ATFS
INDEPENDENT, SOLUTIONS DRIVEN

ATFS Bulletin February 2022
PCI DSS 4.0

PCI DSS Overview

The Payment Card Industry Data Security Standard (PCI DSS) was established in 2006 by the major card brands (e.g., Visa, MasterCard, American Express, Discover Financial Services and JCB International). Designed to improve the safe keeping of payment data by businesses who process, transmit or store cardholder data, to establish a standard if followed, thus creating a safer environment to protect the valuable payment data. The standard would then improve the security within businesses and to protect payment data against theft and use for fraudulent payments, while also bringing into scope the full payment journey with all personal, equipment and systems used to accept card payments.

Due to the complex nature of the PCI standard, Universities struggle to obtain and maintain PCI DSS compliance for a variety of reasons. The first step is understanding the PCI scope you have from the card data you process or store. Card acquirers can assist using internal security teams that should be able to give direction on achieving and maintaining compliance. Should you need external assistance through a QSA or equivalent these can really assist the University understand the correct approach to the pathway of compliance.

Depending on how you take card payments, PCI DSS compliance normally has two areas. A completion of a SAQ (questionnaire based on the way you process or store payments) and a scan of internal and external networks that accepts, processors and stores card holder data. This is normally an automated scan that will highlight and identify vulnerabilities within the University network that may need correcting to achieve compliance.

PCI DSS currently has four levels based on card transaction volume as per below:

Level 1: Merchants processing over 6 million card transactions per year.
Level 2: Merchants processing 1 to 6 million transactions per year.
Level 3: Merchants processing 20,000 to 1 million transactions per year.
Level 4: Merchants processing fewer than 20,000 transactions per year

How to understand your PCI responsibilities

Depending on the way you process, store payments including through your networks, this will impact on which SAQ that you must complete. This includes what type and how the card terminals process through your networks, what type of ecommerce gateway you use, how you store card data etc. will all contribute to the type of SAQ you will need to complete.

It is important to understand what networks you have in scope for PCI compliance and have a good understanding of the SAQ you will need to complete. This will allow you to understand what if any changes to the network need completing and highlight any potential gaps within the SAQ that need correcting through internal changes or policies to achieve PCI compliance.

Internal PCI teams sharing the responsibilities of aiming to achieve or maintain compliance can often lead to the best result, with each playing their own part in meeting the PCI demands across the University.

PCI DSS 4.0

PCI 4.0 is the latest version of the PCI DSS standard that will be released in Q1 2022; this version has had more involvement from the merchant payment community and Qualified Security Assessors (QSA) than previous versions. Currently there have been Request for Comment (RFC) releases and thousands of comments submitted to help improve version 4.0. Currently the focus should still be on PCI DSS version 3.2.1 until 4.0 is finalised and released. Upon release of version 4.0 our recommendation is to add 4.0 into your PCI planning straight away. The expectation is for the new standard you will have 18 months after release to implement. By using version 4.0 for PCI planning on release this will help highlight any gaps or assist moving priorities from projects that may need less work to complete.

We understand that version 4.0 will re-write details within the standard to suit the constant changes in the complex payment world. Changes could include the scoping to areas that we have not seen in previous versions like cloud computing, ensure the standard continues to meet the requirements of the payment world, Anti-Phishing and Social Engineering measures as well as adding a margin of flexibility to support achieving compliance. All changes will have a purpose of complimenting the message of promoting payment security as a continuous process, not just an annual event. The PCI DSS standard has always tried to make security part of a "business as usual" process and in PCI 4.0 we should see this extend to help shift towards the continuous method.

For those that have spent time and effort meeting previous PCI versions, you can rest assured that the twelve core areas will remain in 4.0 as it is the latest version and not a new standard.

The importance with any change in the PCI DSS standard is to understand any areas you may need to implement and look to start working towards them within the defined timescales, normally 18 Months after the release of the new standard. All Universities should have a cross functional PCI working group to also engage with your Acquirers/PSP/Gateways and QSA's where needed, to help assist with achieving and maintaining PCI compliance including payment security.

PCI DSS Considerations

- Set up or maintain a PCI internal working group so the standard is shared between different departments within the University.
- Make sure all terminals are P2PE (Point 2 Point Encrypted) to help lessen the burden of terminal information passing through your network.
- Implement PCI DSS 4.0 to all planning on release to at least know what you need to work towards.
- Understand the gaps you have in meeting the PCI DSS standard and work with your card acquirer or a QSA if you do not understand how to meet the specific requirements outstanding.
- Check with your PSP/Gateway provider that you are on the best version to assist with PCI DSS compliance and security payment needs.

For further information, please contact:

Tim Wilding
Director, Financial Services
M: 07557 367370
E: tim.wilding@atfsltd.co.uk

Carl Fleet
Director Financial Services
M: 07502 485678
E: carl.fleet@atfsltd.co.uk