Payment Card Industry – Data Security Standard (PCI DSS)
Security Policy

1 INTRODUCTION

This document provides an overview of the rules and regulations in place across The University of Northampton (UON) to allow us to achieve and maintain compliance to the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is a global standard managed and maintained by the Payment Card Industry Security Standards Council (PCI SSC), details can be found on their website here: https://www.pcisecuritystandards.org. This document and those sub-documents referred to below deal with security from a PCI DSS standpoint.

This document will be reviewed by IT Service, HR and Finance departments annually, in accordance with the requirements of PCI DSS, and be updated when business objectives or the risk environment changes.

Breach of this policy may be addressed under the disciplinary policy and procedure.

2 OWNERSHIP

The IT Services, Finance and Human Resources departments owns and manages this policy on behalf of The University of Northampton.

3 ORGANISATIONAL SCOPE

This PCI DSS Security policy is a corporate policy and applies to all employees (and workers, as applicable), contractor, vendors and third parties involved in the storage, transfer or processing of cardholder data that can affect the security of the cardholder data environment at the University of Northampton must follow existing security policies, unless an alternative policy exists, subject to any qualifying conditions.

4 POLICY STATEMENT

The University of Northampton is currently a Level 3 Merchant reporting to its acquirer via a series of SAQs (Self Assessment Questionnaires). The UON handles sensitive cardholder information daily. Sensitive information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation. The UON commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end, all University staff involved with any aspect of handling cardholder data are committed to maintaining a secure environment in which to process information so that we can meet these promises.

It is the responsibility of all users of the University's IT facilities to read, understand and comply with this policy and any additional policies related to their activities, including other relevant information security policies.

5 DEFINITIONS

Users
All parties who have been granted access to the University's IT Resources.

Attestation of Compliance (AOC)
The AOC is a form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in the Self-Assessment Questionnaire or report of compliance.

PCI-DSS
The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

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.

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.

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.

6 KEY PRINCIPLES

6.1 Overview

- All University card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS).
- This policy document forms part of UON policy on card payments and directly meets the PCI DSS requirement to "Maintain a policy that addresses information security for all personnel".
- 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.
- 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.
- This policy shall be reviewed annually and updated as required to reflect changes to business objectives, to the risk environment or to PCI DSS.
- Note: Certain requirements stated in this policy are not part of the PCI DSS itself; however, are included to facilitate University PCI DSS compliance and adhere to security best practice.

6.2 Responsibilities

All personnel (e.g. employees, contractors, vendors and third-parties) involved in the storage, transfer or processing of cardholder data or that can affect the security of the cardholder data environment at the UON must abide by relevant PCI DSS policies and procedures.

- Staff or departments must not plan, commission, use or modify any payment card processing procedures or systems without consultation with the Finance Department (Cash Office Manager). 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.
- The Finance Department is responsible for managing PCI DSS compliance across the University and may remove any payment card processing activity causing unacceptable risk.

- IT Services are 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.)
- The Finance Department along with Heads of College/Schools/Departments are jointly responsible for making all relevant staff aware of the importance of cardholder data security strategy and the requirements stated in this policy. Line managers are responsible for ensuring that all new and existing staff receive documentation and basic training in PCI DSS requirements.
- Departments/Areas working in a card payment environment, must nominate a locally responsible person to maintain PCI DSS records/compliance for that area.
- The Finance Department, IT and Records Management will collaborate and manage an incident escalation process, which will be reviewed and tested at regular intervals.
- Any staff requesting a PDQ machine or intending to work with card payments will need to obtain PCI DSS awareness training from the Finance Department and comply with the PCI DSS policy, before being allowed to do so.
- The Finance Department is responsible for ensuring that Central Finance system service providers dealing with cardholder information are PCI DSS compliant.
- A list of all staff currently authorised to 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 Department (Cash Office Manager) who will maintain a central register of authorised users.
- The Finance Department will maintain SharePoint page listing all locally responsible PCI DSS contacts, a list of all authorised PDQ users and evidence of Attestation of Compliance (AOC).

A PCI DSS specific risk-assessment process will be performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.) that identifies critical assets, threats, and vulnerabilities, and results in a formal, documented analysis of risk. (PCI DSS 12.2)

System responsibilities

All personnel involved in maintaining the technical systems for the CDE in the University are responsible for adhering to the rules, regulations, policies and procedures defined within the PCI DSS Systems Security Standard. (e.g. staff with roles in Network Security, Voice & Data and Web/Application Development).

Genuine credit card numbers (aka Live PANs) may not be used for testing or development. (PCI DSS 6.4.3)

6.3 Payment Card Processing

- Staff must not request or agree to accept transmission of any payment card information from University customers via email or other end-user messaging technologies. Any cardholder data received in this way should be deleted immediately.
- Staff must not ask for 3D Secure or Verified by Visa codes, when processing through an online interface.
- Any electronically stored legacy payment card data, or data stored in error, must be deleted.
- 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 or print details of the full PAN. (The first six and last four digits are the maximum number of digits that may be displayed.)
- Full credit card numbers may only be viewed by authorised staff with a need to see them as part of their duties.
- An update to date inventory of cardholder processing assets must be maintained.

6.4 Electronic cardholder data handling

- Staff must not store any electronic payment card information, whether 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.

