PCI DSS (3rd Parties And PCI DSS Compliance)

University of East Anglia

Background

The Payment Card Industry Data Security Standards (PCI DSS) is a set of requirements that all businesses must meet if they are to process, store or transmit credit and debit card payments. The payment card industry has set these standards to ensure that the environment within which card payments are made is safe and secure. The PCI DSS is administered and managed by the PCI SSC which an independent body is created by major credit card brands such as Visa and MasterCard.

An annual assessment is undertaken on every company taking credit and debit card payments. Depending on the types of payments being made companies have a responsibility to perform a Self-Assessment Questionnaire and to be subject to vulnerability scanning and penetration testing.

Responsibilities

UEA is not a service provider to 3rd parties who are using its network, it is also unable to provide 3rd parties with PCI compliant network secure zones and supporting infrastructure to allow systems to be meet PCI compliance. A service provider is any company that stores, processes, or transmits cardholder data on behalf of another entity. 3rd parties are defined as businesses which are not owned or part of the University of East Anglia. Any card payments that the 3rd Party is processing, transmitting or storing will be made to a Merchant ID not owned by the University of East Anglia.

3rd Parties have a responsibility to ensure any form of payments that they processing, transmitting or storing do not take place on the University Network. Any 3rd party which is processing, transmitting or storing card payments must obtain PCI compliance certification with their own acquiring bank.

PED Devices (PIN Entry Devices commonly referred to as PDQ machines)

Any PED device which is on the University network and is owned by a 3rd party should be removed from the University Network unless 3rd parties have approved authorisation from the Finance Department. 3rd Parties can use PEDs as long as they are one of the following:

- A SIM (mobile phone network) PED.
- Has a dedicated analogue phone line or internet connection provided by a service provider such as Virgin Media or BT. The use of analogue to VOIP conversion on the UEA network by 3rd party devices is prohibited.
- A certified P2PE compliant device (which isolates the device from the University Network using encryption). P2PE devices can be operated through the University Network.

UEA will not be able to provide 3rd parties with a PED payment solution as UEA would need to gain certification as a service provider which it currently does not have.

Online Payment Systems

UEA will not be able to provide any external organisation with an online payment solution as UEA would need to gain certification as a service provider which it currently does not have.

For UEA staff and departments, who wish to use an external service provider, will need to contact the finance dept. to authorise any such use. If departments do not use the pre-approved WPM system to receive online payments then due diligence checks on the alternative payment solution is required (including a review of the contract and obtaining the suppliers PCI certificate as a service provider on an annual basis).

Penalties

The Payment Card Industry will fine banks if any organisation is found to be non-compliant with the standards that they have defined. Normally banks will pass on this fine to the customer who is non-compliant to PCI. If data breaches do occur then additional fines could be imposed by PCI and potentially also the ICO (Information Commissioner's Office).

UEA reserves the right to remove any 3rd Party payment device or system that stores, processes, or transmits card payment data from the University network. This includes devices or systems that are non-compliant with PCI standards on the University network or ones which are advertised and redirecting customers to it from the University Network.

Authorisation to take card payments

Any person wishing to take credit or debit card payment on the University Network, **must** contact the Finance Division before accepting any forms of credit/debit card payments. Please complete a Payment Request form and pass to Rhoda Wolf (ext. 3780) if you wish to introduce a service, system or device that processes, stores or transmits credit and debit card payments. Finance will need to provide authorisation to any 3rd party wishing to accept credit or debit card payments.

Reporting Data Breaches

In cases where there is suspicious behaviour or actual data breaches on systems processing, storing or transmitting card holder data, 3rd parties should report their concerns to their acquiring bank.

Further Advice

We are advising all parties that are not part of UEA but are using the UEA network that if debit/credit card payments are being taken they should contact their acquiring bank for advice. If you need external consultancy to aid your compliance journey then your bank may be able to help you. Alternatively, we recommend the use of an independent security consultant such as 7safe (http://pci-dss.7safe.com/).

For further information on PCI compliance see https://www.pcisecuritystandards.org/. The University Financial Regulations stipulating effective control and management of University financial affairs can be found https://portal.uea.ac.uk/finance/regulations-and-procedures.

Further guidance is also available from the University Finance Division by contacting Rhoda Wolf (Senior Finance Accountant).

Telephone: 01603 593780, Email: r.wolf@uea.ac.uk