E-commerce Security Policy

Document Owner: Matt Roach

Date of last review: 13/02/2020

Version: 4.1

This document defines the University's security policy on the use of websites to take payments via payment cards, and is based on the following principles:

- **Where practical, existing approved systems will be used for payments**
- **Use of systems including those provided by third parties must be compliant with the requirements of the PCI DSS**
- **Specifically, all use must satisfy the SAQ A-EP**
- **Many general information security policies also apply as well as more stringent requirements for this particular use of data and equipment**

IMPORTANT: If you are planning on accepting payments by payment card, you must first speak with Finance to ensure that you only set up systems and processes compliant with this policy.

Version history

Version	Date	Note
0.1	4/8/15	First draft
0.2	22/9/15	Second draft
1.0	20/10/15	Approved by ISSC
1.1	25/2/16	Updated reference to names of PCI policies
2.0	26/2/16	Approved by ISSC Chair
2.1	11/5/16	Updated to reflect changes in April 2016 update to PCI DSS, version 3.2
3.0	14/6/16	Approved by ISSC
3.1	30/3/17	Reviewed
4.0	13/6/17	Approved by ISSC
4.1	13/2/20	Document reviewed – 'ISD' replaced with 'ITCS'

Introduction

Payments taken from payment cards are subject to the Payment Card Industry's Data Security Standard (PCI DSS). Where the payment is taken via the use of a website as part of an e-commerce payment channel, the system used must satisfy a subset of the requirements in the PCI DSS. These requirements concern the acquisition and maintenance of the systems as well as their operating environment including network, hardware, and user accounts in the handling of payment card data.

Requirements are placed on the technical staff with responsibility for systems carrying cardholder data (CHD) as well as those processing payments and those overseeing the processing.

To satisfy the PCI DSS, all requirements must be met and documentation showing how they have been met must be generated in the course of their operation and management. Failure to meet the requirements of the PCI DSS may lead to the University being prevented from taking card payments, or fined, or both.

This policy applies to e-commerce payment channels taking card payments using a third party website for payment processing. Alternatively, for Face to Face and MOTO (mail order, telephone order) transactions the University may make use of payment terminals to take card payments. The use of payment terminals must satisfy the University's Face to face and MOTO card payment security policy.

Scope

This policy applies to:

- All those parties with responsibility for use of websites taking payments by payment card. This includes and is not limited to IT staff, FPG staff, and staff in departments operating systems and their managers/supervisors, and contracted staff working on behalf of the University
- The acquisition, installation, configuration, operation, maintenance, management and decommissioning of websites used for taking card payments
- All systems within the cardholder data environment (CDE), including network components, servers, and applications
- All systems hosted on the UEA data network, as well as those operated outside the UEA data network, which includes cloud-hosted systems which have certifications of PCI DSS compliance
- Companies totally owned by the University of East Anglia and its subsidiaries

SAQ A-EP is defined by the Payment Card Industry to apply to:

- E-commerce merchants with a website that does not itself receive CHD but which does affect the security of the payment transaction and/or integrity of the page that accepts the consumer's CHD.
- E-commerce merchants who partially outsource their e-commerce payment channel to PCI DSS validated third parties and do not electronically store, process or transmit any CHD on their systems or premises.

Definitions

The following definitions apply to this policy:

- **Card verification code or value**. The three-digit or four-digit card verification code or value printed on the front of the payment card or the signature panel (CVV2, CVC2, CID, CAV2 data).
- **Cardholder data environment (CDE)**. The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data. It is everything that the CHD or SAD touches and everything which connects to those systems. At the University, this includes: every switch/router/firewall that passes the client to the web application server (which has the code for the URL redirection to WPM for card processing); the servers involved in getting the client to that web application server; and any other supporting system that directly connects to it (DNS, SysAdmin machines, AD etc.). The website directly impacts how the payment card data is transmitted, even though the website itself does not receive any cardholder data.
- **Cardholder data (CHD**). This includes the primary account number (PAN), cardholder name, expiration date, and service code.
- **CVSS.** Common Vulnerability Scoring System. A vendor agnostic, industry open standard designed to convey the severity of computer system security vulnerabilities and help determine urgency and priority of response.

