PCI DSS Compliance in Advancement: Update for 3.2

Ron King

Please find a list below of additional resources from the *PCI DSS Compliance in Advancement: Update for 3.2* webcast. If you wish to print only certain resources, you may click their respective links to jump directly to them in the packet.

PCI DSS Compliance in Advancement: Update for 3.2
Ron King

Sample contract language for use with a service provider in any solicitation / contract that may involve online credit card payments.

PCI DSS COMPLIANCE: <Merchant> requires that the contractor shall at all times maintain compliance with the most current Payment Card Industry Data Security Standards (PCI DSS). The contractor will be required to provide written confirmation of compliance. **Contractor acknowledges responsibility for the security of cardholder data as defined within the PCI DSS**. Contractor acknowledges and agrees that cardholder data may only be used for completing the contracted services as described in the full text of this document, or as required by the PCI DSS, or as required by applicable law. In the event of a breach or intrusion or otherwise unauthorized access to cardholder data stored at or for the contractor, contractor shall immediately notify _____ to allow the proper PCI DSS compliant breach notification process to commence. The contractor shall provide appropriate payment card companies, acquiring financial institutions and their respective designees access to the contractor's facilities and all pertinent records to conduct a review of the contractor's compliance with the PCI DSS requirements.

In the event of a breach or intrusion the contractor acknowledges any/all costs related to breach or intrusion or unauthorized access to cardholder data entrusted to the contractor deemed to be the fault of the contractor shall be the liability of the contractor. Vendor agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify and hold harmless _____and its officers and employees from and against any claims, damages or other harm related to such breach.

PCI Best Practices and Lessons Learned

- *NEVER* e-mail credit card information
- *NEVER* store credit card numbers in any database or spreadsheet
- *DO* truncate all but last 4 digits of cc number
- *DO* keep credit card documentation locked
- *DO* permit only employees who have a legitimate "need-to-know" access to cardholder info
- *DO* destroy documentation containing credit card information when no longer
- *DO* document departmental desktop procedures
- *DO* update cash handling procedures
- *DO* segregate duties – the individual performing reconciliation should not be involved in processing credit card sales or refunds

Compliance Is Not:

- Just a quarterly scan
- Just a signed SAQ
- Just anti-virus and complex passwords
- Vendors saying they are compliant

Compliance Is:

- Annual training for EVERYONE who transmits, stores or processes credit cards with "sign off"
- Redacting credit card information after the payment is processed
- Keeping credit card swipe machines in a secure place
- Certifying that all third party vendors involved in processing, transmitting or storing credit card information are PCI DSS compliant on a quarterly basis.

Things to Look For:

- Inadequate segmentation between card holder environment and campus network
- Inadequate inventory documentation
- Inconsistent forms management and storage
- Inadequate policies and procedures
- Annual training not performed
- Inadequate system scans
- Third party contracts need to be amended to include PCI compliance
- How cards are used in the Development office
- Email used for registration and CHD
- Phone call transactions written on *sticky notes*
- CHD received via voice-mail messages
- CHD processed on forms, left on receptionist desk until they are hand delivered to cashier
- Forms with CHD "ripped up and thrown in the trash"
- Off-hours book sales handled by faculty – who complete forms and turn in to the bookstore
- Receipts stored in unlocked cabinets and large bins
- Keys to file cabinet kept in unlocked desks
- Shared accounts (passwords) in use
- CHD received via phone calls, written on a form and then entered into bank system via touch tone phone - forms then stored in the desk in the office
- CHD stored in boxes in an open area where classes are held

PCI Glossary

Acquirer: Also referred to as “acquiring bank” or “acquiring financial institution.” Entity that initiates and maintains relationships with merchants for the acceptance of payment cards.

Anti-Virus: Program or software capable of detecting, removing, and protecting against various forms of malicious software (also called “malware”) including viruses, worms, Trojans or Trojan horses, spyware, adware, and rootkits.

Application: Includes all purchased and custom software programs or groups of programs, including both internal and external (for example, web) applications.

ASV: Acronym for “Approved Scanning Vendor.” Company approved by the PCI SSC to conduct external vulnerability scanning services.

