Standard: TS0011.05	Category: Technical Security	Version Date: 2/15/2008
Title: E-Commerce Applications and Card Holder Data Security		Effective Date: 04/01/2008
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review: 02/15/2008
Review Resp: HSC Chief, Information Security		Next Review: 02/2010

Purpose:

To provide a source of recommended security controls for E-Commerce software and Card Holder Data.

References:

1. SPICE Policy TS0011 Software Security Compliance.
2. UF Guidelines to Develop Applications for Secure Deployment.
   http://www.it.ufl.edu/policies/guidelines.html
3. UF Implemented Web Payment gateway (IPAY) Documentation
   Contact Keith Hay-Roe, Student Financial Services Technical Lead, 273-1453,
   khayroe@ufl.edu
4. Payment Card Industry Data Security Standard
5. https://www.pcisecuritystandards.org/
6. MasterCard and VISA Lists of Compliant Service Providers
   http://www.mastercard.com/us/sdp/serviceproviders/compliant_serviceprovider.html
   http://usa.visa.com/merchants/risk_management/
7. Payment Card Industry Merchant Education Program
   http://www.mastercard.com/us/sdp/education/pci%20merchant%20education%20program.html
8. SPICE Evaluation Program
   a. Products and Services Security Evaluation Procedures
   b. EV0001 – Information Technology Products and Services Security Evaluation Form

   https://security.health.ufl.edu/isa_ism/eval_artifacts.shtml
9. University of Florida Annual Report; List of UF HSC Affiliates

Standard:

1. Any UF HSC Unit that has implemented a system that captures, transmits, processes or stores full 'primary account numbers' (aka full credit card numbers) in the HSC information computing environment must validate its compliance to the Payment Card Industry Data Security Standard (PCI DSS). Validation requirements depend upon the credit card transaction volume of the UF HSC Unit and typically involves:

   a. Annual PCI Self-assessment Questionnaire, and
   b. Quarterly Network Scan, and
   c. Remediation where standards are not being met
2. To minimize the cost of validation and remediation mentioned above, and to avoid the risk of costly penalties in the event of a security breach:
   a. HSC Units are encouraged to use PCI DSS certified credit card transaction service providers in lieu of acquiring or developing their own hardware and software that captures, stores, processes or transmits 'primary account numbers' (aka full credit card numbers) in the HSC computing environment. Such contracted services might include an outsourced eCommerce web site or an outsourced web site hosting service; a secure financial transaction gateway service; a merchant payment processing service, etc. The HSC Unit must obtain proof of the service provider's PCI DSS certification on an annual basis. Both VISA and MasterCard publish a current list of Compliant Service Providers on their respective web sites (see references above) which can serve as proof of certification.
   b. All UF HSC Units, with the exception of HSC affiliates, desiring to accept payment for financial transactions electronically via the internet using E-commerce, are required to process all sales transactions through the Office of Finance and Administration implemented web payment gateway (IPAY). See references above for IPAY documentation.
3. The security standards listed above are elaborated in the SPICE products and services security evaluation process and procedures which should be performed prior to resource investment (i.e. buying a product, expending integration effort, or writing code) in new credit card handling software or services. The security evaluation process will help determine the extent to which the PCI DSS apply to the Unit's planned implementation. The procedures and evaluation form are in the references above.
4. The recommendations generated from the security evaluation must be completed prior to use of the software on production systems, prior to use by users and prior to interaction with Restricted or Sensitive information unless otherwise stated in the evaluation report.

.