Guideline 5.23.1.10 Payment Card Industry – Technical Requirements

Part 1. Purpose. This guideline emphasizes many of the minimum technical requirements necessary to comply with the Payment Card Industry Data Security Standards (PCI DSS). This is not a comprehensive list, and institutions within Minnesota State Colleges and Universities (system) should refer to the PCI-DSS requirements from the PCI Security Standards Council.

Part 2. Applicability.

Subpart A. This guideline applies to all institutions that accept Payment Cards (e.g. Credit Cards) by any means. Several Self Assessment Questionnaires (SAQs) are used to determine compliance; however identifying which one applies depends on the way payment cards are accepted and how PCI data is retained. Documents from the PCI Security Standards Council can be used to assist with this identification, however this table can be used to approximate which questionnaire should apply:

SAQ Validation Type	Description	SAQ: V1.2	PCI DSS Requirements
1	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.	A	13
2	Imprint-only merchants with no electronic cardholder data storage	B	26
3	Stand-alone terminal merchants, no electronic cardholder data storage	B	26
4	Merchants with POS systems connected to the Internet, no electronic cardholder data storage	C	41 + quarterly scans
5	All other merchants (not included in Types 1-4 above) and all service providers defined by a payment brand as eligible to complete an SAQ.	D	225 + quarterly scans

Subpart B. Requirements below have been categorized with an A, B, C, and/or D to identify to which institutions each requirement applies, based on which SAQ they are required to complete. SAQ D has the most requirements, while SAQ A has the fewest requirements.

Subpart C. It is highly recommended that business processes be reviewed first to determine if it is feasible to modify processes in a way that would enable the institution to fall into a category with fewer requirements.

Subpart D. This guidance applies to only the systems that are in scope for PCI, as defined by the PCI Security Standards Council.

Part 3. Guidelines.

Subpart A. Install and Maintain a Firewall Configuration to Protect Cardholder Data.

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ A	B	C	D
1	1.1.6	Establish firewall and configuration standards which include a change management process, network diagrams, administrative responsibilities, business justification for all rules / services / protocols / ports, and rules are reviewed at a minimum of every six months.				X
2	1.3.1	Firewall configuration must restrict ingress and egress traffic to only that which is necessary, ensures startup configuration files are secure, restricts and/or controls traffic between any wireless environment and the cardholder environment.				X
3	1.3, 1.3.4, 1.3.5, 1.3.6	Ensure the firewall allows systems within the cardholder environment to only communicate to/from the Internet via systems in the demilitarized zone (DMZ), only allows established connections (stateful traffic inspection), and prevents private addresses from being revealed on the Internet.			X	X
4	1.3.7	The database must be placed in an internal zone, segregated from the demilitarized zone (DMZ).				X
5	1.4	Mobile computers accessing the PCI environment must have a host-based/personal firewall installed.				X

Subpart B. Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters.

Item	*PCI DSS Requirement*	*Requirement Description*	*Applicable SAQ* *A*	*B*	*C*	*D*
1	2.1	Change vendor-supplied security defaults before installing the system or device onto the network.			X	X
2	2.2	Develop configuration standards for all system components, based on industry-accepted system hardening standards. Configuration standards must include:				X
2a	2.2.1	Only one primary function per server.				X
2b	2.2.2, 2.2.4	Disable unnecessary and/or insecure services, protocols, or other functionality.				X
2c	2.2.3, 2.1.1(b)	Configure system parameters securely.				X
2d	2.3	Encrypt all non-console administrative access.			X	X

Subpart C. Protect Stored Cardholder Data.

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ A	B	C	D
1	3.1(a), 3.1(b)	Develop a data retention and disposal policy which minimizes cardholder data to only that which is required for business, legal, and or regulatory purposes.				X
2	In lieu of multiple items in Requirement 3	Utilize only Payment Application Data Security Standard (PA-DSS) validated payment applications.			X	X
3	3.2, 3.2.1, 3.2.2, 3.2.3	Do not store sensitive verification data, such as the card verification code (a.k.a. CVV2, CVC2, CID, or CAV2), PIN, or the encrypted PIN block.		X	X	X

Subpart D. Encrypt Transmission of Cardholder Data Across Open, Public Networks.

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ A	B	C	D
1	4.1	Use strong encryption and security protocols when transmitting PCI data over open or public networks.			X	X
2	4.2	Do not send PCI data over end-user messaging technologies, such as e-mail, instant messaging, and chat.		X	X	X

Subpart E. Use and Regularly Update Anti-Virus Software or Programs.