Authentication: Process of verifying identity of an individual, device, or process. Authentication typically occurs through the use of one or more authentication factors such as:

- Something you know, such as a password or passphrase
- Something you have, such as a token device or smart card
- Something you are, such as a biometric

Authorization: Granting of access or other rights to a user, program, or process. For a network, authorization defines what an individual or program can do after successful authentication. For the purposes of a payment card transaction authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.

Cardholder Data (CHD): At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code See Sensitive Authentication Data for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.

Cardholder Data Environment (CDE): The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components.

Card Verification Code or Value: Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features.

1. Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand:
    - **CAV** - Card Authentication Value (JCB payment cards)
    - **CVC** - Card Authentication Value (JCB payment cards)
    - **CVV** - Card Validation Code (MasterCard payment cards)
    - **CSC** - Card Security Code (American Express)
2. For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit unembossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. The following list provides the terms for each card brand:
    - **CID** - Card Identification Number (American Express and Discover payment cards)
    - **CAV2** - Card Authentication Value 2 (JCB payment cards)
    - **CVC2** - Card Validation Code 2 (MasterCard payment cards)
    - **CVV2** - Card Verification Value 2 (Visa payment cards)

Compensating Controls: Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must: (1) Meet the intent and rigor of the original PCI DSS requirement; (2) Provide a similar level of defense as the original PCI DSS requirement; (3) Be “above and beyond” other PCI DSS requirements (not simply in compliance

with other PCI DSS requirements); and (4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement. See "Compensating Controls" Appendices B and C in PCI DSS Requirements and Security Assessment Procedures for guidance on the use of compensating controls.

Compromise: Also referred to as "data compromise," or "data breach." Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.

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.

Encryption: Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure. See Strong Cryptography.

File Integrity Monitoring: Technique or technology under which certain files or logs are monitored to detect if they are modified. When critical files or logs are modified, alerts should be sent to appropriate security personnel.

Firewall: Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.

Forensics: Also referred to as "computer forensics." As it relates to information security, the application of investigative tools and analysis techniques to gather evidence from computer resources to determine the cause of data compromises.

Hosting Provider: Offers various services to merchants and other service providers. Services range from simple to complex; from shared space on a server to a whole range of "shopping cart" options; from payment applications to connections to payment gateways and processors; and for hosting dedicated to just one customer per server. A hosting provider may be a shared hosting provider, who hosts multiple entities on a single server.

Information Security: Protection of information to insure confidentiality, integrity, and availability.

Information System: Discrete set of structured data resources organized for collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

IP: Acronym for "internet protocol." Network-layer protocol containing address information and some control information that enables packets to be routed. IP is the primary network-layer protocol in the Internet protocol suite.

IP Address: Also referred to as "internet protocol address." Numeric code that uniquely identifies a particular computer on the Internet.

IPS: Acronym for "intrusion prevention system." Beyond an IDS, an IPS takes the additional step of blocking the attempted intrusion.

LAN: Acronym for "local area network." A group of computers and/or other devices that share a common communications line, often in a building or group of buildings.

Magnetic-Stripe Data: Also referred to as "track data." Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe.

Mainframe: Computers that are designed to handle very large volumes of data input and output and emphasize throughput computing. Mainframes are capable of running multiple operating systems, making it appear like it is operating as multiple computers. Many legacy systems have a mainframe design.

Malicious Software / Malware: Software designed to infiltrate or damage a computer system without the owner‹s knowledge or consent. Such software typically enters a network during many business-approved activities, which results in the exploitation of system vulnerabilities. Examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits.

Merchant: For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.

Two or more computers connected together via physical or wireless means.

Network Security Scan: Process by which an entity's systems are remotely checked for vulnerabilities through use of manual or automated tools. Security scans that include probing internal and external systems and reporting on services exposed to the network. Scans may identify vulnerabilities in operating systems, services, and devices that could be used by malicious individuals.

Network Segmentation: Network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the cardholder data environment and thus reduce the scope of the PCI DSS assessment. See the Network Segmentation section in the PCI DSS Requirements and Security Assessment Procedures for guidance on using network segmentation. Network segmentation is not a PCI DSS requirement. See System Components.

PA-QSA: Acronym for "Payment Application Qualified Security Assessor," company approved by the PCI SSC to conduct assessments on payment applications against the PA-DSS.

PAN: Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

Password / Passphrase: A string of characters that serve as an authenticator of the user.

Patch: Update to existing software to add functionality or to correct a defect.