- **DMZ**. Abbreviation for “demilitarized zone.” Physical or logical sub-network that provides an additional layer of security to an organization’s internal private network. The DMZ adds an additional layer of network security between the Internet and an organization’s internal network so that external parties only have direct connections to devices in the DMZ rather than the entire internal network.
- **DSS**. Data Security Standard.
- **Network segmentation**. Network segmentation isolates system components that store, process, or transmit CHD from systems that do not. Adequate network segmentation may reduce the scope of the CDE and thus reduce the scope of the PCI DSS assessment.
- **PAN**. Primary Account Number. The customer’s card number.
- **Payment card**. The PCI DSS defines payment card to be any payment card bearing the logo of one of the founding members of the PCI SSC (Security Standards Council), namely, American Express, Discover, JCB, MasterCard or Visa.
- **Payment card processing entities**. All those bodies involved in the processing of a payment made by payment card. This includes the merchant (UEA in this case), processors, acquirers, issuers, and service providers.
- **PCI**. Payment Card Industry.
- **Penetration test**. Penetration tests attempt to identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the environment (external testing) and from inside the environment.
- **PIN**. Personal identification number.
- **PTS**. PIN transaction security.
- **SAQ**. Self-Assessment Questionnaire.
- **Secure coding**. The process of creating and implementing applications that are resistant to tampering and/or compromise.
- **Sensitive authentication data (SAD)**. This includes the full track data (magnetic stripe data or equivalent on a chip), card verification code or value, and PINs/PIN blocks.
- **Service provider**. Any third party organisation which processes CHD on behalf of the University, e.g. a document retention company that stores paper documents that include CHD. PCI DSS Requirements also apply to the service provider to ensure continued protection of the data. Processing includes transmitting, retrieving, storing, and destroying.
- **System components**. Any network devices, servers, computing devices, or applications included in or connected to the CDE.
- **Trusted network**. Network of an organization that is within the organization’s ability to control or manage.
- **Untrusted network**. An untrusted network is any network that is external to the networks belonging to the University, and/or which is out of the University’s ability to control or manage.
- **Vulnerability scan**. A scan for flaws or weaknesses which, if exploited, may result in an intentional or unintentional compromise of a system.

Aims

The aim of this policy is to ensure that the University:

- Meets the requirements of the PCI DSS as they apply to the use of web systems processing payments by card as defined by SAQ A-EP.

Policy statements – general

The University will only use payment channels which are PCI compliant. For e-commerce transactions, it will aim to achieve PCI compliance under SAQ A-EP, and for Face to Face and MOTO transactions - SAQ B and SAQ P2PE-HW.

E-commerce system proposals

- All e-commerce systems receiving payments by card on behalf of the University are to be approved for use by the University and these must comply with the SAQ A-EP requirements as described in this policy.
- Where practical, all proposals must use existing approved systems for receiving payments in preference to establishing any new systems.
- All plans for e-commerce systems receiving payments by card must be approved by Finance. ITCS, SPC and CIS will provide advice on the technical compliance of systems (it.servicedesk@uea.ac.uk).
- Each element of the payment page delivered to the customer's browser must originate from either the University website or a PCI DSS compliant service provider.
- The University will not electronically store, process, or transmit any CHD on its own systems or premises, but will rely entirely on a third party to handle all these functions.
- The University will retain only paper reports and receipts with CHD, and these documents must not be received electronically.

Use of third party service providers

- All processing of CHD, with the exception of the payment page, must be entirely outsourced to a PCI DSS validated third-party payment processor.
- University e-commerce websites will not receive CHD but will control how customers, or their CHD, are redirected to a PCI DSS validated third party payment processor.
- If the website is hosted by a third party provider, the provider must be validated to all applicable PCI DSS requirements.
- Where a number of different service providers are involved in different steps in a payment channel, all steps must be compliant with this policy, and all service providers must be PCI DSS validated.

Acting as a service provider for third parties

- UEA departments must not set up any payment processing services for third parties through University systems, e.g. selling tickets on behalf of a third party, including any collecting, retrieving, transmitting, storing, or destroying of CHD. To operate in this way the University would need to become a service provider in its own right and would therefore need to achieve an additional more stringent level of PCI compliance.

Exceptions

- Where an e-commerce proposal does not meet the requirements of SAQ A-EP, explicit authorisation to accept the risks of non-compliance (including the University receiving unlimited fines and the removal of its ability to accept payments by card) must be obtained from the Director of Finance and Planning. Otherwise, the e-commerce system must not be used.
- If it is not possible for a service provider supporting a payment channel to achieve PCI DSS compliance, the risk to the University must be accepted and signed off by the Director of Finance and Planning. Otherwise, the payment channel must not be used.

- Any e-commerce systems receiving payments by card which are found to have been installed or operated in contravention to this policy will be shut down and disconnected from the network, and will be subject to an investigation.

Policy statements – PCI DSS requirements

Where a policy statement relates directly to a requirement of the PCI DSS, the relevant requirement reference is provided.

Build a secure network [Req 1]

The CDE is a sensitive area within the University's trusted network and traffic in and out of it must be controlled by use of firewalls.