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ A	B	C	D
1	5	Deploy, maintain, and update anti-malware software on all commonly affected systems.			X	X

Subpart F. Develop and Maintain Security Systems and Applications.

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ A	B	C	D
1	6.2(a), 6.2(b)	Establish a process to identify newly discovered security vulnerabilities, and use this to update configuration standards.				X
2	6.1(a)	Ensure all systems components and software have the latest security patches installed.			X	X
3	6.6	Review public-facing web applications annually, or install a web-application firewall in front of public-facing applications.				X
4	6.3, 6.5	Internally developed software should not be used in conjunction with PCI data.				X

Subpart G. Restrict Access to Cardholder Data by Business Need-to-Know.

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ A	B	C	D
1	7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access, and only to the level of access required.		X	X	X

Subpart H. Assign a Unique ID to Each Person with Computer Access.

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ			
			A	B	C	D
1	8.1, 8.2, 8.5.8	All users must have a unique ID which is, at a minimum, password protected.				X
2	8.5	User IDs must be securely issued and handled:				X
2a	8.5.1, 12.3.1	Authorization forms defining required access must be completed, approved by management, and filed				X
2b	8.5.2, 12.3.2	User identity must be verified prior to password resets				X
2c	8.5.3	First time passwords are unique, and must change immediately after the first use				X
2d	8.5.4	Terminated users have access revoked immediately				X
2e	8.5.5	Inactive accounts are disabled at least every 90 days				X
2f	8.5.6	Vendor maintenance accounts are enabled only during the time period needed, and immediately deactivated after use			X	X
2g	8.5.9	User passwords are changed at least every 90 days				X
2h	8.5.10, 8.5.11	Passwords are at least seven characters long and alpha-numeric				X
2i	8.5.12	Users cannot re-use one of the last four passwords				X
2j	8.5.13	User IDs are locked out after no more than six attempts				X
2k	8.5.14	Accounts are locked out for 30 minutes or until the administrator re-enables it				X
2l	8.5.15	Sessions idle for 15 minutes must require the user to re-enter the password				X
2m	8.5.16	All access to databases must be authenticated				X
3a	8.3	Two-factor authentication for remote access				X
3b	12.3.8	Automatically disconnect remote access connections after a specific period of inactivity				X
3c	12.3.10	When accessing cardholder data remotely, prohibit copy, move, and storage of data onto local hard drives and removable electronic media				X

Subpart I. Restrict Physical Access to Cardholder Data.

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ			
			A	B	C	D
1	9.1, 9.1.1(a), 9.1.1(b), 9.1.1(c), 9.4, 9.4(c)	Physically secure access to PCI data/processing facilities (excluding POS systems) sufficiently to identify individuals entering/exiting. Monitor and retain data for three months.				X
2	12.3.3	Maintain a list of computing devices (laptops, PDAs, PCs) and personnel with access				X
2a	12.3.4	Label computing devices with owner, contact information, and purpose				X
3	9.1.2, 9.1.3	Restrict physical access to network accessible jacks, wireless access points, gateways, etc.				X
4	9.2, 9.3, 9.3.1, 9.3.2, 9.3.3	Develop procedures to distinguish between employees and visitors. Visitor access must be authorized, logged, provided a badge or token, and surrender the badge or token upon departure.				X
5	9.5	Securely store media. Ensure a secure courier is utilized and management approves of transporting materials. Classify the media and maintain controls over location and access.	X	X	X	X
6	9.6	Securely destroy media or data when no longer needed for business or legal reasons.	X	X	X	X

Subpart J. Track and Monitor All Access to Network Resources and Cardholder Data.

