# C:\Users\garryrob\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\ICRV480M\UoE_Horizontal Logo_CMYK (2).JPG

# **Payment Card Industry Data Security Standards - Compliance Plan - V3.2**

Policy: PCIDSS-002 v3.2

**Change Control:**  
Change control added  
Policy Version added  
Document Owner updated from Garry Robertson to John Bannaghan  
Last Review Date added  
References to Virtual Terminal updated (no longer used)  
Date added for Document compliance of Internal Systems and processes   
Date added for Complete Self-Assessment SAQ A and record compliance with merchant services.  
Date added for Complete Self-Assessment SAQ B and record compliance with merchant services.  
Reference to PCI-DSS Compliance Plan – SAQ P2PE added

Document Owner – John Bannaghan Systems Accounting Section.

Last Review Date 28/4/2017

## Overview

We have engaged a QSA to assess our current situation and make recommendations on the way forward. This involved a 2 day onsite review and gap-analysis, providing guidance to establish a baseline level of compliance and to address any areas of non-compliance.

The recommendation is to split our compliance reporting by payment channel:

1. Web payments using sites hosted by WPM
2. Face-to-face payments using Verifone or Ingenico stand alone terminals
3. Virtual Terminal payments using Global Blue / SagePay / Realex (no longer used)

**Option 1: Web payments using sites hosted by WPM.**

Ensure all web payment processes are outsourced, and subject to SAQ A.

**Option 2: Face-to-face payments using Verifone or Ingenico standalone terminals (PDQs).**

Maintain PDQs for face-to-face payments, and telephone payments where possible, and to record compliance of these against SAQ-B.

To maintain simplicity for this solution, avoid deploying PDQs which connect to networks, or which connect directly to PCs – these need more complex requirements.

Achieving these solutions will eliminate all internal servers, virtual hosts, non-payment terminals and other systems from scope.

In addition, there will be reduced physical security and policy requirements to meet, avoiding the need for significant changes to the University network environment.

**Option 3: Virtual Terminal payments using Global Blue / SagePay / Realex.** (no longer used)

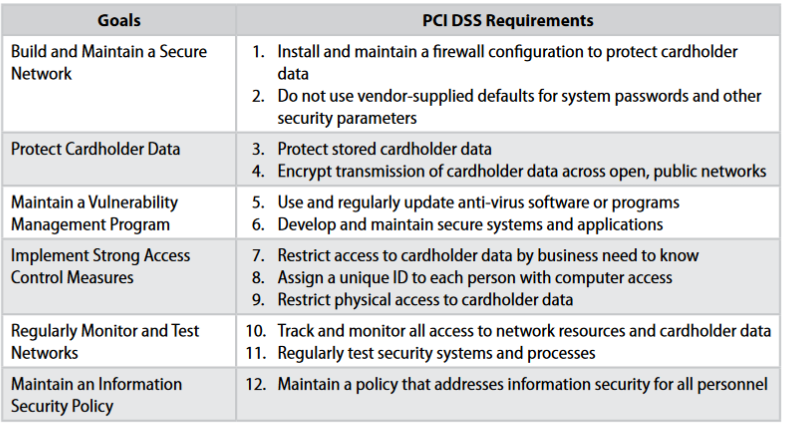
~~Review procedures to move from Virtual terminals to PDQ’s where possible. Create dedicated sub nets for payment-processing terminals.~~

~~Compliance can be recorded for this solution in SAQ-C-VT.~~

~~Much of the work is likely to involve documenting processes, ensuring procedures and policies are in place and communicated, along with network scans and network security issues.~~

## PCI-DSS Goals and Requirements

The 12 requirements of PCI DSS are listed below:



## PCI-DSS Compliance Plan

|  |  |  |
| --- | --- | --- |
| **Target Date** | **Completed Date GR** | **Task** |
| 23/01/2015 | 23/02/2015 | **Create a website for guidance and information**  Add pages to the Finance Department Website to explain the purpose and scope of PCI DSS, the University’s approach to compliance and important information that departments need to be aware of. |
| 19/12/2014 | 19/12/2014 | **Liaise with Merchant Services**  Contact World Pay to clarify tasks necessary to compliance and inform them of our progress toward compliance. |
| 27/02/2015 | 10/07/2015 | **Document all card processing systems**  Produce a list of all physical credit card terminals, and online applications that process card payments. This information should be available through the Wiki and include the type of customer interaction, e.g.   * Cardholder present * Cardholder not present * eCommerce   This will enable us to assess the risks presented by these different processes and create suitable guidance and controls. |
| 30/01/2015 | 03/04/2015 | **Communicate with Stakeholders**  Identify all relevant areas. E-mail heads of departments and communicate with staff involved in processing card payments. |
| 23/01/2015 | 23/01/2015 | **Draft PCIDSS Compliance Policy**  This policy will be based on the card processing systems used at the University, communication with Streamline and the requirements of PCI-DSS.  It is worth noting that IS have produced an information security policy (see <http://www.ed.ac.uk/schools-departments/information-services/about/policies-and-regulations/security-policies/security-policy>)  However, this policy is quite general and makes no reference to PCI-DSS. PCI-DSS requires that merchants have a policy addressing PCI-DSS. It may be best to extend the existing IS policy with PCI-DSS specific sections, and to liaise with IS at an early stage. |
| 30/01/2015 | 20/02/2015 | **Finalise PCIDSS Compliance Policy**  The Information Security Policy should be completed and approved. |
| 30/01/2015 | 31/07/2015 | **Prepare guidance for departments handling card data**  This will be based on the finalised Information Security policy.  Guidance will be made available through the web/wiki.  Guidance will probably be organised based on the type of cardholder interaction, e.g. cardholder present, over the phone transactions, eCommerce etc. |
| 14/05/2015 | 14/05/2015 | **Offer face-to-face guidance sessions**  Departments involved in card processing may find it beneficial to attend face-to-face information and guidance sessions to explain the intent of PCI-DSS, how we are working toward compliance and how they will be affected. |
| 14/05/2015 | 31/07/2015 | **Visit departments, suggest changes and document processes**  Visit all departments that handle card payments in order to ensure that the correct procedures and guidance are understood and to check:   * Access control * Physical access to data   We would also want record the number of staff involved in card processing and the turnover of staff in order to assess the requirement for training, and how frequently this should be delivered.  We would probably want to take a risk based approach and ensure that areas handling the greatest volume of transactions are assessed first.  PCI have guidance and information on using a prioritised approach which may be useful in organising the work to be done at this stage. |
| 30/04/2015 | 15/3/2017 | **Document compliance of Internal Systems and processes**  Liaise with IS to ensure that any cardholder data transmitted across university networks is done in a manner compliant with PCI DSS.  This work is likely to be minimal due to the lack of University information systems that handle cardholder data. |
| 30/04/2015 | 31/07/2015 | **Document compliance of External Systems and processes**  The third parties that we work with, e.g. WPM, WorldPay etc should all be PCI DSS compliant. We will need to get document confirmation from these companies that this is the case. Procedure to review this every year. |

## PCI-DSS Compliance Plan - SAQ A For Web Payment Processes

|  |  |  |
| --- | --- | --- |
| 14/05/2015 | 20/02/2015 | Requirement 9 - Restrict physical access to cardholder data:  Cardholder data should not be held in relation to WPM payments. Review policies and procedures to ensure this is included. |
| 20/03/2015 | 31/07/2015 | Requirement 12 – Maintain an Information Security Policy:  Review policies and procedures  12.8.1 – Maintain a list of service providers, observe agreements.  12.8.2 – Maintain a written agreement with service providers acknowledging their responsibility for the security of cardholder data.  12.8.3 – List the established process for engaging service providers including due diligence prior to engagement.  12.8.4 – Maintain a program to monitor service providers PCI DSS compliance status annually.  12.8.5 – Maintain details about which PCI DSS requirements are managed by each service provider and which by the entity. |
| 31/07/2015 | 30/06/2017 | Complete Self-Assessment SAQ A and record compliance with merchant services. |