- Firewalls and router must be configured to established standards. [Req 1.1]
- All network connections and changes to the firewall and router configurations must follow a formal test and approval process. [Req 1.1.1]
- There must be a current network diagram which identifies all connections between the CDE and other networks including wireless networks. [Req 1.1.2]
- The network diagram must show all CHD flows across systems and networks. [Req 1.1.3]
- Firewall configuration standards must be written and include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone [Req 1.1.4]
- The network diagrams for the associated CDE must be consistent with the firewall configuration standards, which requires an illustrative drawing on the diagrams of the logical and/or physical positioning of the firewalls within the network topology. [Req 1.1.4]
- Authorized personnel must regularly review network configuration documentation for the purposes of verifying that firewalls are in place at each Internet connection and between any DMZ and the internal network zone. [Req 1.1.4]
- Firewall and router configuration standards must include a documented list of services, protocols and ports used, a business justification for why they are being used, and approval for use. [Req 1.1.6]
- Any insecure services, protocols and ports used must be identified, the business justification for why they are being used and approval for use must be given. The security features used to remove or reduce the risk associated with use of insecure services must be documented. [Req 1.1.6]
- Firewall and router rule sets must be reviewed at least every six months. [Req 1.1.7]
- Firewall and router configurations must restrict connections between untrusted networks and any system components in the CDE. [Req 1.2]
- Inbound and outbound traffic must be restricted to that which is necessary for the CDE. All other traffic is denied. [Req 1.2.1]
- Router configuration files must be secured and synchronized. [Req 1.2.2]
- Perimeter firewalls must be installed between all wireless networks and the CDE. The firewalls must deny all traffic except that required for business purposes. [Req 1.2.3]
- Direct public access between the Internet and any system component in the CDE must be prohibited. [Req 1.3]
- A DMZ must be implemented to limit inbound traffic to only system components that provide authorised publicly accessible services, protocols and ports. [Req 1.3.1]
- Inbound Internet traffic must be limited to IP addresses in the DMZ. [Req 1.3.2]
- Anti-spoofing measures must be implemented to detect and block forged sourced IP addresses from entering the network, e.g. internal addresses cannot pass from the internet to the DMZ. [Req 1.3.3]

- Ensure that any outbound traffic from the CDE to the Internet is explicitly authorised. [Req 1.3.4]
- Stateful inspection (dynamic packet filtering) must be implemented. Only established connections are allowed onto the network. [Req 1.3.5]
- Measures must be in place to prevent the disclosure of private IP addresses and routing information from internal networks to unauthorised parties except where authorised. [Req 1.3.7]
- Personal firewall software must be installed on any portable computing devices (including those owned by the University or individual) which connect to the Internet when outside the network and which also are used to connect to the CDE. The firewall must be configured to specified settings, actively running, and cannot be altered by the user of the portal computing device. [Req 1.4]
- Security policies and operational procedures for managing firewalls must be documented, in use, and known to affected parties. [Req 1.5]

Review system default settings [Req 2]

Individuals (external and internal to the University) could use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information. They must therefore be removed from systems as part of the installation and configuration process.

- Before installing a system on the network, all vendor supplied defaults must be reviewed and changed, and all unnecessary default accounts must be removed or disabled. [Req 2.1]
- System components must be configured to industry-accepted security hardening standards. Standards must address all known security vulnerabilities and:
    - Review and amend all vendor supplied defaults
    - Removal of unnecessary default accounts
    - Implementation of only one primary function per server, including virtual servers [Req 2.2.1]
    - Enablement of only those services, protocols, daemons etc. as required for the system's functioning. Use of insecure services, protocols, daemons etc. must be justified in documented configuration standards and have additional security features implemented [Req 2.2.2, 2.2.3]
    - Configuration of system security parameters to prevent misuse [Req 2.2.4]
    - Removal of all unnecessary functionality, e.g. scripts, drivers, features, subsystems, file systems, and web servers, and confirmation that only documented functionality is present [Req 2.2.5]
- System configuration standards must be maintained and updated as new vulnerability issues are identified. [Req 2.2]
- New system components must be configured and verified to system configuration standards before being installed on the network. [Req 2.2]
- All non-console administrative access must be encrypted using agreed strong encryption over technologies such as SSH, VPN and TLS. All insecure remote access means such as Telnet must be disabled from use for non-console access. The strong encryption method must be invoked before the administrator's password is requested and implemented according to industry best practices and/or vendor recommendations. [Req 2.3]

Protect stored CHD [Req 3]

CHD must not be stored. If found, CHD must be securely destroyed.

- CHD must not be stored electronically. [Req 3.2]

- If sensitive authentication data is held, after authorisation, all data must be deleted and rendered unrecoverable. [Req 3.2]
- All system components (including incoming transaction data, all logs, history files, trace files, database schemas, database contents) must be configured to ensure that sensitive authentication data is not stored after authorisation, including:
    - Card verification code or value (CVV2, CVC2, CID, CAV2) [Req 3.2.2]
    - Personal identification number (PIN) [Req 3.2.3]
    - Encrypted PIN block

Encrypt transmission of CHD [Req 4]

Sensitive CHD must be encrypted during transmission over networks that are easily accessed by malicious individuals.