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ A	B	C	D
1	10.1	Audit trails must link access to system components to an individual. Audit trails must include logging of:				X
1a	10.2.1	Individual access to cardholder data				X
1b	10.2.2	All actions taken by individuals with root/administrative privileges				X
1c	10.2.3	Access to audit trails				X
1d	10.2.4	Invalid access attempts				X
1e	10.2.5	Use of identification and authorization mechanisms				X
1f	10.2.6	Initialization of the audit log				X
1g	10.2.7	Creation and deletion of system-level objects				X
1h	10.3	For each event:				X
1h(i)	10.3.1	User identification				X
1h(ii)	10.3.2	Type of event				X
1h(iii)	10.3.3	Date and time				X
1h(iv)	10.3.4	Success or failure				X
1h(v)	10.3.5	Origination of event				X
1h(vi)	10.3.6	Identity of affected data, system component, or resource				X
2	10.4	System clocks must be synchronized to multiple external known good sources				X
3	10.5, 10.5.1, 10.5.2, 10.7	Audit trails must be secured against unauthorized viewing or modifications, with one year of data being retained, and the previous three months immediately available for analysis				X
4	10.6	Audit trails of intrusion detection or intrusion prevention systems (IDS/IPS) and authentication, authorization and accounting activities on all system components must be reviewed daily				X

Subpart K. Regularly Test Security System and Processes.

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ			
			A	B	C	D
1	11.1	Test for presence of wireless access points at least quarterly, or deploy wireless intrusion detection or intrusion prevention systems			X	X
2	11.2	Run internal vulnerability scans at least quarterly, and after significant changes			X	X
3	11.2	Have an external vulnerability scan conducted by a PCI Approved Scanning Vendor (ASV) at least quarterly			X	X
4	11.3(a)	Have an annual internal and external penetration test covering both the network and application layer conducted by a qualified and independent party				X
5	11.4(a), 11.4(b)	Monitor all traffic in the cardholder environment with intrusion detection / intrusion protection systems, ensuring signatures stay up to date and appropriate individuals are notified of suspected compromises				X
6	11.5(a), 11.5(b)	Use file integrity monitoring software at least weekly to alert personal to unauthorized changes in critical system files, such as system executables, application executables, configuration files, and audit / log files				X

Subpart L. Maintain an Information Security Policy.

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ A	B	C	D
1	12.1.2, 12.1.3	Conduct an annual formal risk assessment that identifies threats and vulnerabilities, and update as the environment changes				X
2	12.2	Create documented operational procedures to ensure policy items are properly executed				X
3	12.5	Assign an individual or team the information security management responsibilities including:				X
3a	12.5.1	Establishing, documenting, and distributing security policies and procedures				X
3b	12.5.2	Monitoring, analyzing, and distributing security alerts and information				X
3c	12.5.4	Administer user accounts				X
3d	12.5.5	Monitor and control all access to data				X
4	12.6.1	Provide security awareness training to employees upon hire and at least annually thereafter		X	X	X
5	12.6.2	Employees must annually acknowledge reading and understanding security policies and procedures				X
6	12.7	Conduct background checks for all potential employees with access to more than one credit card number at a time or to the cardholder data environment				X
7	12.8	Manage service providers, at a minimum:	X	X	X	X
7a	12.8.1	Maintain a list of providers	X	X	X	X
7b	12.8.2	Maintain a written agreement acknowledging responsibility for securing cardholder data	X	X	X	X
7c	12.8.3	Perform proper due diligence prior to engagement of service providers	X	X	X	X
7d	12.8.4	Monitor the service providers' PCI DSS compliance status	X	X	X	X
8	12.9.1(a)	Establish, document, and distribute security incident response and escalation procedures		X	X	X
8a	12.9.1(b)	Include roles, responsibilities, communication, and contact strategies, including notification of the payment brands				X
8b	12.9.1(b)	Include business recovery and continuity procedures				X
8c	12.9.1	Include data back-up processes				X
8d	12.9.1	Include analysis of legal requirements for reporting requirements				X

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ A	B	C	D
8e	12.9.1	Reference or include incident response procedures from the payment brands				X
8f	12.9.2	Test the plan at least annually				X
8g	12.9.3	Designate specific personnel to be available 24x7 to respond to alerts				X
8h	12.9.4	Provide appropriate incident response training to staff				X
8i	12.9.5	Include alerts from intrusion detection system / intrusion protection system (IDS, IPS) and file-integrity monitoring systems				X
8j	12.9.6	Include a process to evolve the incident response plan with lessons learned and industry developments				X

Subpart M. Policy amendment. The system office will review and update subparts A thru L of System Guideline 5.23.1.10 annually to reflect changes in the PCI DSS. No further approval required.

Part 4. Definitions.

Subpart A. Access. Approved authorization to view, modify or delete system information/data. Access shall be authorized to individuals or groups of users depending on the application of law, system policy or guideline. Technical ability to access information is not necessarily equivalent to legal authority.