- Staff must not transfer cardholder data via email, or other end-user messaging technologies, whether encrypted.
- 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 Department will work with departments, IT Services, system vendors and QSAs as appropriate to achieve and maintain PCI-DSS compliance.
- Cardholder data must not be stored on a removable media device.
- Computers being used by University staff to access outsourced e-commerce solutions, such as WPM on behalf of customers must automatically run updating anti-virus software.

6.5 Paper cardholder data handling

- 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.
- Sensitive card authentication data must not be recorded on paper.
- Cardholder data stored on paper, which must 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.
    - 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.)
    - 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.
    - 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.
- Incoming mail containing cardholder data from outside the University may be received through the internal mail system. Where there is the expectation that

mail may contain card data, two members of staff should be involved in the mail opening process. However, regard should be had to Section 6.5 point 1 with a view to eliminating the need for paper-based processes.

- 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.
- 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.

6.6 Retention of cardholder data

- Cardholder data, excluding any sensitive authentication data, may be retained if there is a business need, only as paper records.
- Except in exceptional circumstances and with explicit approval of the Finance Department, retained cardholder data for any financial year (August-July) must be destroyed by the end of the following January.

6.7 Physical security

- Any physical access to data or systems that house cardholder data provides the opportunity for persons to access and/or remove devices, data, systems or hard copies and should be appropriately restricted. Therefore:
- Entry controls to card payment environment should be limited and physical access monitored. All staff should wear identification badges to verify access to the area and where possible, having monitoring on entries and exits available.
- Any visitors entering the environment where cardholder data is processed should be logged. Visitors can include third-party vendors or guests. They should be identified with a unique ID (such as a badge) to determine who should and should not have access to areas where cardholder data is stored.
- PCI-DSS suggests not only escorting guests but the ID badge having an expiration date upon their entry. Visitors must surrender the badge before leaving the facility or at the date of expire. A visitor log is to be maintained as an audit trail of guests who enter and leave the cardholder facility.
- Physical access to areas where cardholder data is processed should be based upon their individual job function. Upon an employee's termination, their

access both systematically and physically should be revoked or disabled immediately.

Devices used to process payment cards, this includes but is not limited to: computers, removable electronic media, paper receipts, 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 near the equipment should be checked for any suspicious devices, “hidden” cameras etc.
- Out-of-hours visitors to areas giving access to payment equipment must be supervised and details of such visits must be logged.
- Spot checks will be performed as part of an agreed audit process with the PCI-DSS Project Team.

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

6.8 Awareness Training

- A formal awareness programme shall be implemented to make all staff associated with the card data environment aware of the University cardholder data security policy and procedures. (PCI DSS 12.6)
- Staff associated with the CDE will be trained in the requirements relevant to their role upon hire and at least annually. (PCI DSS 12.6.1)
- Staff will be required to acknowledge at least annually that they have read and understood the University PCI DSS policy and procedures.
- In the case where annual training is administered via the online PCI DSS training course, the course will track this information automatically. In the

case where other methods of training are used training administrators are responsible.

- All staff members are required to confirm with a signature that they have completed assigned training and understand the PCI DSS requirements for their role.
- All staff will review University PCI-DSS policy and undergo additional PCI DSS training while their role is connected to processing of card data.
- Staff will receive additional PCI DSS awareness training in the event of:
    - Role change where new duties involved card data processing
    - Role change where level of responsibility for card data processing changes
    - System changes altering the way card data is taken or processed
    - Introduction of new payment channels for card processing
    - Annual refresher/renewal
    - Changes in University policy, legislation or University contractual obligations that govern or impact on card processing activities.
- The UON is a member of the PCI DSS Special Interest Group, an organisation that proactively supports the promotion of PCI DSS awareness across the Higher Education sector.
- Individuals and departmental PCI DSS awareness is validated as part of the face to face PCI DSS audits within each department. The level of understanding is documented as part of the audit results.
- Where an individual is found to lack the necessary PCI DSS awareness, remedial training will be provided before the individual is permitted to process or handle card data.
- All individuals will confirm annually to Finance via email that they have read and understand the University PCI DSS security policy and procedures (as is required by PCI DSS requirement 12.6.1). This is recorded in the log referenced.

7 PROCEDURE

7.1 Reporting issues and breaches

If users do suspect or identify a security breach or concern relating to cardholder and personal information they should inform IT Services via the IT Service Desk on x3333.

Breaches to the Information Security policies should be discussed with managers and reported to IT Services via the portal or Portal or the IT Service Desk.

In the event of loss or theft of a UON device or device containing UON information or data, the user must act promptly to minimise the risk of compromise to UON information by immediately notifying IT Services. Theft of the device should also be reported to the police.

Managers should discuss the concerns Information Security policies with employees at the earliest opportunity with the intension to resolve issues informally, for by example, offering support, help and appropriate training to members of staff.

Failure to report a loss will be dealt with under the appropriate disciplinary and GDPR and PCI DSS policies.

8 ASSOCIATED DOCUMENTS

- PCI DSS Incident procedure
- Key Logger check list
- AOC Collection Process
- Disciplinary Policy and Procedure
- Code of Conduct
- GDPR Policy

9 EQUALITY IMPACT ASSESSMENT

There is no adverse equality impact within this policy. All responses to breaches of rights will be dealt with in accordance with this Policy, Procedure and relevant Appendices irrespective of an individual's specific characteristics.

10 VERSION CONTROL

Version Control	1.0	**Approval record**	
Author:	IT Services	Approval:	Trade Union Liaison JCNC UMT Governors 23RD August 2019
Date written:		June 2019	
Current status:		Approved	
Record of Amendments			
Date	Details of Change		Approval