- CHD including PANs are classed as CONFIDENTIAL information and must be handled in accordance with the University's Information Classification and Data Management policy.
- Sensitive CHD must be encrypted with strong encryption and security protocols (TLS, IPSEC, SSH, etc.) when transmitted or received over open, public networks. Protocols must be implemented to use only secure configurations, and must not support insecure versions or configurations. [Req 4.1]
- System components must accept only trusted keys or certificates. [Req 4.1]
- Encrypted and unencrypted PANs must not be sent via any end-user messaging technology including email, instant messaging, fax, chat or forum sessions. [Req 4.2]
- Security policies and operational procedures for encrypting transmissions of CHD must be documented, in use, and known to affected parties. [Req 4.3]

Protect systems against malware [Req 5]

Systems in the CDE can be compromised by malware and therefore steps must be taken to protect against malware infection, including the installation and maintenance of anti-virus software.

- Agreed anti-virus software must be deployed on all systems commonly affected by malicious software and be capable of detecting, removing and protecting against all known types of malicious software (e.g. viruses, Trojans, worms, spyware, adware, and rootkits). [Req 5.1, 5.1.1]
- Periodic reviews must be made to evaluate evolving malware threats and whether systems not commonly affected by malicious software remain as such. Reviews should be conducted at least once a year, and prior to planning for the annual programme of work so that any remediation can be built into plans if required. [Req 5.1.2]
- Licensed anti-virus software must be run on all system components in or connected to the CDE as well as all computers not directly associated with the CDE. Anti-virus software must:
    - Be kept current and have current definition files.
    - Perform periodic scans.
    - Generate audit logs which are retained in accordance with Req 10.7. [Req 5.2]
    - Be actively running and not able to be disabled or altered by users (unless specifically authorised by management on a case-by-case basis for a limited time period). [Req 5.3]
- Security policies and operational procedures for protecting systems against malware must be documented, in use, and known to affected parties. [Req 5.4]

Develop secure systems and applications [Req 6]

Vulnerabilities in systems can be exploited. To protect against this, vendor supplied patches must be installed.

- A process for identifying security vulnerabilities must be established by subscribing to industry-leading security sources, vulnerability announcements and security patch management alerts. The security patch management process must include risk ranking (H/M/L) covering: significance of the threat, threat of exploitation, and risks to service of applying patches. [Req 6.1]
- Critical patches (as identified by the risk ranking process) must be installed within 1 month of release. [Req 6.2]
- All system components and software must be protected from known vulnerabilities by installing vendor-supplied security patches. [Req 6.2]
- Change control procedures must include the following:
    - Documentation of impact. [Req 6.4.5.1]
    - Documented change approval by authorised parties. [Req 6.4.5.2]
    - Testing to ensure that the change does not adversely impact the security of the system. [Req 6.4.5.3]
    - Rollback procedures. [Req 6.4.5.4]
- Following any significant change, all relevant PCI DSS requirements must be implemented on all new and changed systems and networks. Documentation must be updated. [Req 6.4.6]
- Staff with responsibility for developing code must be trained at least annually in secure coding techniques, including avoidance of common coding vulnerabilities and the handling of personal data in memory. [Req 6.5] Coding techniques must address:
    - Injection flaws (SQL, OS and LDAP injection) [Req 6.5.1]
    - Buffer overflows [Req 6.5.2]
    - Insecure communications [Req 6.5.4]
    - Improper error handling [Req 6.5.5]
    - All high risk vulnerabilities identified in the vulnerability identification process [Req 6.5.6]
    - Cross-site scripting [Req 6.5.7]
    - Improper access control [Req 6.5.8]
    - Cross-site request forgery [Req 6.5.9]
    - Broken authentication and session management [Req 6.5.10]
- For public-facing web applications, new threats and vulnerabilities must be addressed on an ongoing basis either by running application vulnerability security assessment tools annually or after every change by an organisation that specialises in application security including all vulnerabilities listed in Req 6.5 and that all vulnerabilities are corrected and the application re-evaluated after corrections, **or** by installing an automated solution which detects and prevents web-based attacks which is situated in front of public-facing web applications, actively running, generating audit logs and configured to block web-based attacks or generate an alert which is investigated. [Req 6.6]
- Security policies and operational procedures for developing and maintaining secure systems and applications must be documented, in use, and known to affected parties. [Req 6.7]

Restrict access to CHD by business need to know [Req 7]

Access to the CDE must be limited to the least amount of data and privileges required to perform a job function.