## PCI-DSS Compliance Plan - SAQ B For PDQ Dial Out Terminals

|  |  |  |
| --- | --- | --- |
| 14/05/2015 | 31/07/2015 | Requirement 3 – Protect cardholder data:  3.2 - Is sensitive data deleted after authorisation:- Review policies and procedures and examine deletion processes.  3.2.1 – Magnetic strip data is not stored – Examine data sources if applicable.  3.2.2 – Card Verification code is not stored – Examine data sources if applicable.  3.2.3 – PIN is not stored - Examine data sources if applicable  3.3 – Is PAN masked? only personnel with a legitimate business need can see the full PAN. – Review policies and procedures, review roles. |
| 27/04/2015 | 31/07/2015 | Requirement 4 – Encrypt transmitted cardholder data across open public networks.  4.2 – Are policies in place that state that unprotected PAN’s are not to be sent via end-user messaging technologies. - Review policies and procedures |
| 27/04/2015 | 31/07/2015 | Requirement 7 – Restrict access to cardholder data. Access to system components and cardholder data limited to those individuals whose jobs require access.  7.1.2 – Access to privileged User ID’s restricted to least privileges necessary and to roles specifically requiring that access. – Review written access control policy, interview management, review privileged user ID’s.  7.1.3 – Access assigned based on job classification and function. As above. |
| 27/04/2015 | 31/07/2015 | Requirement 9 - Restrict physical access to cardholder data:  9.5 – Are all media (electronic and paper) physically secured – Review policies and procedures and interview personnel.  9.6 – Is strict control maintained over the internal or external distribution of any media – Review policies and procedures.  9.6.1 – Is media classified so the sensitivity of the data can be determined – Review policies and procedures.  9.6.2 – Is media sent by secured courier or other delivery method that can be tracked – Review media distribution documentation.  9.6.3 – Is management approval obtained prior to moving media - Review media distribution documentation.  9.7 – Is strict control maintained over the storage and accessibility of media – Review policies and procedures.  9.8 – Is all media destroyed when it is no longer needed for business or legal reasons – Review media destruction policies and procedures.  9.8.1 – Are hardcopy materials cross-cut shredded, incinerated or pulped – Review policy and procedures, interview personnel, observe processes.  9.8.1b – Are storage containers secured to prevent access - Review policy and procedures, interview personnel, observe processes.  9.9 – Are devices to capture card details protected against tampering and substitution. Maintain a list of such devices, periodically inspect to look for tampering or substitution, train personnel to be aware of suspicious behaviours and tampering/substitution. – Review policy and procedures.  9.9.1 – List of devices should include, Make, Model, Serial Number, Location. – Maintain a list of devices up to date and accurate. Include in policies and procedures.  9.9.2 – Device surfaces periodically inspected to detect tampering – Policy and procedures. Interview.  9.9.3 – Training materials for point of sale staff to verify identity of third parties claiming to repair or replace. Only install/replace/return devices with verification. Report suspicious behaviour or suspected tampering. - Review training materials and policy and procedures. Ensure POS staff are aware and have had training. |
| 27/04/2015 | 27/04/2015 | Requirement 12 – Maintain an Information Security Policy:  Review policies and procedures  12.1 – Is a security policy established, published, maintained and disseminated to all relevant personnel – Review the information security policy  12.1.1 – Is the security policy reviewed annually and updated when the environment changes – review the policy and interview responsible personnel.  12.3 – Are usage policies for critical technologies (remote access, wireless, laptops, tablets, removable electronic data, email usage, internet usage) developed to define proper use  12.3.1 – Explicit approval by authorised parties to use the technologies – Review usage policies, interview responsible personnel.  12.3.3 – A list of all such devices and personnel with access - Review usage policies, interview responsible personnel.  12.3.5 – Acceptable uses of the technologies - Review usage policies, interview responsible personnel.  12.4 – Do security policy and procedures clearly define information security responsibilities for all personnel - Review usage policies, interview responsible personnel.  12.5 – Are the following information security management responsibilities formally assigned to an individual or team  12.5.3 – Establishing, documenting and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations - Review usage policies and procedures.  12.6 – Is a formal security awareness program in place to make all personnel aware of the importance of cardholder security. – Review security awareness program.  12.8 – Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data as follows  12.8.1 – Maintain a list of service providers, observe agreements.  12.8.2 – Maintain a written agreement with service providers acknowledging their responsibility for the security of cardholder data.  12.8.3 – List the established process for engaging service providers including due diligence prior to engagement.  12.8.4 – Maintain a program to monitor service providers PCI DSS compliance status annually.  12.8.5 – Maintain details about which PCI DSS requirements are managed by each service provider and which by the entity.  12.10.1 – Has an incident response plan been created to be implemented in the event of system breach – Review incident response plan and procedures. |
| 27/04/2014 | 30/06/2017 | Complete Self-Assessment SAQ B and record compliance with merchant services. |

## PCI-DSS Compliance Plan – SAQ P2PE

Investigations have identified P2PE devices may be in use in Accommodation Services (ACE). If so we may need to complete this SAQ.

## PCI-DSS Compliance Plan - SAQ-C\_VT for Virtual Terminals (no longer in use)

|  |  |  |
| --- | --- | --- |
| ~~27/05/2015~~ |  | ~~Review procedures to move from Virtual terminals to PDQ’s.~~ |
| ~~27/05/2015~~ |  | ~~Publish policy on Virtual terminals.~~ |
| ~~27/05/2015?~~ |  | ~~\*Replace virtual terminals with PDQ’s?~~ |
| ~~27/05/2015?~~ |  | ~~\*Semafone/Keyivr to allow caller to key their card details to 3~~~~rd~~ ~~party?~~ |
| ~~31/05/2015?~~ |  | ~~\*IS work to create dedicated sub nets for payment processing terminals?~~ |
| ~~31/05/2015~~ |  | ~~Network scanning.~~ |
| ~~31/05/2015~~ |  | ~~Resolve any network security issues.~~ |
| ~~31/05~~  ~~/2015~~ |  | ~~Complete Self-Assessment SAQ-C-VT and record compliance with merchant services.~~ |
|  |  |  |
| ~~30/09/2015~~ |  | ~~WorldPay date for UoE compliance.~~ |