

PCI DSS Text for Third Party Vendor Proposals/Agreements

Include the following provision in proposals and agreements involving vendors with access to University of Arizona credit cardholder data or sensitive authentication data, as defined by the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS AND PABP COMPLIANCE

Contractor is currently certified to be in compliance with the PCI Security Standards Council's Payment Card Industry Data Security Standard, including PCI DSS Version 1.1 Requirement 12.10 for processors and service providers, and Appendix A for Hosting Providers, by a qualified security assessor (QSA) and approved scanning vendor (ASV), as applicable. Any changes in Contractor's certification require prompt written notification to the client. Contractor agrees to continue to meet all PCI DSS requirements and to validate compliance annually according to the credit card industry rules, which include but are not limited to the Payment Card Industry Data Security Standard. Contractor will also provide written evidence of this compliance to the University of Arizona annually. If applicable, Contractor agrees that its electronic check processing functionality will comply with the appropriate NACHA-The Electronic Payment Association provisions.

Applications purchased from a third party that will be used by a Merchant to store, process or transmit sensitive cardholder data must be Payment Application Best Practices (PABP) certified. This certification ensures that the application is compatible with Payment Card Industry Data Security Standard requirements. Information about PABP validation is available from Visa at (http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html).