- Access to system components and CHD must be limited to only those individuals whose job requires access. [Req 7.1]

- Access rights for privileged users must be limited to the least privileges necessary to perform job responsibilities. [Req 7.1.2]
- Access control systems must be configured to enforce privilege assigned to individuals based on their job classification and function. [Req 7.1.3]
- Privileges assigned to individuals must be have documented approval by authorised parties. [Req 7.1.4]

Identify and authenticate access to system components [Req 8]

Users with access to the CDE or any system associated with it must be identified and authenticated, and remote access protected with two factor authentication. These requirements do not apply to accounts used by consumers (cardholders).

- All users must have a unique ID before they access system components or CHD. [Req 8.1.1]
- Addition, deletion and modification of user IDs and credentials must be controlled (i.e. implemented as authorised). [Req 8.1.2]
- Access for terminated users must be revoked immediately. [Req 8.1.3]
- Inactive user accounts must be disabled or removed within 90 days. [Req 8.1.4]
- IDs used by third parties to access, support or maintain system components via remote access must be managed as follows:
    - Enabled only during the time period when needed
    - Disabled when not in use
    - Monitored when in use [Req 8.1.5]
- User IDs must be locked out after no more than six attempts to log on. [Req 8.1.6]
- The lockout period must be for a minimum of 30 mins, or until an administrator enables the user ID. [Req 8.1.7]
- If a session has been idle for more than 15 minutes, the user must re-authenticate to re-activate the session. [Req 8.1.8]
- In addition to assigning a unique user ID, users must use one or more of the following methods for authentication:
    - Something that is known (such as a password)
    - Something which is held (such as a token device or smartcard)
    - Something that the individual is (such as a fingerprint or iris pattern) [Req 8.2]
- All authentication credentials must be rendered unreadable when transmitted and stored on system components by use of strong encryption. [Req 8.2.1]
- The user's identity must be verified before modifying any authentication credential, such as a password reset. [Req 8.2.2]
- Passwords/passphrases must be a minimum of seven characters and contain both numeric and alphabetic characters. [Req 8.2.3]
- Passwords/passphrases must be changed at least every 90 days. [Req 8.2.4]
- A new password/passphrase must differ from the last four passwords/passphrases used. [Req 8.2.5]
- Passwords/passphrases for first-time use and upon reset must be a unique value for each user, and changed after first use. [Req 8.2.6]
- Multi factor authentication (MFA) must be implemented for all individual non-console administrative access and all remote access to system components in the CDE by users, administrators and third parties (such as support and maintenance or vendors). [Req 8.3] MFA is required for:
    - All non-console access into the CDE for personnel with administrative access. [Req 8.3.1]

    - All remote network access (user, administrator, and third parties) originating from outside the network. [Req 8.3.2]
- All authentication policies and procedures must be documented and communicated to users. Guidance includes: selection of strong authentication credentials; protection of authentication credentials; instructions not to reuse passwords; and instructions to change password if there is any suspicion of compromise. [Req 8.4]
- Group, shared, or generic user IDs must not be used to administer any system components. [Req 8.5]
- Where other authentication methods are used (e.g. physical or logical security tokens or smartcards), they must be assigned to an individual account and not shared between accounts. Controls must be in place to ensure that only the intended account can use the mechanism to gain access. [Req 8.6]
- Security policies and operational procedures for identification and authentication must be documented, in use, and known to affected parties. [Req 8.8]

Restrict physical access to CHD and CDE [Req 9]

All physical media including paper holding copies of CHD must be held and destroyed securely.

- Appropriate entry control mechanisms must be used to limit and monitor physical access to systems in the CDE. [Req 9.1]
- All physical media containing CHD must be physically secured to prevent any access by unauthorised personnel, e.g. by storage in a locked drawer, cabinet or safe, or secure offsite backup facility. The location's security must be reviewed at least annually. [Req 9.5]
- Internal or external distribution of any media must be strictly controlled [Req 9.6]:
    - Classify media to determine the sensitivity of the data [Req 9.6.1]
    - Send media via secured courier or other delivery method to enable tracking [Req 9.6.2]
    - Management must approve any movement of media from a secured area [Req 9.6.3]
- The storage and accessibility of media is to be strictly controlled. [Req 9.7]
- All hardcopy material containing CHD must be securely destroyed when no longer needed so it cannot be reconstructed. [Req 9.8.1]
- Storage containers used for holding hardcopy material containing CHD awaiting destruction must be securely locked. [Req 9.8.1]

Track and monitor access to network resources and CHD [Req 10]

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise and in investigating the cause of a compromise.