Subpart B. Approved Scanning Vendor (ASV). Organizations certified by the PCI Security Standards Council to validate adherence to PCI DSS by performing vulnerability scans of Internet facing environments of merchants and service providers.

Subpart C. Authorized Individual. Employee, consultant, volunteer or other individual who is approved and allowed access to information within the system to perform an activity on behalf of an institution. The individual may have access to any class of information, according to policy.

Subpart D. Breach. Any accidental or deliberate non-compliance with policies or other security controls.

Subpart E. Card Verification Code (CVV2, CVC2, CID, or CAV2). A three or four digit value printed on the payment card, but not embossed. It is usually found on the back of the card in or near the signature strip, but is on the front of American Express cards.

Subpart F. Data. Information collected, stored, transferred or reported for any purpose, whether in computers or in manual files. Data can include: financial transactions, lists, identifying information about people, projects or processes, and information in the form of reports. Because data has value,

and because it has various sensitivity classifications defined by federal law and state statute, it must be protected.

Subpart G. Demilitarized Zone (DMZ). Networks containing filtered anonymous or authenticated Internet accessible access devices or servers. Examples may include but are not limited to web email servers, instant messaging servers, virtual private network (VPN) or remote access servers/services, etc.

Subpart H. Electronic Cardholder Data. Data that must be protected by the PCI DSS defined as either all of the information found on the full magnetic strip, or the PAN plus any of the following: cardholder name, expiration data, service code.

Subpart I. Employee. Full-time and/or part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site.

Subpart J. May. A statement that is optional.

Subpart K. Merchant Bank. The merchant bank is a financial institution which offers financial services to organizations and individuals. The requirement to be PCI compliant is typically found in the contracts between merchant banks and entities with credit card processing accounts (a.k.a. merchant accounts).

Subpart L. Must. A statement that is required for a compliant implementation.

Subpart M. Must Not. A statement that is prohibited for a compliant implementation.

Subpart N. Payment Application Data Security Standard (PA DSS). Provides the definitive data standard for software vendors that develop payment applications.

Subpart O. Primary Account Number (PAN). Payment card number that identifies the issuer and the particular cardholder account.

Subpart P. Payment Card Industry Data Security Standards (PCI DSS). A standard that defines controls that must be in place around cardholder data. A contractual agreement with the merchant bank requires that all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands comply with this standard.

Subpart Q. Payment Brand. One of the brands of credit cards (e.g. MasterCard, Visa, American Express, etc).

Subpart R. Payment Cards. Cards containing payment data, used in purchasing goods and services. Typically referred to as either credit cards or debit cards.

Subpart S. PCI Data. Payment card information, as defined by the Payment Card Industry Security Standards Council. PCI data is subject to the PCI Data Security Standards. Such information includes payment account numbers (PANs) plus expiration dates, cardholder names, or verification codes, or data stored on track 2 of the payment card.

Subpart T. PCI Security Standards Council. The organization responsible for assembling, updating, and maintaining the PCI-DSS.

Subpart U. POS System. Point-of-Sale system.

Subpart V. Self Assessment Questionnaire. Merchants that process fewer than a given amount of transactions annually are able to complete a Self-Assessment Questionnaire (or SAQ) to demonstrate compliance. Each payment brand has individual requirements, but as an example, Visa allows organizations to complete a SAQ if they process fewer than six million Visa transactions annually.

Subpart W. Should. A statement that is recommended but not required.

Subpart X. Should Not. A statement of practices that are not recommended but which may be followed.

Subpart Y. Stateful Inspection. Firewall capability that provides enhanced security by keeping track of communications packets. Only incoming packets with a proper response ("established connections") are allowed through the firewall.

Subpart Z. System. Denotes the Minnesota State Colleges and Universities Board of Trustees, the system office, the state colleges and universities, and any part or combination thereof.

Subpart AA. Token. A device that performs dynamic authentication.

Subpart BB. Web Application Firewall. An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation.

Part 5. Authority.

Subpart A. Board policies 1A.1 and 5.23 delegate authority to the vice chancellor to develop system guidelines, consistent with Board policy and system procedure, for the purposes of implementing Board policy 5.23.

Approval Date: 05/17/10,
Effective Date: 05/17/10,

Date and Subject of Revision:
1/25/12 – The Chancellor amends all current system procedures effective February 15, 2012, to change the term "Office of the Chancellor" to "system office" or similar term reflecting the grammatical context of the sentence.