PAYMENT CARD INDUSTRY DATA BREACH CONTAINMENT POLICY AND PROCEDURE

CONTENTS

1 PURPOSE

1.1 This policy and procedure aims to minimise risk and ensure appropriate action is taken in the event of a payment card (credit or debit) data breach at CQUniversity, by taking control of the situation in an appropriate manner in order to prevent the release of further payment card data. Unreported payment card data breaches may result in additional fines.

1.2 This policy and procedure outlines the process for staff to follow in the event that a customer's credit or debit card data has been compromised.

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.

2.2 This document applies to all cardholder data breaches, including those of an accidental or malicious nature.

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 to improve security around processing and storing payment card details. CQUniversity is required to be complaint 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.

3.2 CQUniversity has an obligation under the *Information Privacy Act 2009* (Qld) to put in place reasonable security safeguards and to take reasonable steps to protect personal information from loss and from unauthorised access, use, modification or disclosure, or other misuse. This includes customer's credit and debit card information.

3.3 The Deputy Vice-Chancellor (Finance and Planning) will take all risks into consideration and consult with expert advisors in order 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 PCI non-compliant.

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 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.

4.4 CQUniversity is required to adhere to the Information Privacy Act and take reasonable steps to protect the personal information from misuse, loss, from unauthorised access, modification or disclosure. The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cwlth) legislates mandatory breach notifications for all data breaches that impact privacy. If a PCI related data breach occurs that impacts privacy the Information Privacy Policy and Procedure also applies.

Report suspected breaches

4.5 All staff working for or on behalf of CQUniversity and or an entity, are charged with the responsibility of reporting any suspected payment card data breaches to the Deputy Vice-Chancellor (Finance and Planning).

4.6 The Deputy Vice-Chancellor (Finance and Planning) will immediately appoint a delegate who will follow all merchant bank and card brand investigation procedures. The delegate will liaise with the Chief Information and Digital Officer and Deputy Director, Financial Accounting and Operations when appropriate.

4.7 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.

4.8 The appointed delegate will accurately document the breach and advise the Deputy Vice-Chancellor (Finance and Planning) accordingly.

Incident investigation

4.9 In the event that CQUniversity discovers or suspects that a credit or debit card data breach has occurred, it should take immediate steps to limit the breach to prevent additional exposure of cardholder data and ensure compliance with the PCIS DSS, PCI Payment Application Data Security Standard (PA DSS), and PCI PIN Transaction Security Requirements (PCI PTS).

.

4.10 The Deputy Vice-Chancellor (Finance and Planning) or delegate shall start an incident investigation within 24 hours to determine the following:

- 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.

4.11 Whilst the incident is being investigated by the appointed delegate, the Chief Information and Digital Officer and Deputy Director, Financial Accounting and Operations will provide daily progress updates to the Deputy Vice-Chancellor (Finance and Planning) via the appointed delegate.

4.12 If it is determined that cardholder data has not been compromised, the Deputy Vice-Chancellor (Finance and Planning) or delegate shall notify the payment card companies (including the merchant bank).

Risk evaluation

4.13 The Deputy Vice-Chancellor (Finance and Planning) or delegate and the Chief Information and Digital Officer will manage the risk in accordance with the Risk Management Policy and Procedure (FMPM). Specific PCI risk records pertaining to either the Finance and Planning Division or the Information and Technology Directorate may be recorded.

Confirmed security breach

4.14 Within 24 hours of knowledge of a confirmed security breach and knowledge that cardholder data has been compromised, the Deputy Vice-Chancellor (Finance and Planning) or delegate shall notify the relevant entities as necessary.

Police notification

4.15 In cases of unauthorised access, malice or theft the Deputy Vice-Chancellor (Finance and Planning) or delegate 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

4.16 Within three business days of the reported compromise, the Deputy Vice-Chancellor (Finance and Planning) or delegate shall:

- Provide an Incident Response Report to one or more of the following:
  - MasterCard Merchant Fraud Control staff

- Visa USA Fraud Investigation and Incident Management Group
- American Express
- The merchant bank (CBA).

4.17 Within 10 business days, the Deputy Vice-Chancellor (Finance and Planning) or delegate shall provide all compromised PANs to the merchant bank.

Additional requirements

4.18 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 the following:

- 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

4.19 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

4.20 With the aim to reduce the risk of a similar breach occurring again, the Deputy Vice-Chancellor (Finance and Planning) will communicate any required changes to the Chief Information and Digital Officer and/or Deputy Director, Financial Accounting and Operations for immediate implementation.

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 Responsibilities:

- appoint a delegate to follow breach procedures – Deputy Vice-Chancellor (Finance and Planning)
- provide all information pertaining to electronic or system breach – Chief Information and Digital Officer
- provide all information pertaining to procedural or hard copy breach – Deputy Vice-Chancellor (Finance and Planning)
- report suspected payment card breach – all staff
- report payment card breaches to merchant bank, card brands and Police – Deputy Vice-Chancellor (Finance and Planning).

Reporting

5.3 No additional reporting is required.

Records management

5.4 All documentation in relation to the breach, containment, risk, prevention measures and follow-up notes must be retained for a period no less than that stipulated by the Queensland State Archives in relation to the General Retention and Disposal Schedule for Administrative Records (GRDS) and in accordance with s.13 of the *Public Records Act 2002* (Qld).

5.5 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

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

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

Cardholder data: all personally identifiable data associated with the cardholder. PAN only or PAN plus either of the following: cardholder name, 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 block format and encryption: when a card holder enters his 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 (primary account number) and padding. The plain text PIN block is then encrypted using a standard algorithm.

7 RELATED LEGISLATION AND DOCUMENTS

Data Breach Management *(available to staff only)*

Information Privacy Act 2009 (Qld)

Information Privacy Policy and Procedure

MasterCard Account Compromise User Guide

MasterCard Safety and Security Merchant Information

Payment Card Industry Data Security Standards:

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

Payment Card Industry Data Security Standard Policy and Procedure

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

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

Public Records Act 2002 (Qld)

Risk Management Policy and Procedure (FMPM)

Visa Inc. Fraud Control and Investigations Procedures

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	