Payment Card Data Security Procedures

1. LEGISLATION/ENTERPRISE AGREEMENT/POLICY SUPPORTED

Best Practice Financial Management Policy

Physical and Information Security Policy

2. PROCEDURAL DETAILS

2.1 Introduction

2.1.1 This procedure deals with situations where a company or individual provides their Payment Card Data to the University for the purposes of making payment to the University.

2.1.2 Under the Payment Card Industry Data Security Standards (PCI DSS), the University is required to use, store and destroy Payment Card Data in a manner which protects the Cardholder Data from misuse or unauthorised transactions. The risks to the University of non-compliance with PCI DSS include significantly increased compliance costs, restitution of fraudulent transaction amounts, fines and other penalties, and adverse impact to public reputation.

2.1.3 Under the *Financial Management Act 2006* (WA), officers of the University may be liable for all or part of any loss suffered by the University due to their deliberate or serious disregard of a reasonable standard of care.

2.1.4 Failure of Staff to comply with these procedures may be regarded as a deliberate or serious breach of their duty of care and may lead to disciplinary action under relevant Enterprise Bargaining Agreements.

2.2 General PCI DSS compliance

2.2.1 Staff, and the Supervisors of such Staff, who:

(a) handle or process Payment Card transactions; or

(b) are in a position where they may monitor or approve such information or requests for such information

must comply with these procedures.

2.2.2 Additionally, the Supervisor of a business area must maintain and comply with the PCI DSS business area work instruction approved by Financial Services or utilise the work instruction located on Financial Services website.

2.2.3 The Manager, Transaction Processing or nominee must:

(a) maintain a University PCI DSS register (which combines business area registers together); and

(b) conduct regular audits of business area PCI DSS registers.

2.3 Payment card data: transmission, storage and destruction

2.3.1 Payment Card Data will not be stored electronically on any University infrastructure. Storage includes any:

(a) database;

(b) electronic file; or

(c) electronic repository of information including portable electronic media devices.

Stored Payment Card Data will be reported to CITS Information Security immediately, who will ensure that the data is removed in accordance with PCI DSS.

2.3.2 Payment Card Data will only be accepted into the University though the University's on-line payment pages, telephone or Dedicated Facsimile.

2.3.3 If Payment Card Data is received in any manner other than as per section 2.3.2, the recipient must immediately:

(a) advise (with the Payment Card Data deleted), that "Curtin University does not accept Payment Card Data other than via the secure Curtin web payment pages or via telephone. Storage of such data will only be undertaken in accordance with Curtin's PCI DSS Procedures"; and

(b) securely destroy any hardcopy or electronic correspondence as per section 2.3.5(c).

2.3.4 Payment Card Data must not be stored in hardcopy form unless authorised in writing by the Chief Financial Officer or approved nominee.

2.3.5 Where Payment Card Data is authorised for hardcopy storage, the business area must:

(a) securely store the data in a locked cabinet or within a locked office;

(b) restrict access to Staff with a business need for such data; and

(c) destroy the data (either the entire form, page, etc. or the section containing the Payment Card Data) as soon as the business need for such storage is no longer relevant, or within six months (whichever is the shorter timeframe) using a secure storage bin or a cross-cut shredder.

2.3.6 Payment Card Data may be accepted over the telephone; however, any data that is written down must be handled as per section 2.3.5 above.

2.3.7 Credit Card Verification (CCV) codes (e.g., CAV2, CVV2, CVC2, CID) must not be stored or recorded under any circumstances once the transaction has been processed.

2.4 Payment card data: processing

2.4.1 Payment Card Data will only be processed using approved University payment processing systems (see Financial Services website).

2.4.2 Only systems approved by the Chief Financial Officer or approved delegate may be used to process Payment Card transactions.

2.5 Staff access and training

2.5.1 Only relevant Staff (as specified in their role's position description) will be permitted access to Cardholder Data.

2.5.2 Staff and Supervisors listed on the University's PCI DSS register must undergo annual training and examination in PCI DSS.

2.5.3 Staff who fail to successfully complete the assessment must:

(a) successfully complete the assessment within one month; or

(b) be removed from any position where they are required to handle Payment Card Data, including telephone assistance positions.

2.6 Service providers and third party vendors

2.6.1 The Chief Financial Officer or approved nominee must ensure that service providers and third party vendors are in compliance with PCI DSS.

3. RESPONSIBILITIES

In addition to the responsibilities set out in section 2,

3.1 The Manager, Transaction Processing or nominee will ensure that random audits are conducted at least once per financial year for all University business areas in order to verify compliance with these procedures.

4. SCOPE OF PROCEDURES

These procedures apply to all Staff.

5. DEFINITIONS

(Note: Commonly defined terms are located in the Curtin Common Definitions. Any defined terms below are specific to this document)

Cardholder Data
Personal Account Number (PAN) only or PAN plus any of the following: Cardholder name, Expiration date.

Credit Card Verification (CCV) codes
These are the 3-digit number on the signature panel on the Visa or MasterCard or the 4-digit number on the front of the Amex Card (above the logo). These are referred to accordingly:

- CAV2: Card Authentication Value (JCB) on signature panel
- CVC2: Card Verification Code (MasterCard) on signature panel
- CVV2: Card Verification (Visa) on signature panel
- CID: Card Identification number (American Express) above logo on front of card.

Dedicated Facsimile
Standalone fax machine with single dedicated telephone line connection.

Payment Card
Any credit or debit card that bears the logo of Visa, MasterCard, American Express, Discover, or JCB.

Payment Card Data
Any data contained on a Payment Card that may be 'stored, processed or transmitted' in any form, whether hardcopy or electronic. Note: If the PAN is not 'stored, processed or transmitted' then PCI DSS does not apply.

Payment Card Industry (PCI)
The Payment Card Industry operates through a body known as the PCI Security Standards Council. This Council comprises the following credit card service suppliers: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

Payment Card Industry Data Security Standards (PCI DSS)
A set of security standards promulgated by the payment card industry so that merchants have a single set of Cardholder Data Security Standards against which to measure the security of the infrastructure, systems and processes used to process card transactions with respect to sensitive credit Cardholder Data such as card number, card security number, etc.

Staff
For the purposes of these procedures, this term encompasses all forms of employee status, including contractors, involved in supervising or processing payment card transactions through any of the University's approved payment systems, or both.

Supervisor
For the purposes of this procedure, Supervisor can mean manager, team-leader or other title for the person assuming direct Supervisory responsibility for Staff involved in processing Payment Card transactions through any of the University's approved payment systems.

6. SCHEDULES

Nil

7. RELATED DOCUMENTS/LINKS/FORMS

Money Handling Procedures

Financial Services Website

Payment Card Industry Data Security Standards

CITS Information Security

Policy Compliance Officer	Philip Thomas, Director, Financial Operations and Strategic Procurement | Financial Services
Policy Manager	Chief Financial Officer
Approval Authority	Chief Financial Officer
Review Date	1st April 2017

REVISION HISTORY

Version	Approved/ Amended/ Rescinded	Date	Committee / Board / Executive Manager	Approval / Resolution Number	Key Changes and Notes
New	Approved	11/09/2013	Chief Financial Officer	EM1323	Unconditional
	Amended	06/12/2013	Chief Financial Officer	EM1326	Unconditional