1. Introduction

1.1. This document supports implementation of the "Payment Card Industry Data Security Standard (PCI DSS) compliance" policy referred to in policy document Compliance Policy (ISP-S3).

1.2. 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.

1.3. 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 - The “Payment Card Industry Data Security Standard” (see above).
- Stripe / track data - Information stored in the magnetic strip or chip on a payment card.
- PAN - A “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) - Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.
- PDQ Machine – A credit card swipe machine.
- PED – PIN Entry Device.
• Internal Security Assessor (ISA) – A person who has been certified by the PCI Security Standards Council to audit merchant they are employed by for Payment Card Industry Data Security Standard (PCI DSS) compliance

• 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.

1.4. This document includes statements on:

• Scope
• PCI DSS outline
• PCI DSS compliance policy
• Authorisation and responsibilities
• Payment card processing
• Electronic cardholder data handling
• Paper cardholder data handling
• Retention of cardholder data
• Physical security of payment card processing equipment

2. Scope

2.1. Policy statements in this document apply to:

• All staff involved in payment card processing
• All payment card processing arrangements across the University
• Both manual and IT-based payment card processing

3. PCI DSS outline

3.1. The Payment Card Industry Data Security Standard (PCI DSS) sets out an extensive and detailed list of requirements and security assessment procedures. The goals and requirements of the standard (currently v3.1) are summarised as:

• Build and Maintain a Secure Network
  o Requirement 1: Install and maintain a firewall configuration to protect cardholder data
  o Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

• Protect Cardholder Data
  o Requirement 3: Protect stored cardholder data
  o Requirement 4: Encrypt transmission of cardholder data across open, public networks

• Maintain a Vulnerability Management Program
  o Requirement 5: Use and regularly update anti-virus software or programs
  o Requirement 6: Develop and maintain secure systems and applications

• Implement Strong Access Control Measures
  o Requirement 7: Restrict access to cardholder data by business need to know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

- Regularly Monitor and Test Networks
  - Requirement 10: Track and monitor all access to network resources and cardholder data
  - Requirement 11: Regularly test security systems and processes.

- Maintain an Information Security Policy
  - Requirement 12: Maintain a policy that addresses information security for all personnel.

4. PCI DSS compliance policy

4.1. All University card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS).

4.2. This policy document forms part of University of Leicester information security policy and directly meets the PCI DSS requirement to “Maintain a policy that addresses information security for all personnel”.

4.3. Card processing activities must be conducted as described herein and in accordance with the PCI DSS standards. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.

4.4. All relevant staff must be made aware of the importance of cardholder data security and must be aware of the requirements stated in this policy.

4.5. This policy shall be reviewed annually and updated as needed to reflect changes to business objectives, to the risk environment or to PCI DSS.

4.6. The prospective procurement of any solution that includes card payment processing must be validated as being PCI-DSS compliant prior to purchase. As a requirement all prospective solutions must be contractually specified as being PCI-DSS compliant within the University of Leicester’s IT infrastructure.

(Note: Certain requirements stated in this policy are not part of the PCI DSS itself; however, are included to facilitate University PCI DSS compliance.)

5. Authorisation and responsibilities

5.1. Staff or departments must not plan, commission, use or modify any payment card processing procedures or systems without consultation with the Finance Office and authorisation by the Finance Director. (This includes any payment card processing activity to be undertaken on behalf of the University or which involves any use of University IT or networking equipment.)

5.2. The Finance Office is responsible for managing PCI DSS compliance across the University and may remove any payment card processing activity causing unacceptable risk.

5.3. IT Services is responsible for arranging and assessing the results of the external and internal network security scans required for PCI DSS compliance. (Approved external and internal network scans must be run at least quarterly to check for security against external access to any networked devices that process payment card data.)
5.4. The Finance Office and Information Assurance Services are jointly responsible for making all relevant staff aware of the importance of cardholder data security and the requirements stated in this policy.

5.5. The Finance Office is responsible for ensuring that for service providers with whom cardholder information is shared:

- Contracts require adherence to PCI-DSS by the service provider.
- Contracts include acknowledgement or responsibility for the security of cardholder data by the service provider.
- Their PCI DSS compliance status is monitored at least annually.

