4 A cardholder data breach will render the University non-compliant with the PCI DSS.

3.5 Non-compliance may 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.

3.6 Failure to notify the card brands of a suspected or confirmed breach will subject the University to additional penalties.

4 PROCEDURE

4.1 Data breaches are not limited to malicious actions, such as theft or hacking, but may also arise from accidental loss or disclosure. Data breaches can be caused or exacerbated by a variety of factors, affecting different types of personal information and give rise to a range of actual or potential harms to individuals, agencies and organisations.

4.2 There is no single way of responding to a data breach. Each breach will need to be dealt with on a case-by-case basis, undertaking an assessment of the risks involved, and using that risk assessment as the basis for deciding what actions to take in the circumstances.

4.3 The major payment card companies have specific and required procedures for providing notification to them in the event of a suspected and/or confirmed unauthorised acquisition of cardholder data.

Report suspected breaches

4.4 Employees working for or on behalf of the University and/or a controlled entity, must report any suspected payment card data breaches to the Chief Operating Officer.

4.5 The Chief Operating Officer will immediately notify Internal Audit who will follow the merchant bank and card brand investigation procedures. Internal Audit will liaise with the Deputy Vice-President (Digital Services) and Deputy Director Financial Accounting and Operations when appropriate.

4.6 The merchant bank and/or the card brands may deem it necessary, that an independent forensic investigation be conducted by a Payment Card Industry Forensic Investigator.

4.7 Internal Audit will document the breach and advise the Chief Operating Officer accordingly.

Incident investigation

4.8 If the University discovers or suspects a credit or debit card data breach, immediate steps will be taken to limit the breach to prevent additional exposure of cardholder data and ensure compliance with the PCI DSS, PCI Payment Application Data Security Standard (PA DSS), and PCI Transaction Security Requirements (PCI PTS).

4.9 Internal Audit will start an incident investigation within 24 hours to determine the:

- type of cardholder data at risk. Data may include:
  - cardholder name
  - cardholder address
  - cardholder primary account number (PAN)
  - card expiration date
  - card validation code/card verification value
  - magnetic stripe (track) data
  - PIN
  - PIN blocks.
- number of cardholder accounts at risk
- incident timeframe for cardholder accounts at risk
- suspected cause of incident.

4.10 The Chief Operating Officer will be provided daily progress updates while the incident is being investigated.

4.11 If it is determined that cardholder data has not been compromised, the Chief Operating Officer will notify the payment card companies (including the merchant bank).

Risk evaluation

4.12 The Chief Operating Officer and the Deputy Vice-President (Digital Services) will manage any risk in accordance with the Risk Management Policy. Specific PCI DSS risk records pertaining to either the Finance Directorate or the Digital Services Directorate may be recorded.

Confirmed security breach

4.13 Within 24 hours of knowledge of a confirmed security breach and knowledge that cardholder data has been compromised, the Chief Operating Officer will notify the relevant entities as necessary.

Police notification

4.14 In cases of unauthorised access, malice or theft the Chief Operating Officer will notify the relevant law authority. The Confirmed Security Breach Contacts Listing should be used for contact information for entities to be notified in the event of a breach

Subsequent notification

4.15 Within three business days of the reported compromise, the Chief Operating Officer will provide an Incident Response Report to:

- MasterCard Merchant Fraud Control
- Visa USA Fraud Investigation and Incident Management Group
- American Express, and/or
- the merchant bank (Commonwealth Bank of Australia).

4.16 Within 10 business days, the Chief Operating Officer will provide compromised PANs to the merchant bank.

Additional requirements

4.17 Depending upon the level of risk and data elements obtained by unauthorised persons, additional requirements are at the sole discretion of the payment card companies and are likely to include:

- an independent forensic investigation and vulnerability scan of the campus network

- weekly written status reports addressing open questions and issues, until the audit is considered to be complete, and
- completion of a PCI DSS Compliance Questionnaire.

PCI response to non-compliance

4.18 If investigation of the incident reveals that the University's non-compliance with the PCI DSS contributed to the account compromise or was negligent in reporting or investigating the loss of cardholder data, fines and penalties may apply.

Prevention

4.19 With the aim to reduce the risk of a similar breach occurring again, the Chief Operating Officer will communicate any required changes to the Deputy Vice-President (Digital Services) for immediate implementation.

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 Responsibilities:

- appoint Internal Audit to follow breach procedures – Chief Operating Officer
- provide information pertaining to electronic or system breach – Deputy Vice-President (Digital Services)
- provide information pertaining to procedural or hard copy breach – Chief Operating Officer
- report suspected payment card breach – all employees
- report payment card breaches to merchant bank, card brands and Police – Chief Operating Officer.

Reporting

5.3 No additional reporting is required.

Records management

5.4 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.

5.5 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

Acquiring bank: the University's primary banking service provider.

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 either the cardholder name or expiration data.

Merchant: for the purpose of the PCI DSS and this policy and procedure, a merchant is defined as any University campus, location, department or entity that accepts payment cards bearing the logos of any of the five members of the PCI Security Standards Council (AMEX, Discover, JCB, MasterCard or VISA), as payment for goods, services rendered, or accepted in the form of a donation.

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

PIN blocks: when a card holder enters their PIN, the information is first encoded into a plain text PIN block, derived from the PIN length, the PIN digits, a portion of the PAN and padding. The plain text PIN block is then encrypted using a standard algorithm.

7 RELATED LEGISLATION AND DOCUMENTS

Data Breach Management

Enterprise Risk Management Framework

Information Privacy Act 2009 (Qld)

MasterCard Safety and Security Merchant Information

Payment Card Industry Data Security Standards:

- PCI Data Security Standard (PCI DSS)
- PCI Payment Application Data Security Standard (PA DSS)
- PCI PIN Transaction Security Requirements (PCI PTS)

Payment Card Data Security Policy and Procedure

PCI Forensic Investigators (PFIs) (from the PCI Security Standards Council)

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

Privacy Policy and Procedure

Risk Management Policy

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	16/11/2024

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; Audit, Risk and Finance Committee 16/11/2021; Editorial amendment 03/01/2023.
Notes	This document was formerly known as the Payment Card Industry Data Breach Containment Policy and Procedure (last approved 08/11/2018).