University of Bristol
Information Security Policy

Title:	**PCI-DSS Cardholder Data Policy**
Reference:	**ISP-19**
Status:	**Approved**
Version:	**1.1**
Date:	**March 2017**
Reviewed:	**June 2019**
Classification:	**Public**

Contents

- Introduction
- Compliance requirements
- University of Bristol Policies
- Policy
  - General
  - Credit Card Handling
  - Monitoring and Compliance Responsibilities

Introduction

This policy provides essential information for everyone involved with handling credit and debit cards, credit and debit card data and the systems processing such data within the University of Bristol. It is designed to ensure we can meet the standards required by the Payment Card Industry's Data Security Standard (PCI-DSS), which is a worldwide standard set up to help businesses (merchants) process card payments securely and reduce card fraud. The University of Bristol must comply with PCI DSS to process card payments.

Compliance Requirements

Compliance with this policy is mandatory. Failure to follow this policy will be considered under the University's conduct procedure (Ordinance 28) and may result in disciplinary action. A serious breach of the policy may constitute gross misconduct and lead to dismissal. Compliance with policies is primarily enforced through process and standard documents. Finance Services and IT Services will provide guidance and support but due to the diverse nature of some of our activities these process and documents must be developed by each business area.

University of Bristol Information Security Policies

University of Bristol policies affecting the entire University, not just cardholder data, can be found at: http://www.bristol.ac.uk/infosec/policies/docs/. Where any contradictions arise within the handling of cardholder data, this policy takes precedent.

Definitions

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organisations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud.

'Credit/Debit card' or 'cardholder' data means most of the information on a credit card or debit card and includes the long 16 digit card number (Primary Account Number - PAN). It also includes the issue and expiry dates and the cardholder's name. The three digit security code on the back of the card is known as the Card Verification Value (CVV).

General

- Failure to protect card data can lead to large fines from banks, expensive investigations, litigation, loss of reputation and in the worst case scenario, withdrawal of the ability to take payment by credit card; which would greatly hinder the University of Bristol's ability to conduct business.
- No staff member should handle cardholder data unless they have a business need and explicit authorisation to do so.
- Cardholder data should only be handled in such a manner as is explicitly authorised by job roles.
- Electronic credit card data shall not be transmitted by the University of Bristol via any private network that the University is responsible for **unless in accordance with with the handling requirements in this policy**. This includes wired and wireless connections.
- University staff and students shall not store credit and debit cardholder data on local hard drives, shared storage (myFiles), cloud storage solutions, or any removable media (memory stick, CD/DVD) under any circumstances.
- Cardholder data shall not be transmitted or requested to be transmitted via end-user messaging technologies such as email, instant messaging or SMS. If unsolicited cardholder data is received via such means, this must be notified to the Information Security Manager and the data securely deleted.
- Any card data stored on University of Bristol systems must be reported to pci.dss@bristol.ac.uk immediately upon discovery.

Credit/Debit Card Handling

It is the University's policy not to store cardholder data electronically or process that data on the University network. There will be however some processing of cardholder data done by the University on behalf of its staff and students. All processing of cardholder data must be agreed and recorded by IT Services (the Information Security Manager) and by Finance Services.

Any processing (including by third parties) must meet the following conditions:

- All handlers of cardholder data must be adequately screened and trained before being allowed access. This training must be recorded and repeated/updated regularly.
- Cardholder data must not be processed via digital connections provided by the University (wired or wireless). Where it is agreed that cardholder data can be directly processed by staff; public data networks (GPRS/3G/4G/5G) combined with strong encryption or properly-configured P2PE solutions implemented in accordance with their respective Implementation Guides must be used instead. Analogue (telephone) lines are acceptable. Analogue telephone infrastructure must be properly secured against interference by unauthorised personnel.
- Cardholder data shall not be stored in any voice recordings. Where cardholder data may be taken over the telephone, any call recording solution shall be disabled whilst cardholder data is being given
- Any device used to process cardholder data on behalf of the University must be first agreed by Finance Services (the Associate Director of Financial Operations)
- Where the device may be a laptop or PC, they will be 'standalone' and entirely separate from the configuration of devices used on the University network. The device must be approved by the Information Security Manager to an agreed secure configuration. This includes but is not exclusive to up to date anti-virus, encrypted storage, strong access controls and security updates being applied at least every month.
- Where the device is a Point-of-Sale (POS) terminal it must be of a type approved by Finance Services. The details (model, serial number, security features and location) of all examples in use must be recorded and supplied to Finance Service for inclusion in the asset list that they maintain. Such devices must be configured and used in accordance with Finance procedures.
- All devices must be stored securely when not in use and checked regularly for tampering or substitution. Any suspicion of tampering must be reported in line with the Incident response procedure.
- University staff and students must not store cardholder data on paper unless specifically agreed by the Information Security Manager and the Associate Director of Financial Operations. Any cardholder data stored on paper must only be done so prior to authorisation (not after). It must be securely stored when not in use and destroyed in line with the University's Confidential Waste Disposal procedure (requires authentication to access).

Third Parties

Any third party commissioned to handle cardholder information on behalf of the University of Bristol must be approved by Finance and IT based on proper due diligence prior to engagement. Their compliance status must be assessed by the Information Security Manager. If they are a PCI DSS compliant Service Provider for the contracted services they provide to the University, they will be required to provide the University with an up-to-date version of their Attestation of Compliance before engagement and each year thereafter.

Any contracts or written agreements with third party providers must make clear their responsibility for maintaining/protecting the University's compliance. A full list of Third Party Payment Service Providers will be maintained by Finance Services, and the service providers PCI DSS compliance will be checked by Finance Services at least annually.

Incident response

An Incident/Breach Response Plan must be in place, reviewed and tested at least annually. Any breach or suspected breach must be reported immediately to the PCI incident response email address - pci.dss@bristol.ac.uk. This will acknowledged shortly after receipt.

Monitoring and compliance responsibilities

Overall responsibility for the University's PCI DSS compliance is held by the Chief Financial Officer (CFO), as they are responsible for management of income, as well as the signatory of any contract with our acquirer/s. As the storage, transmission and processing of cardholder data and the associated risks are largely an Information Technology challenge, the Chief Information Officer (CIO) also has a significant responsibility for ensuring adherence to this policy and associated procedures.

Any staff or students including all permanent (direct hire), temporary and contract staff are responsible for ensuring our adherence with this policy. IT Services (the Information Security Manager) and the Associate Director of Financial Operations shall ensure it is available and promoted to those that need to see it.

It is the responsibility of the Information Security Manager to maintain this policy and ensure it is reviewed at least annually or if the environment changes. An assessment of the risks relating to the processing of cardholder will be conducted annually by the Information Security Manager with the support of IT Services and Finance Services.

The PCI DSS Internal Security Assessor, Information Security Manager, Associate Director of Financial Operations, or any of their representatives, are authorised to inspect any systems, databases, or physical areas of the University where cardholder data might be processed or stored.

Many areas of the University process credit/debit cards as payment for the services they provide. Separate Merchant IDs (MIDs), set up by our acquiring bank have been authorised for use by a number of Divisions. All relevant Heads of Division are responsible for ensuring this Policy is adhered to and that each MID has an identified responsible manager. The Income Office Manager is responsible for maintaining a full register of all MIDs, the manager responsible, and all assets in use relating to each MID (e.g. point-of-sale / PDQ terminals).