Payment Application: Any application that stores, processes, or transmits cardholder data as part of authorization or settlement.

Payment Cards: For purposes of PCI DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or Visa, Inc.

PCI: Acronym for "Payment Card Industry."

PED: PIN entry device

Penetration Test: Penetration tests attempt to exploit vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the network trying to come in (external testing) and from inside the network.

PIN: Acronym for "personal identification number." Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder's signature.

Policy: Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures

POS: Acronym for "point of sale." Hardware and/or software used to process payment card transactions at merchant locations.

Private Network: Network established by an organization that uses private IP address space. Private networks are commonly designed as local area networks. Private network access from public networks should be properly **protected with the use of firewalls and routers.**

Procedure: Descriptive narrative for a policy. Procedure is the "how to" for a policy and describes how the policy is to be implemented.

Public Network: Network established and operated by a telecommunications provider, for specific purpose of providing data transmission services for the public. Data over public networks can be intercepted, modified, and/or diverted while in transit. Examples of public networks in scope of the PCI DSS include, but are not limited to, the Internet, wireless, and mobile technologies.

QSA: Acronym for "Qualified Security Assessor," company approved by the PCI SSC to conduct PCI DSS on-site assessments.

Remote Access: Access to computer networks from a remote location, typically originating from outside the network. An example of technology for remote access is VPN.

Report on Compliance: Also referred to as "ROC." Report containing details documenting an entity's compliance status with the PCI DSS.

Report on Validation: Also referred to as "ROV." Report containing details documenting a payment application's compliance with the PCI PA-DSS.

Risk Analysis / Risk Assessment: Process that identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.

Router: Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways.

Scoping: Process of identifying all system components, people, and processes to be included in a PCI DSS assessment. The first step of a PCI DSS assessment is to accurately determine the scope of the review.

Security Officer: Primary responsible person for an entity's security-related affairs.

Security Policy: Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Protocols: Network communications protocols designed to secure the transmission of data. Examples of security protocols include, but are not limited to SSL/TLS, IPSEC, SSH, etc.

SAQ: Acronym for "Self-Assessment Questionnaire." Tool used by any entity to validate its own compliance with the PCI DSS.

Server: Computer that provides a service to other computers, such as processing communications, file storage, or accessing a printing facility. Servers include, but are not limited to web, database, application, authentication, DNS, mail, proxy, and NTP.

Service Provider: Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.

SQL Injection: Form of attack on database-driven web site. A malicious individual executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization's host computers through the computer that is hosting the database.

Trojan: Also referred to as "Trojan horse." A type of malicious software that when installed, allows a user to perform a normal function while the Trojan performs malicious functions to the computer system without the user's knowledge.

Truncation: Method of rendering the full PAN unreadable by permanently removing a segment of PAN data. Truncation relates to protection of PAN when stored in files, databases, etc. See Masking for protection of PAN when displayed on screens, paper receipts, etc.

Two-Factor Authentication: Method of authenticating a user whereby two or more factors are verified. These factors include something the user has (such as hardware or software token), something the user knows (such as a password, passphrase, or PIN) or something the user is or does (such as fingerprints or other forms of biometrics).

Virtualization: Virtualization refers to the logical abstraction of computing resources from physical constraints. One common abstraction is referred to as virtual machines or VMs, which takes the content of a physical machine and allows it to operate on different physical hardware and/or along with other virtual machines on the same physical hardware. In addition to VMs, virtualization can be performed on many other computing resources, including applications, desktops, networks, and storage.

Virtual Machine: A self-contained operating environment that behaves like a separate computer. It is also known as the "Guest," and runs on top of a hypervisor. Virtual Terminal: A virtual terminal is web-browser-based access to an acquirer, processor or third party service provider website to authorize payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.

VLAN: Abbreviation for “virtual LAN” or “virtual local area network.” Logical local area network that extends beyond a single traditional physical local area network.

VPN: Acronym for “virtual private network.” A computer network in which some of connections are virtual circuits within some larger network, such as the Internet, instead of direct connections by physical wires. The end points of the virtual network are said to be tunneled through the larger network when this is the case. While a common application consists of secure communications through the public Internet, a VPN may or may not have strong security features such as authentication or content encryption. A VPN may be used with a token, smart card, etc., to provide two-factor authentication.

