****

**Payment Card Industry (PCI) Data Security Standard (DSS):**

**Ensuring Compliance When Drafting RFPs and Contracts**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. **What is PCI DSS?**

PCI DSS is a set of global data security standards designed to protect payment card account numbers. Any payment card (credit, debit, prepaid, stored value, gift or chip) bearing the logo of one of five payment brands is required to be protected as prescribed by the standards. The brands are: American Express, Discover, JCB, MasterCard and Visa. Specifically, PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. If PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply. Storage includes any type of recording (paper or electronic.)

1. **When drafting any RFP or initiating or renewing any agreement, ask:**

 *“Will the services sought under the RFP or procured under the contract involve the storage, processing or transmittal of payment card account numbers?”*

* ***If the answer is yes,*** PCI DSS requirements are applicable. You need to take steps to include specific references to PCI DSS in both the RFP and the subsequent agreement and ensure that any vendor selected meets the referenced obligations.
* ***If the answer is no,*** PCI DSS requirements are not applicable.
* ***If you are unsure,*** contact your campus CFO.
1. **What specific terms need to be incorporated into existing contracts, RFPs and new agreements?**
* **Existing contracts.** Approach vendor to amend contract to add PCI DSS

responsibilities. Amendments must be in writing and signed by both parties. A form amendment is provided on the Office of the Chancellor Finance division Web site. Contact the Office of General Counsel or the Attorney General’s Office with questions.

* **RFP and New Contracts:** Include following terms:

|  |
| --- |
| “Vendor agrees to establish security procedures to protect cardholder data and comply with the Payment Card Industry Data Security Standard. Vendor can find details of the PCI DSS at <https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml> . “Vendor agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of cardholder data. In the event of a breach of any of Vendor's security obligations or other event requiring notification under applicable law, Vendor agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless and defend Minnesota State Colleges and Universities and [College or University] and its trustees, officers, and employees from and against any claims, damages, or other harm related to such a breach.” |

1. **How do I determine whether a vendor or prospective vendor is PCI-compliant?**

In order to accept payment cards, a merchant (your vendor) must enter into a contract with its acquiring bank, which, in turn, has contracts with the payment card brands. These contracts require the merchant to follow PCI data security standards. The standards include, among other things, maintaining a secure IT environment, training staff, and developing policies and procedures to keep data secure.

Initially, an organization can establish that it is PCI-compliant via either of two forms developed by the PCI DSS Council: “Attestation of Compliance” form or “Confirmation of Report Accuracy” form.

Note, however, compliance is a moving target. An organization that is PCI-compliant one day may become non-compliant the next by making changes, either to business practices or by reconfiguring its IT environment. Because processes, personnel and IT resources do change over time, it is important to have ongoing discussions with vendors regarding data security and PCI DSS compliance.

To satisfy the requirements of PCI, a merchant [your vendor] must complete the following steps:

* Identify its Validation Type as defined by PCI DSS – see below.  This is used to determine which Self Assessment Questionnaire is appropriate for your business.

****

* Complete the Self-Assessment Questionnaire according to the instructions in the Self- Assessment Questionnaire Instructions and Guidelines.
* Complete and obtain evidence of a passing vulnerability scan with a PCI DSS Approved Scanning Vendor (ASV).  Note scanning does not apply to all merchants.  It is required for Validation Type 4 and 5 – those merchants with external facing IP addresses. Basically if a merchant electronically stores cardholder information or if the merchant’s processing systems have any internet connectivity, a quarterly scan by an approved scanning vendor is required.
* Complete the relevant Attestation of Compliance in its entirety (located in the SAQ tool).
* Submit the SAQ, evidence of a passing scan (if applicable), and the Attestation of Compliance, along with any other requested documentation, to the merchant’s acquirer.

The PCI Council maintains lists of compliant software and service providers. See links below.

**To see a sample Attestation of Compliance form, go to:**

<https://www.pcisecuritystandards.org/saq/docs/aoc_merchants.doc>

[See attached “Confirmation of Report Accuracy” and “PCI Attestation for Online Compliance for Merchants”]

**To check whether software you plan to purchase is PCI compliant, go to:**

<https://www.pcisecuritystandards.org/security_standards/vpa/>)

**To check whether a service provider is compliant, go to:**

<http://usa.visa.com/merchants/risk_management/cisp_service_providers.html>

**For fuller information on the PCI Security Council (Main PCI Reference), go to:**

[https://www.pcisecuritystandards.org/index.shtml](https://www.pcisecuritystandards.org/index.shtml%20)

**For free PCI Training Webinars, go to:**

[http://www.mastercard.com/us/merchant/support/merchant\_education.html](http://www.mastercard.com/us/merchant/support/merchant_education.html%20)

Revised OGC / March 2010