University of Sunderland – Business Assurance

PCI Security Policy

Document Classification: **Public**

Policy Reference – Central Register	IG008_____
Policy Reference – Faculty / Service	**IG 008**
Policy Owner	**Interim Director of Finance**
Date Policy Written	**March 2015**
Date Policy Last Updated	
Author	**Assurance Manager, Business Assurance**
Date to Information Governance Group	**12th March 2015**
Date to Executive	
Date for next Review	**December 2016**
Comments	

1. Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard defined and published by the Payment Card Industry Security Standards Council. The standard was created to help payment card industry organisations that process card payments prevent payment card fraud through increased controls around data and its exposure to compromise. The standard applies to all organisations that hold, process, or exchange cardholder information. Enforcement of compliance is done by the organisation's card provider. Organisations that fail to meet the compliance requirement risk losing their ability to process payment card payments and being audited and/or fined.

2. Purpose and Scope

This policy sets out the requirements which are necessary to protect the security of all credit and debit card payments received and processed by the University which are governed by the Payment Card Industry Data Security Standard (PCI-DSS). Compliance with PCI-DSS is mandatory for any company or organisation which stores, processes, or transmits payment cardholder data. Failure to comply with these requirements could result in the University being fined and no longer permitted to process card payments.

The University is a 'Level 4 Merchant' which means that certification to the Standard requires the completion of an annual self-assessment questionnaire (SAQ) to demonstrate compliance against a subset of the prescriptive controls set out within the standard. The University's CDE requires completion of a SAQ C.

3. Definitions

Payment card :	A card backed by an account holding funds belonging to the cardholder, or offering credit to the cardholder such as a debit or credit card.
PCI DSS:	Payment Card Industry Data Security Standard
Stripe / track data:	Information stored in the magnetic strip or chip on a payment card.
PAN:	"Primary Account Number" is a 14 or 16 digit number embossed on a debit or credit card and encoded in the card's magnetic strip which identifies the issuer of the card and the account.
PIN:	A "Personal Identification Number" is a secret numeric password used to authenticate payment cards.
CAV2/CVC2/CVV2/CID	3-digit security code displayed on payment cards
Cardholder Data	Payment card data including: Primary Account Number (PAN), name of cardholder, expiration date and service code.
Sensitive Authentication Data	Full magnetic stripe data or equivalent on a chip, CAV2/CVC2/CVV2/CID or PINs/PIN blocks
Cardholder Data Environment (CDE)	Privacy Impact Assessment is usefully defined as a process whereby a project's potential privacy issues and risks are identified and examined from the perspectives of all stakeholders, and a search is undertaken for ways to avoid or minimise privacy concerns.
PDQ Machine	A credit card swipe machine.
PED	PIN Entry Device.
Qualified Security Assessor (QSA)	A person who has been certified by the PCI Security Standards Council to audit merchants for Payment Card Industry Data Security Standard

	(PCI DSS) compliance.
SAQ	Self-Assessment Questionnaire
Acquirer	Also referred to as "merchant bank," "acquiring bank," or "acquiring financial institution." Entity that initiates and maintains relationships with merchants for the acceptance of payment cards.
Level 4 Merchant	Merchants processing fewer than 20,000 Visa or MasterCard eCommerce transactions annually and all other merchants processing up to one million Visa or MasterCard transactions annually.

4. Roles and Responsibilities

All individual employees and contractors have responsibility for ensuring that they comply with this policy and any related policies and guidance. Staff should attend training and awareness sessions provided by the University. Employees also have a duty to report any incidents or 'near misses' in relation to information security.

The University has identified the following roles specific to the security of PCI data:-

Role	Responsibility
Chief Financial and Assurance Officer	• Owner of this document and responsible for the implementation of the policy. Responsible for the signing of the SAQ.
Senior Information Risk Owner (SIRO) **Director of Business Assurance**	• ensuring that an overall culture exists that values and protects information within the University • owning the University's overall information risk policy and risk assessment process, testing its outcome and ensuring that it is used • owning the University's information incident management framework
Assurance Manager (Business Assurance - Information Governance)	• drawing up information governance policy, process and guidance and ensuring compliance with this policy • overseeing the Information Governance Framework and ensure its successful operation
IT Security Manager (ITS)	• developing IT Security Policy, standards and guidelines • ensuring that effective IT Security systems, controls and standards are in place. • arranging and assessing the results of the external internal network security scans for PCI Compliance.
Revenues Officer	• managing the financial aspects in relation to PCI compliance across the University. May remove any payment card processing activity causing unacceptable risk. • developing and delivering training for staff involved in card payment processing, ensuring they are aware of cardholder data security and the statements contained within this policy. • maintaining a list of all University payment card service providers and ensuring their PCI-DSS compliance status is monitored.

5. Policy Detail

Policy Undertaking	
Req.	**Requirement 1 – Install and maintain a firewall configuration to protect cardholder data**
1.2	Firewall and router configurations shall restrict connections between un-trusted networks and any system components in the CDE.
1.2.1	Inbound and outbound traffic shall to be restricted to that which is necessary for the CDE.
1.2.3	Perimeter firewalls must be installed between any wireless networks and the CDE, and configured to deny or control (as applicable) any traffic from the wireless environment into the CDE.
1.3	Direct public access between the Internet and any system component in the CDE is prohibited.
1.3.1	A DMZ must be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.
1.3.3	Direct connections inbound or outbound for traffic between the Internet and the CDE is not allowed.
1.3.5	Unauthorized outbound traffic from the CDE to the Internet is not allowed.
1.3.6	Stateful inspection (dynamic packet filtering) must be implemented.
Req.	**Requirement 2 - Do not use vendor-supplied defaults for system passwords and other security parameters**
2.1	Vendor-supplied defaults must be changed before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.
2.1.1	The wireless vendor defaults for wireless environments connected to the CDE must be changed before connectivity, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.
2.2.2	Only necessary and secure services, protocols and daemons as required for the function of the system are to be enabled.
2.3	All non-console administrative access must be encrypted using strong cryptography. Technologies such as SSH, VPN, or SSL/TLS must be used for web-based management and other non-console administrative access.
Req.	**Requirement 3 - Protect stored cardholder data**
3.3	The Primary Account Number (PAN) will be masked when displayed.
Req.	**Requirement 4 - Encrypt transmission of cardholder data across open, public networks**
4.1	Strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH) must be used