Vulnerability: Flaw or weakness which, if exploited, may result in an intentional or unintentional compromise of a system..

WAN: Acronym for “wide area network.” Computer network covering a large area, often a regional or company wide computer system.

Web Application: An application that is generally accessed via a web browser or through web services. Web applications may be available via the Internet or a private, internal network.

Web Server: Computer that contains a program that accepts HTTP requests from web clients and serves the HTTP responses (usually web pages).

CAMPUSGUARD

Required PCI DSS Documentation

PCI DSS Reference	Documentation Requirement	SAQ	SAQ A	SAQ A-EP	SAQ B	SAQ B-IP	SAQ C	SAQ C-VT	SAQ D	SAQ P2PE-HW
1.1	Firewall and routing configuration standards	SAQ D							X	
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations	SAQ D							X	
1.1.2	Current diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	SAQ B-IP SAQ D				X			X	
1.1.3	Current diagram that shows all cardholder data flows across systems and networks	SAQ D							X	
1.1.5	Description of groups, roles, and responsibilities for management of network components	SAQ D							X	
1.1.6	Documentation and business justification for use of all services, protocols, and ports allowed	SAQ A-EP SAQ B-IP SAQ D		X		X			X	
1.1.7	Requirement to review firewall and router rule sets at least every six months	SAQ D							X	
1.3.8b	Document reviewed that specifies whether any disclosure of private IP addresses and routing information to external parties is permitted	SAQ A-EP SAQ D		X					X	
1.5	Security policies and operational procedures for managing routers and firewalls	SAQ C-VT SAQ D						X	X	
2.1.1	Vendor documentation examined to compare defaults to current configuration	SAQ B-IP SAQ C SAQ C-VT SAQ D				X	X	X	X	
2.2	Configuration standards and procedure	SAQ A-EP SAQ C SAQ D		X			X		X	
2.4	Maintain inventory of system components (hardware and software) in scope for PCI DSS	SAQ C-VT SAQ D						X	X	
2.6	Security policy and operational procedures for managing vendor defaults and other security parameters	SP							*SP**	
3.1	Data Retention disposal policy and procedure	SAQ D SAQ P2PE-HW							X	X
3.5.1	User access list to card holder data	SAQ D							X	
3.6	Key (encryption) management procedures	SAQ D							X	
3.6.8	Key custodian responsibility management form	SAQ D							X	
3.7	Security policies and operational procedures for protecting stored cardholder data	SAQ D SAQ P2PE-HW							X	X
4.3	Security policies and operational procedures for encrypting transmissions of cardholder data	SAQ D							X	
5.4	Security policies and operational procedures for protecting systems against malware	SAQ D							X	
6.1	Process to identify security vulnerabilities	SAQ A-EP SAQ B-IP SAQ C SAQ C-VT SAQ D		X		X	X	X	X	
6.3	Software development process	SAQ D							X	
6.4	Change control process and procedure	SAQ D							X	
6.6	Application security assessment	SAQ A-EP SAQ D		X					X	
6.7	Security policies and operational procedures for developing and maintaining secure systems and applications	SAQ D							X	
7.2	Documented access approvals	SAQ D							X	
7.3	Security policies and operational procedures for restricting access to cardholder data	SAQ D							X	
8.1.1	Account maintenance procedure	SAQ A-EP SAQ D		X					X	
8.2.1	Vendor documentation for all software in PCI DSS scope	SAQ A-EP SAQ D		X					X	
8.2.2	Authentication procedures	SAQ D							X	
8.4	User guidance on authentication practices	SAQ D							X	
8.7	Database authentication policy and procedure	SAQ D							X	
8.8	Security policies and operational procedures for identification and authentication	SAQ D							X	
9.3	Access control lists	SAQ D							X	
9.4	Visitor process	SAQ D							X	

