PAYMENT CARD INDUSTRY DATA SECURITY POLICY 2019

The Vice-Principal, Operations, as delegate of the Senate of the University of Sydney, adopts the following policy.

Dated: 31 July 2019

Last amended:

Signature:

Position: Vice-Principal, Operations

CONTENTS

1 Name of policy

This is the Payment Card Industry Data Security Policy 2019.

2 Commencement

This policy commences on 1 August 2019.

3 Policy is binding

Except to the extent that a contrary intention is expressed, this policy binds the University, staff, students and affiliates.

4 Statement of intent

This policy:

(a) establishes the principles upon which the University manages cardholder data security; and

(b) requires the University's payment card activities to be managed in a manner which enhances cardholder data security.

5 Application

This policy applies to:

(a) all staff and affiliates; and

(b) storing, processing or transmitting cardholder data or sensitive authentication data.

6 Definitions

cardholder data	means the data found on the front and back of a credit or debit payment card, other than a University corporate card, which includes: • Primary Account Number: the card number which can be up to 16 digits; • Cardholder's name; • Expiration date (month/year); and • Security number or CCV: a 3- or 4-digit number usually on the back of the card.
ICT asset	has the meaning given in the *Cyber Security Policy 2019*. At the date of this policy this is: means University owned or connected hardware, software, cloud-based services, communication devices, and network.
ICT network	means a digital telecommunications network between network devices that allows ICT assets to communicate.
merchant bank facility	means a banking facility that enables payments to be accepted by debit payment card, credit payment card or electronic funds transfer point of sale (EFTPOS).
network device	means any ICT asset that provides a technology function within a telecommunications network, including but not limited to firewalls, switches, routers, wireless access points, network appliances and other security appliances.
PCI DSS	means *Payment Card Industry Data Security Standard* which is an international standard mandated by major payment card brands to identify and protect payment card data.
sensitive authentication	means data used by the issuers of cards to authorise card transactions including, but not limited to, security validation codes (e.g., 3- or 4-digit number printed on cards), magnetic-stripe data,

data	Personal Identification Numbers (PINs), and chip and contactless card data.
SMS	means short message service, a text messaging service component of most telephone, internet and mobile device systems.
University's bank	means the bank with which the University holds a merchant account.
University corporate card	has the meaning set out in the *Corporate Card Procedures*. At the date of this policy, this is: means a University corporate credit card. **Note:** Information related to a University corporate card must be held securely, consistently with the *Cyber Security Policy 2019* and associated procedures and technical standards.

7 General principles

(1) The University is a merchant and must comply with the *Payment Card Industry Data Security Standard* (PCI DSS) which specifies 12 requirements for managing credit card information.

(2) The requirements of the PDI DSS are summarised in Table 1.

Table 1:

Build and maintain a secure network and systems	1	Install and maintain a firewall configuration to protect cardholder data
	2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3	Protect stored cardholder data
	4	Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5	Protect all systems against malware and regularly update anti-virus software or programs
	6	Develop and maintain secure systems and applications
Implement strong access control measures	7	Restrict access to cardholder data by business need to know
	8	Identify and authenticate access to system components
	9	Restrict physical access to cardholder data
Regularly monitor and test networks	10	Track and monitor all access to network resources and cardholder data
	11	Regularly test security systems and processes
Maintain an information security policy	12	Maintain a policy that addresses information security for all personnel

8 PCI DSS compliance

(1) Staff and affiliates must handle all cardholder data in a manner consistent with PCI DSS and this policy.

(a) Non-compliance with the PCI DSS is outside the University's risk tolerance.

(b) The Treasurer, FCT must assess compliance with the PCI DSS annually and report to the University's bank.

(2) Staff and affiliates must not store, process or transmit cardholder data within ICT assets connected to any University owned or managed ICT network.

(a) Card-based transactions must be stored, processed or transmitted using PCI DSS compliant:

(i) networks and systems owned and operated by third party providers;

(ii) interactive voice response services operated by third party providers;

(iii) card equipment isolated from the University's ICT networks (e.g. standalone);

(iv) ICT assets isolated from the University's ICT networks (e.g. standalone); or

(v) mobile telephones used to receive voice cardholder data.

(3) Staff and affiliates must not:

(a) send or receive cardholder data by email, instant messaging, SMS or any other ICT service;

(b) store sensitive authentication data in any form, after authorisation of a card transaction; or

Note: Storage includes paper, photocopy, spreadsheet, scanned copy and email.

(c) specifically, direct students to University provided workstations to use University e-commerce payment channels.

(i) Using University ICT resources to make a payment to the University is not mandated, and if it occurs must be the student's choice.

(4) No one must be able to view a full primary account number unless:

(a) there is a legitimate business reason for them to do so; and

(b) written approval has been given by the Director, Financial Control and Treasury.

9 Roles and responsibilities

(1) **Financial Control and Treasury** is responsible for:

(a) maintaining a list of all ICT assets that store, process or transmit cardholder data, including the University personnel who manage the assets;

(b) managing third party service providers with whom cardholder data is shared or which could affect the security of the University's cardholder data, including;

(i) maintaining a list of service providers and the cardholder data related services that are provided;

(ii) establishing written agreements between the University and each applicable service provider, which assign responsibility for the security of cardholder data; and

(iii) verifying the PCI DSS compliance status of each service provider at least annually.

(c) managing merchant bank facilities and implementing card payment processes that comply with PCI DSS;

(d) permitting only personnel with a business need to have access to third party systems and standalone University ICT assets used to store, process or transmit cardholder data;

(e) training relevant personnel to be aware of suspicious behaviour and to report tampering or substitution of devices to Campus Security; and

(f) reporting of any breach of PCI DSS to the University's bank.

(2) **The Information and Communications Technology unit** is responsible for:

(a) University cyber security, as specified in the relevant policy, procedures and technical standards; and

(b) configuring and maintaining standalone ICT assets used for processing cardholder data consistent with the PCI DSS.

(3) **Campus Infrastructure and Services** is responsible for providing physical security for:

(a) ICT assets used for processing cardholder data.

NOTES

Payment Card Industry Data Security Policy 2019

Date adopted:	31 July 2019
Date registered:	12 August 2019
Date commenced:	1 August 2019
Administrator:	Jointly Chief Financial Officer and Chief Information Officer
Review date:	2 August 2024
Related documents:	Payment Card Industry Data Security Standard
	Cyber Security Policy 2019
	Acceptable Use of ICT Resources Policy 2019
	Recordkeeping Policy 2017
	Cyber Security Procedures 2019

AMENDMENT HISTORY

Provision	Amendment	Commencing