- Audit trails must link all access to system components to individual users. [Req 10.1]
- Automated audit trails for system components must be implemented [Req 10.2], recording
    - All actions by users with root or administrative privileges [Req 10.2.2]
    - Access to all audit trails [Req 10.2.3]
    - Invalid logical access attempts [Req 10.2.4]
    - Use of and changes to identification and authentication mechanisms [Req 10.2.5]
    - Initialisation, stopping or pausing of the audit logs [Req 10.2.6]
    - Creation and deletion of system-level objects [Req 10.2.7]
- The audit logs for system components must record at least the following details for each event [Req 10.3]
    - User ID [Req 10.3.1]

    - Type of event [Req 10.3.2]
    - Date and time [Req 10.3.3]
    - Success or failure indication [Req 10.3.4]
    - Origination of event [Req 10.3.5]
    - Identity or name of affected data, system component, or resource [Req 10.3.6]
- All critical system clocks must be synchronised using time-synchronisation technology. [Req 10.4] The following must be implemented:
    - Critical systems have the correct and consistent time [Req 10.4.1]
    - Time data is protected [Req 10.4.2]
    - Time settings are accepted from industry-accepted time sources [Req 10.4.3]
- Audit trails must be secured so that they cannot be altered. [Req 10.5] This includes:
    - Viewing of audit trails must be limited to only those with a job-related need [Req 10.5.1]
    - Audit trails must be protected from unauthorised modifications [Req 10.5.2]
    - Audit trail files must be promptly backed up to a central log server (or media which is difficult to alter) [Req 10.5.3]
    - Logs for external-facing technologies must be written onto a secure, centralised internal log server [Req 10.5.4]
    - File integrity monitoring or change-detection software must be used on logs to ensure that existing logs cannot be changed without generating alerts. (New data added should not generate an alert) [Req 10.5.5]
- Authorised personnel must review the following logs and security events on a daily basis for all system components to identify anomalies and suspicious activity. [Req 10.6.1]
    - All security events
    - System components that store, process or transmit CHD or SAD
    - Critical system components
    - Servers and system components that perform security functions (firewalls, IDS, IPS, authentication servers, e-commerce redirect servers, etc.)
- All other system components must be reviewed periodically based on the University's risk management strategy as determined by the annual risk assessment. [Req 10.6.2]
- All exceptions and anomalies identified by the review of audit logs must be followed up. [Req 10.6.3]
- The audit trail history must be retained for at least one year, with a minimum of three months immediately available for analysis. [Req 10.7]

Regularly test security systems and processes [Req 11]

System components, processes, and custom software should be frequently tested for vulnerabilities to ensure security controls continue to reflect a changing environment and remain effective.

- An Approved Scanning Vendor (ASV) must perform external vulnerability scans at least every quarter and after every significant change in the network (e.g. new system component installations, changes in network topology, firewall rule modifications, product upgrades). Rescan as necessary until the ASV Program Guide requirements for a passing scan have been met. [Req 11.2.2]
- Qualified personnel must perform internal and external scans and rescans as needed (e.g. after any significant change). Change control process for system components subject to significant change must include a requirement for a scan. Rescan until: for external scans, no vulnerabilities exist that scored 4.0 or higher by the CVSS; for internal scans, all high risk vulnerabilities are resolved. [Req 11.2.3]
- A methodology for penetration testing must be implemented covering:
    - Use of industry-accepted penetration testing approaches (NIST SP800-115)

    - Inclusion of the entire CDE perimeter and critical systems
    - Tests from both inside and outside the network
    - Validation of segmentation and scope reduction controls
    - Application layer penetration tests to include vulnerabilities listed in Req 6.5
    - Network layer penetration tests to include components that support network functions as well as operating systems
    - Reviews and consideration of threats and vulnerabilities experienced in the last 12 months
    - Retention of penetration testing results and remediation activities results. [Req 11.3]
- Qualified personnel must perform internal and external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (e.g. operating system upgrade, or subnetwork or a web server added to the environment). [Req 11.3.1,]
- Any exploitable vulnerabilities found during penetration testing must be corrected, and repeated testing verifies that the corrections have been made. [Req 11.3.3]
- Penetration tests must also be performed annually and after any changes to segmentation controls or methods to verify that segmentation methods are operational and effective, and isolate all out of scope systems from the CDE. Tests must be performed by a qualified internal resource or qualified external third party. [Req 11.3.4]
- Intrusion detection and intrusion prevention techniques must be used to detect or prevent intrusions into the network. All traffic must be monitored at the perimeter of the CDE as well as at critical points in the CDE. Personnel must be alerted to suspected compromises. All intrusion detection and prevention engines, baselines and signatures must be kept up to date. [Req 11.4]
- A change detection mechanism (such as file integrity monitoring tools) must be deployed to alert personnel to any unauthorised modification of critical system files, configuration files, or content files. Critical file comparisons must be performed at least weekly. Authorised personnel must investigate and resolve all alerts. [Req 11.5] A process must be implemented to respond to any alerts generated by the change-detection solution. [Req 11.5.1]

Maintain a policy that addresses information security [Req 12]

Policies and procedures must be in place to address the requirements for the security of the University's CDE especially around the use of third party service providers.