5.6. A list of all staff currently authorised to routinely use devices to process payment cards, such as tills, PEDs, PDQ machines etc. must be maintained by the department responsible for providing that service and a copy submitted to the Finance Income Systems Specialist who maintains the central log.

5.7. Staff are reminded of the requirement to report security incidents and any suspected security weaknesses as specified in Reporting Information Security Incidents (ISP-I3).

5.8. The Finance Office is responsible for maintaining a current list of all University payment card service providers.

6. Payment card processing

6.1. Students wishing to pay course fees by payment card must be directed to use the online payment system (see 6.8). Where that is not possible another form of payment i.e. cheque, draft or bank transfer must be used instead.

6.2. Staff must not request transmission of any payment card information from University customers via email, SMS/text, Skype, social networking, Microsoft Lync or other end-user messaging technologies.

6.3. Departments should, under no circumstances, ask students/customers to release the three-digit security code held on the reverse of their card. (The University pays a higher payment card transaction fee to avoid having to collect and process the security code.)

6.4. When staff process card details on a PED or PDQ credit card terminal, they should press the Enter key in order to skip the three-digit security code entry field. (Please note this does not apply to GPRS mobile terminals refer to 6.10)

6.5. Any electronically stored legacy payment card data, or data stored in error, must be deleted securely.

6.6. Payment card information, including full PAN numbers, must not be displayed or made visible to anyone except authorised staff. For example, payment equipment such as tills must not show the full PAN. (The first six and last four digits are the maximum number of digits that may be displayed.)

6.7. Full credit card numbers may only be viewed by authorised staff with a need to see them as part of their duties.

6.8. Students **must not** be specifically directed to University of Leicester IT equipment to use University of Leicester provided online payment solutions. If a student wishes to use
University IT infrastructure to make an online payment, then it is their choice and not mandated by the University.

6.9. Administrators of the Recurring Card Payment, when setting up a new payment plan on behalf of a student, are permitted to ask for the three digit security code if prompted by the system. This is an allowed exception to 6.3.

6.10. Finance provides GPRS mobile PED for short term. When making a MOTO payment, administrator’s using this type of terminal maybe prompted for a CVV and are permitted to ask for the three digit security code if prompted. This is an allowed exception to 6.3

7. Electronic cardholder data handling

7.1. Staff must not store any electronic payment card information, whether or not encrypted, on any computers or storage devices whether by scanning, keying or any other means. Note:

- This applies to all types of payment card data including PAN, PIN, three-digit security codes and full track data.
- This requirement limits the scope of the CDE and so controls the cost, difficulty and feasibility of implementing and maintaining the PCI DSS controls necessary for compliance.

7.2. Staff must not send cardholder data via email, sms/text, Skype, social networking, Microsoft Lync or other end-user messaging technologies, whether or not encrypted.

7.3. Systems which are specifically designed and deployed to transfer cardholder data electronically such as tills, PEDs and PDQs and outsourced e-commerce solutions must do so in a way that meets PCI DSS compliance requirements. When planning and deploying such systems, the Finance Office will work with departments, IT Services, system vendors, ISAs and QSAs as appropriate to achieve and maintain PCI DSS compliance.

7.4. Computers must not be used by University staff to access outsourced e-commerce solutions, such as WPM or YESPay, on behalf of customers.

7.5. University staff may only use PDQ machines to make payments on behalf of customers.

7.6. Authorised university staff may only access the WPM Recurring Card Payment application via the secure remote desktop & virtual server solution provided by IT Services.

7.7. Authorised university staff may only access the Realex virtual terminal via the secure remote desktop & virtual server solution provided by IT Services.

8. Paper cardholder data handling

8.1. The aim should be to reduce and preferably eliminate the need for cardholder data to be held in paper form. Processes should be regularly reviewed to determine whether online payment processes can be implemented to replace paper-based procedures.

8.2. Sensitive card authentication data must not be recorded on paper.

8.3. Cardholder data stored on paper, which exclude sensitive authentication data, must be:
• In a locked cabinet whenever not in use or supervised. Offices housing such cabinets must also be locked when not occupied. Keys to afore mentioned locked cabinets and offices should be kept securely at a location away from the locked cabinet and office.