CAMPUSGUARD

Required PCI DSS Documentation

PCI DSS Reference	Documentation Requirement	SAQ	SAQ A	SAQ A-EP	SAQ B	SAQ B-IP	SAQ C	SAQ C-VT	SAQ D	SAQ P2PE-HW
9.4.4	Visitor log	SAQ D							X	
9.5.1	Policies and procedures for reviewing offsite media locations	SAQ D							X	
9.6	Policies and procedures for distribution of media	SAQ A SAQ A-EP SAQ B SAQ B-IP SAQ C SAQ C-VT	X	X	X	X	X	X	X	
9.6.1	Policies and procedures for media classification	SAQ A SAQ A-EP SAQ B SAQ B-IP SAQ C SAQ C-VT	X	X	X	X	X	X	X	
9.6.2	Media distribution and tracking logs	SAQ A SAQ A-EP SAQ B SAQ B-IP SAQ C SAQ C-VT	X	X	X	X	X	X	X	
9.6.3	Management approval*		?	?	?	?	?	?	?	
9.7.1	Media inventory log	SAQ D							X	
9.8	Periodic media destruction policies and procedures	SAQ A SAQ A-EP SAQ B SAQ B-IP SAQ C SAQ C-VT	X	X	X	X	X	X	X	X
9.9.3	Training documentation for handling media in PCI DSS scope	SAQ B SAQ B-IP SAQ C SAQ D SAQ P2PE-HW			X	X	X		X	X
9.10	Security policies and operational procedures for restricting physical access to cardholder data	SAQ D SAQ P2PE-HW							X	X
10	Audit logs*									
10.4.1	Time configuration standards and process	SAQ D							X	
10.6.2	Risk assessment process and documentation (Same as 12.2)	SAQ A-EP SAQ C SAQ D		X			X		X	
10.8	Security policies and operational procedures for monitoring all access to network resources and cardholder data	SAQ D							X	
11.1	Methodology for detecting and identifying all unauthorized wireless access points	SAQ C SAQ D					X		X	
11.1.1	Inventory of wireless access points	SAQ C SAQ D					X		X	
11.1.2	Incident Response Procedure (Same as 12.10.1)	SAQ C SAQ D					X		X	
11.2.1	Internal quarterly Vulnerability scans	SAQ C SAQ D					X		X	
11.2.2	External quarterly vulnerability scans	SAQ A-EP SAQ B-IP SAQ C SAQ D		X		X	X		X	
11.3	Methodology for penetration tests	SAQ A-EP SAQ D		X					X	
11.3.1	External annual penetration scan	SAQ A-EP SAQ D		X					X	
11.3.2	Internal annual penetration scan	SAQ D							X	
11.3.4	Segmentation Controls	SAQ A-EP SAQ C SAQ D		X			X		X	
11.4	IDS/IPS vendor documentation	SAQ D							X	
11.5	File integrity monitoring logs	SAQ A-EP SAQ C SAQ D		X			X		X	
11.6	Security policies and operational procedures for security monitoring and testing	SAQ D							X	
12.2	Risk assessment process and documentation (Same as 10.6.2)	SAQ D							X	
12.3.1	Usage Policy for critical technologies	SAQ B SAQ B-IP SAQ C SAQ C-VT SAQ D			X	X	X	X	X	
12.6	Security awareness program	SAQ A-EP SAQ B SAQ B-IP SAQ C SAQ C-VT SAQ D		X	X	X	X	X	X	X
12.8.1	List of service providers	SAQ A SAQ A-EP SAQ B SAQ B-IP SAQ C SAQ C-VT	X	X	X	X	X	X	X	X
12.8.2	Written agreement between service providers and merchant	SAQ A SAQ A-EP SAQ B SAQ B-IP SAQ C SAQ C-VT	X	X	X	X	X	X	X	X
12.10.1	Incident Response Procedure (Same as 11.1.2)	SAQ A-EP SAQ B SAQ B-IP SAQ C SAQ C-VT SAQ D		X	X	X	X	X	X	X

Administration and Department Payment Card Policy

Payment Card Industry
Data Security Standard (PCI DSS)
PCI DSS Version 3.0

Contents

Revisions/Approvals

Ver. #	Changes By	Ver. date	Reason
2.2.1	O. Davies	04/26/2013	Separated procedures from policies.
2.2.2	J. Seguy	10/09/2014	Modified references to “institution” for consistency / ease of replacement

Purpose

This document and additional supporting documents represents {INSTITUTION NAME}'s policy to prevent loss or disclosure of customer information including credit card numbers. Failure to protect customer information may result in financial loss for customers, suspension of credit card processing privileges, and fines imposed on and damage to the reputation of the unit and the university.