- A security policy must be established, published, maintained and disseminated. [Req 12.1]
- The security policy must be reviewed at least annually and updated when the environment changes. [Req 12.1.1]
- The security policy and procedures must clearly define information security responsibilities for all personnel. [Req 12.4]
- A security incident response and escalation procedure must be created. [Req 12.5.3, 12.10.1]
- The incident response plan must address at a minimum:
    - Roles, responsibilities, communication and contact strategies in the event of a compromise including notification of the payment brands
    - Specific incident response procedures addressing the most likely incident scenarios
    - Business recovery and continuity procedures
    - Data backup procedures
    - Legal requirements for reporting compromises
    - Coverage and responses of all critical system components
    - Reference to or inclusion of incident response procedures for the payment brands [Req 12.10.1]

- A formal security awareness programme must be implemented to ensure that all personnel are aware of the CHD security policy and procedures and the importance of maintaining the security of CHD. [Req 12.6]
- A current and accurate list of approved service providers must be maintained including contact details for all personnel and a description of the services provided. [Req 12.8.1]
- For any services engaged with service providers that may affect or have a relationship or function associated with CDE, there must be a written agreement which includes an acknowledgement by the service providers of their responsibility for securing the CHD they possess, process or transmit. [Req 12.8.2]
- Due diligence must be exercised before engaging with any service providers that may affect or have a relationship or function associated with the University's CDE. [Req 12.8.3]
- Service providers' compliance with PCI DSS will be monitored and checked at least annually by supplying a copy of its current PCI certification. [Req 12.8.4]
- Any agreement with a service provider must make clear which PCI DSS requirements are to be managed by the service provider, and which will be the responsibility of the University. [Req 12.8.5]

Responsibilities

Within this policy, the following individuals or groups have the following responsibilities [Req 12.4]:

Responsibility	**PCI DSS Requirement**	**Owner**
Approval for the use of e-commerce systems taking payments by payment card		FIN
Advise on the technical compliance of e-commerce systems taking payments by payment card		ITCS, CIS
Sign off on risks associated with use of non-compliant systems or suppliers in a payment channel		Director of Finance and Planning
Produce and apply firewall configuration standards	1.1, 1.1.4, 1.2, 1.2.1, 1.2.2, 1.2.3, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.7	ITCS networking
Define and follow formal test and approval process for network connections and changes to firewall and router configurations	1.1.1	ITCS networking
Produce and maintain network diagrams	1.1.2, 1.1.3, 1.1.4	ITCS networking
Review network configuration documentation	1.1.4	ITCS
Provide business justification for services, protocols and ports used in firewall and router configuration standards	1.1.6	System owners
Review firewall and router rule sets	1.1.7	ITCS networking
Install personal firewall on personal computing devices	1.4	ITCS desktop services
Ensure security policies are documented, in use, and known	1.5, 4.3, 5.4, 6.7, 8.4, 8.8	ITCS SPC
Securely configure any system to be added to the network	2.1, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.3	System owners

Responsibility	PCI DSS Requirement	Owner
Produce and maintain system configuration standards to follow industry-accepted security hardening methodologies	2.2	System owners
Store no CHD electronically	3.2	All users handling CHD
Configure system components to ensure that: no SAD is stored after authorisation; strong encryption and security protocols are used to send CHD over open networks; and only trusted key or certificates are accepted	3.2.2, 3.2.3, 4.1	System owners
Send no PANs via end user messaging technologies	4.2	All users handling CHD
Deploy anti-virus on all system commonly affected by malware	5.1, 5.1.1, 5.2, 5.3	IT Systems Team
Review risk to systems not commonly affected by malware	5.1.2	ITCS
Develop process for identifying security vulnerabilities and ranking the risk to the organisation	6.1	IT Systems Team
Install vendor-supplied security patches on system components following change control procedures. Ensure that all critical patches are installed within 1 month of release	6.2	System owners
Change control for implementation of security patches	6.4.5.1, 6.4.5.2, 6.4.5.3, 6.4.5.4, 6.4.6	ITCS Management Team
Train staff with responsibility for developing code in secure coding techniques	6.5, 6.5.1, 6.5.2, 6.5.4, 6.5.5, 6.5.6, 6.5.7, 6.5.8, 6.5.9, 6.5.10	ITCS CIS
Ensure that threats and vulnerabilities to public-facing web applications are addressed on an ongoing basis	6.6	ITCS CIS
Restrict access to the CDE and CHD to only those who require it. Ensure that access rights are set to least privilege required, and based on job classification and function	7.1, 7.1.2, 7.1.3, 7.1.4	System owners, Departments running e-commerce
Issue all users with a unique ID and revoke access on staff departure. Disable inactive accounts. Check identity before password resets	8.1.1, 8.1.2, 8.1.3, 8.1.4	IT Systems Team System owners
Manage and monitor third party access to system components	8.1.5	System owners
Configure secure access to system components. Individual non-console administrative access to use MFA. Shared IDs must not be used. Lock out idle sessions	8.1.6, 8.1.7, 8.1.8, 8.2, 8.2.1, 8.2.3, 8.2.4, 8.2.5, 8.2.6, 8.3, 8.3.1, 8.3.2, 8.5, 8.6	System owners