	to safeguard sensitive cardholder data during transmission over open, public networks.
4.1.1	Wireless networks transmitting cardholder data or connected to the CDE, must use industry best practices to implement strong encryption for authentication and transmission.
4.2	PANs must not be sent by unprotected end-user messaging.
Req.	**Requirement 5 - Use and regularly update anti-virus software or programs**
5.1	Anti-virus software must be deployed on all systems commonly affected by malicious software.
5.1.1	Ensure that all utilised anti-virus programs used are capable of detecting, removing, and protecting against known types of malicious software.
5.2	All anti-virus mechanisms must be current, actively running, and generating audit logs.
Req.	**Requirement 6 - Develop and maintain secure systems and applications**
6.1	All system components and software are to be protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Critical security patches must be installed within one month of release.
Req.	**Requirement 7 - Restrict access to cardholder data by business need to know**
7.1	Access to system components and cardholder data must be limited to only those individuals whose job requires such access. Access limitations must include the following:
7.1.1	Access rights to privileged user IDs will be restricted to the least privileges necessary to perform job responsibilities.
7.1.2	Assignment of privileges must be based on individual personnel's job classification and function.
Req.	**Requirement 8 - Assign a unique ID to each person with computer access**
8.3	Where applicable, two-factor authentication will be used for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication).
8.5.6	Accounts used by vendors for remote access must only be enabled when needed and must be monitored when in use.
Req.	**Requirement 9 - Restrict physical access to cardholder data**
9.6	All cardholder data must be physically secure.
9.7	Strict control is to be maintained over the internal and external distribution of any kind of media.
9.7.1	Media must be classified so the sensitivity of the data can be determined.
9.7.2	The media must be sent by secure courier or by another delivery method that can be accurately tracked.
9.8	Management must approve any and all media that is moved from a secured area.
9.9	Strict control must be maintained over the storage and accessibility of media.
9.10	All media must be destroyed when it is no longer needed for business or legal reasons as follows:
9.10.1	Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.
Req.	**Requirement 10 - Track and monitor all access to network resources and cardholder data**

10.1	Audit controls must be implemented to track access to cardholder data.
10.5	Audit trails must be secured to prevent unauthorised modification.
10.5	Audit logs and security events must be monitored on a daily basis
Req.	**Requirement 11 - Regularly test security systems and processes**
11.1	Tests are to be undertaken on a quarterly basis for the presence of wireless access points and to detect any unauthorized wireless access points.
11.2	Both internal and external network vulnerability scans must be performed at least quarterly and after any significant change to systems which form part of the CDE or which support payment card transactions.
11.2.1	Perform quarterly internal vulnerability scans.
11.2.2	Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).
11.2.3	Perform internal and external scans after any significant change.
Req.	**Requirement 12 - Maintain a policy that addresses information security for all personnel**
12.1	The University's PCI-DSS Security Policy shall accomplish the following:
12.1.1	Addresses all applicable PCI DSS requirements.
12.1.3	Include a review at least annually and updates when the environment changes.
12.2	Daily operational security procedures must comply with Information Security Policy.
12.3	Usage policies for critical technologies, which define proper use of these technologies, have been developed which:
12.3.1	Require explicit approval by authorised parties.
12.3.2	Stipulate authentication requirements for use of the technology.
12.3.3	List of all such devices and personnel with access.
12.3.5	Define acceptable uses of the technology.
12.3.6	Define acceptable network locations for the technologies.
12.3.8	Automatic disconnect sessions for remote-access technologies after a specific period of inactivity.
12.4	Information security responsibilities for all personnel are clearly defined within the security policy and procedures.
12.5	The following information security management responsibilities are to be assigned to an individual or team:
12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
12.6	A formal security awareness program which is designed to make all personnel aware of the importance of cardholder data security has been implemented.

12.6.1	Personnel are required to undertake security awareness training upon hire and at least annually.
12.6.2	That there is an established process for engaging service providers including proper due diligence prior to engagement.

6. Training and Education

Information is the lifeblood of the University. It is essential that a culture is developed whereby information management is part of everyday activities and becomes part of the culture of the organisation. Increasing staff awareness is key to successfully implementing a University-wide approach to Information Governance. Training and awareness will be available to all staff:

Induction

All newly employed staff will receive basic guidance in organisational policy in relation to information governance as part of the University's induction.

Information Governance Training

All staff will receive basic Information Governance training, at least 3 yearly. Additionally service specific and subject specific training will be provided as appropriate and necessary to inform staff of policy and process.

PCI Specific Training

In addition to the standard training outlined aboveFollowing the conduct of a training needs analysis, specific training will be provided to relevant staff in policies and procedures for:-

- PCI Data Security Standards
- IT and information security
- Cash Handling

Training will be deployed using a variety of techniques including:-

- e-learning
- face to face training sessions
- facilitated workshops

7. Related Policies

This policy should be read in conjunction with the policies listed in Appendix A of the Overarching Information Governance Policy.