PCI DSS

The PCI DSS is a mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express and JCB. These security requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council Web site (https://www.pcisecuritystandards.org)

In order to accept credit card payments, {INSTITUTION NAME} must prove and maintain compliance with the Payment Card Industry Data Security Standards. The {INSTITUTION NAME} Payment Card Policy and additional supporting documents provides the requirements for processing, transmission, storage and disposal of cardholder data of payment card transactions in order to reduce the institutional risk associated with the administration of credit card payments by university departments to ensure proper internal control and compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Visa Cardholder Information Security Plan (CISP)

Visa Inc. instituted the Cardholder Information Security Program (CISP) in June 2001, CISP is intended to protect Visa cardholder data–wherever it resides–ensuring that members, merchants, and service providers maintain the highest information security standard. In 2004, the CISP requirements were incorporated into an industry standard known as Payment Card Industry (PCI) Data Security Standard (DSS).

MasterCard Site Data Protection Program (SDP)

The SDP Program, with the PCI DSS as its foundation, details the data security requirements and compliance validation requirements to protect stored and transmitted MasterCard payment account data.

Scope/Applicability

The {INSTITUTION NAME} Payment Cards Policy applies to all faculty, staff, students, organizations, third-party vendors, individuals, systems and networks involved with credit card handling. This includes transmission, storage and/or processing of credit card numbers, in any form (electronic or paper), on behalf of {INSTITUTION NAME}.

Authority

UNIVERSITY policies fall within a greater hierarchy of laws, statutes and regulations. The Board has been authorized by the State to govern {INSTITUTION NAME}. The Board has delegated the authority to manage the UNIVERSITY to the President.

As a part of that management, the President, will direct the development and implementation of UNIVERSITY's policies and procedures.

Policy

It is the policy of {INSTITUTION NAME} to allow acceptance of payment cards as a form of payment for goods and services upon written approval from the University Controller. {INSTITUTION NAME} requires all departments that accept payment cards to do so only in compliance with credit card industry standards and in accordance with the procedures outlined in this policy document, the {INSTITUTION NAME} payment card procedures and other supporting documents.

Procedures and Other Supporting Documents

- {INSTITUTION NAME} - PCI Administration and Department Payment Card Procedures
- {INSTITUTION NAME} - Appendix 1 - PCI Payment Card Security Incident Response Plan
- {INSTITUTION NAME} - Appendix 2 - PCI Application for New Payment Card Merchants
- {INSTITUTION NAME} - Appendix 3 - PCI Annual Merchant Survey
- {INSTITUTION NAME} - Appendix 4 - PCI Payment Card Best Practices

Interpretations

The authority to interpret this policy rests with the {HEAD OF THE INSTITUTION} and the {INSTITUTION'S LEADERSHIP COMITTEE}.

Exclusions

Enter exclusions here.

Glossary

Term	Definition
Payment Card Industry Data Security Standards (PCI DSS)	The security requirements defined by the Payment Card Industry Security Standards Council and the 5 major Credit Card Brands: • Visa, MasterCard, American Express, Discover, JCB
Cardholder	Someone who owns and benefits from the use of a membership card, particularly a credit card.
Card Holder Data (CHD)	Those elements of credit card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date and the Service Code.
Primary Account Number (PAN)	Number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.
Cardholder Name	The name of the Cardholder to whom the card has been issued.
Expiration Date	The date on which a card expires and is no longer valid. The expiration date is embossed, encoded or printed on the card.
Service Code	The service code that permits where the card is used and for what.
Sensitive Authentication Data	Additional elements of credit card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN/PIN block.

Magnetic Stripe (i.e., track) data	Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.
CAV2, CVC2, CID, or CVV2 data	The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card- not-present transactions.
PIN/PIN block	Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
Disposal	CHD must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, USB storage devices,(Before disposal or repurposing, computer drives should be sanitized in accordance with the (Institution's) Electronic Data Disposal Policy). The approved disposal methods are: • Cross-cut shredding, Incineration, Approved shredding or disposal service
Merchant Department	Any department or unit (can be a group of departments or a subset of a department) which has been approved by the (institution) to accept credit cards and has been assigned a Merchant identification number.
Merchant Department Responsible Person (MDRP)	An individual within the department who has primary authority and responsibility within that department for credit card transactions.
Database	A structured electronic format for organizing and maintaining information that is accessible in various ways. Simple examples of databases are tables or spreadsheets.