Responsibility	PCI DSS Requirement	Owner
Limit and monitor physical access to systems in the CDE	9.1	System owners
Create procedures for the secure storage of physical media holding CHD. Review storage at least annually	9.5	System owners, Departments running e-commerce
Strictly control the distribution of media holding CHD	9.6, 9.6.1, 9.6.2, 9.6.3, 9.7	System owners, Departments running e-commerce
Securely destroy hardcopy material holding CHD when no longer needed	9.8.1	System owners, Departments running e-commerce
Implement audit trails on all system components	10.1, 10.2, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6	System owners
Synchronise system clocks using time-synchronisation technology	10.4, 10.4.1, 10.4.2	IT Systems Team System owners
Set up, configure and maintain central log server. Secure logs so they cannot be altered. Review logs and follow up on suspicious behaviour. Retain logs for a year	10.5, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.5.5, 10.6.1, 10.6.3, 10.7	ITCS IT Systems Team
Review system components annually to determine risk of compromise	10.6.2	ITCS
Engage with an approved scanning vendor to conduct quarterly vulnerability scans	11.2.2	ITCS
Perform internal and external scans for vulnerabilities	11.2.3	ITCS
Develop and implement a methodology for penetration tests including network segmentation controls	11.3, 11.3.1, 11.3.2, 11.3.4	ITCS
Set up and operate intrusion detection and prevention systems	11.4	ITCS
Deploy a change detection mechanism to identify modifications to critical system files	11.5, 11.5.1	ITCS
Fix any vulnerabilities or issues discovered by scans, tests, or monitoring	11.3.3	System owners
Create and maintain incident response plan	12.5.3, 12.10.1	ITCS
Deliver general security awareness training for all staff with access to systems handling CHD covering the importance of securing CHD	12.6	ITCS
Maintain a list of approved service providers	12.8.1	FIN

Responsibility	PCI DSS Requirement	Owner
Draft agreements and manage relationship with approved service providers on a daily basis	12.8.2, 12.8.5	ITCS, System owners, Departments running e-commerce
Conduct due diligence checks, approval and selection of service providers and their regular review	12.8.3, 12.8.4	FIN, ITCS
Review and update of this policy	12.1, 12.1.1	ITCS
Internal audit of compliance with this policy		ITCS

References

This E-commerce Security policy is supported within the context of the following pieces of legislation, professional standards, and University documents:

- Face to face and MOTO card payment security policy. https://portal.uea.ac.uk/documents/6207125/7103513/Face-to-face-and-MOTO-security-policy/
- General information security policy. https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies/information-security/gisp. In particular,
    - GISP1 – Risk assessment and risk management
    - GISP2 – Conditions of computer use
    - GISP3 – Physical and environmental security
    - GISP4 – Identification, authentication and authorisation
    - GISP5 – Use of passwords
    - GISP7 – Onsite access control
    - GISP8 – Offsite access control
    - GISP9 – Change management
    - GISP10 – Protection against malicious software
    - GISP11 – Information classification
    - GISP14 – Incident reporting and handling
    - GISP15 – Network monitoring
    - GISP16 – Legal and regulatory compliance
    - GISP17 – IT and information asset management
    - GISP18 – Encryption use and key material handling
    - GISP19 – Personnel security
    - GISP22 – Working with third parties
    - GISP24 – System management and development
- Records management policy. https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies/records-management
- Information classification and data management policy https://portal.uea.ac.uk/documents/6207125/6857482/Information+classification+policy.pdf/
- PCI DSS Requirements v3.2. https://www.pcisecuritystandards.org/security_standards/pcidss_agreement.php?association=pcidss

- PCI SAQ A-EP v3.2. https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-A_EP.pdf
- PCI DSS Glossary v3.2. https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf
- PCI Approved Scanning Vendor (ASV) Program Guide - https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v2.pdf

Breaches

Any breaches of this policy must be reported at the earliest opportunity to ITCS via misuse@uea.ac.uk. ITCS will lead on an investigation in consultation with FIN and the affected department. Serious breaches will be referred to HRD as matters to be deal with under staff disciplinary procedures.

Review

The E-commerce Security policy will be reviewed every 12 months or sooner as necessary by the ITCS Strategy, Policy and Compliance team to ensure it remains current in the light of relevant legislation, organisational procedures, contractual obligations or changes to the environment or updates to PCI requirements [Req 12.1.1]. Changes will be agreed with the Director of Information Services, and authorisation and quality assurance will be provided by the Information Strategy and Services Committee (ISSC).