• Destroyed when no longer required by secure onsite cross-cut shredding, incineration or pulping. (Paper records holding unwanted payment card information must be locked away until destroyed.) (also see 9.2 below.)

• Marked to distinguish it from other paperwork. Departments may use their own classification and marking system for cardholder data paperwork. A suitable solution would, for example, be to use distinctively coloured stationery.

• Photocopies of credit cards should never be taken or stored.

8.4. Where it is necessary to transfer paper cardholder data within the site:

• The only acceptable method is delivery by hand during office hours.

• The internal mail system must not be used.

• Card holder data movement must be logged with a despatch record and corresponding received record. Both should be reconciled to ensure movement of the data is complete.

• Card holder data when being transported should be in a sealed envelope or packet.

8.5. Incoming mail containing cardholder data from outside the University may be received through the internal mail system. However, regard should be had to Section 8.1 with a view to eliminating the need for paper-based processes.

8.6. There should not be any requirement for cardholder data to be sent via an external postal service. However, if in exceptional circumstances a need should arise, approval must be first obtained from the Director of Finance. In such cases the data must be delivered by hand to the Post Room and a tracked courier service must be used.

8.7. A record must be kept detailing any transfer of payment card data within the University and by external postal service should a need arise. Management approval is required prior to the transfer.

8.8. The use of faxes to receive card data should be discouraged, however if it is necessary to receive a fax, then the fax machine being used should not have an internal memory, hard drive or other storage solution capable of recording details of the received fax.

8.9. University multi-functional devices, network fax machines or computer based fax solutions should not be used to receive card data.

9. Retention of cardholder data

9.1. Cardholder data, excluding any sensitive authentication data, may be retained only as paper records. The only acceptable card holder data stored as paper records after processing a customer credit card are Merchant Receipts generated by:

| Finance distributed Chip & Pin devices |
| University EPOS system Chip & Pin devices |
| Chip & Pin devices connected to XN sports management system |

However it should be noted that under normal business procedures merchant receipts do
not display the full pan and that paper records of the PAN number after processing are not kept. (See 9.6)

9.2. Except in exceptional circumstances and with explicit approval of the Finance Office, retained cardholder data for any financial year (August-July) must be destroyed by the end of the following January.

9.3. Card holder data that is due to be destroyed must be secured in locked containers prior to destruction. The content should not be accessible.

9.4. Card holder data will be destroyed by the University's shredding service, using a means that makes it impossible to reconstitute the content of the paper based media.

9.5. Audits will be conducted by the Finance Office to ensure destruction.

9.6. The retention of card holder data after it has been processed is only permitted after written confirmation by the Deputy Director of Finance, subject to the team/department/staff member having:

- A proven business reason to retain card holder data
- The necessary processes and procedures in place to secure the card holder data in a compliant manner.
- A proven data management process that supports auditing, removal and secure destruction of the card holder data when no longer required.

10. Physical security of payment card processing equipment

10.1. Devices used to process payment cards, such as tills, PEDs and PDQ machines must:

- Only be used by staff authorised to do so as part of their duties.
- Be protected from physical access out-of-hours by those not authorised to use the equipment or authorised to be in the area. (Small devices such as PDQs must be locked away and larger devices such as tills must be in rooms with restricted access when not in use.)
- Be subjected to routine visual inspection, preferably each day or before use. Equipment, cabling and connections should be inspected for signs of tampering. The working area in the vicinity of the equipment should be checked for any suspicious devices, “hidden” cameras etc.
- Not be taken off site for testing, repair or use without written approval of a senior member of the Finance team.

10.2. Out-of-hours visitors to areas giving access to payment equipment must be supervised and details of such visits must be logged.

10.3. The installation of new or replacement equipment must be validated and approved by Finance working with IT services to ensure security of payment equipment has not been compromised.

10.4. Payment devices must not be positioned where University CCTV cameras can pick up card numbers, pin numbers and/or secure card data.

10.5. The use of University issued or personal video recording devices by University Staff must not be used in the vicinity where card numbers, pin numbers or secure card data can
be observed. This includes body cameras, Google Glass (and similar) and mobile phone cameras. Customers should be asked to deactivate any such device if they are in the vicinity of a card payment device.

**Failure to comply with University Policy may lead to disciplinary action.**

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.