College of Charleston
Information Security
Vendor Worksheet

Please complete and return as a separate pdf document when submitting your proposal.

Vendor and Product Name:

Vendor Technical Contact:

IT Technical Contact:

Department Contact:

Information Security Engineer:

Network Security Engineer:

Application / Service Security

Does your application function with Virtual Machines?

Does your application support being virtualized?

Will you application support integration with other authentication and authorization system (e.g. Active Directory or CAS)

Will your application support external authentication services (e.g. Active Directory, LDAP) in place of local authentication? Mixed?

Describe all authentication methods the system supports.

Can user access be customized to allow read-only access, update access or no-access to specific types of records, record attributes, components or functions?

Are security roles fully customizable?

How is user security administration performed?

Have you experienced a breach?

Database

Do you currently use encryption in you database?

Doers the database support encryption of specified data elements in Storage?

What type of encryption is supported?

Application Architecture and Revisions

Describe the facilities available in the system to provide separation of duties between security administration and system administration functions.

Describe the overall application architecture, including applicable diagrams. Include a full description of the data communications architecture for all components of the system.

Describe the recommended network security architecture for implementation of the system components. Include diagrams that expose any requirements for external security devices.

Describe all web-enabled features and functionality of the system.

Describe additional software / products necessary to implement a functional system.

How are critical patches applied?

Are updates to the product released on a schedule?

Will we be notified of major changes to your environment that could impact our security posture?

Can you provide a demo version for testing?

Information and Network Security

Does the system provide data input validation and error messages?

Are audit logs available that include login, logout, action performed and source IP address?

Describe the system capability to log security / authorization changes as well as user and administrator security events (e.g. login failures, access denied, changes accepted) and all requirements necessary to implement logging and monitoring of the system.

Hosted Systems

Is the application hosted in a high availability environment?

Are you utilizing a Stateful Packet Inspection (SPI) firewall? If "yes", are you utilizing an IDS/IPS system?

Are you using a Web Application firewall?

Can you enforce password / passphrase aging requirements?

Can you enforce password / passphrase complexity requirements?

Are user accounts passwords / passphrases visible in administration modules? User data?

Are user accounts passwords / passphrases stored encrypted? What is the algorithm?

Are employees allowed to remove customer data in any form?

Do your physical security controls include video monitoring, restricted access areas, mantraps, card access controls, etc.?

Do you have a documented Patch Management process?

Can you accommodate encryption requirements using Open Standards?

Can you accommodate authentication utilizing Open Standards?

Describe your cryptographic key management process. (Generation, Exchange, Storage, Safeguarding, use, vetting, and replacement)

Have your developers been trained in Secure Coding Techniques?

Are information security principles designed into the product lifecycle?

Do you have a documented System Development Life Cycle?

Do you have a formal Incident Response plan?

Will you comply with South Carolina Breach Notification Laws?

Have you viewed and will you comply with the College of Charleston IT Policies?

Was your application developed using Secure Coding techniques?

Are your applications scanned externally for vulnerabilities?

Are your systems scanned externally for vulnerabilities?

Are your applications scanned for vulnerabilities prior to new releases?

What tool or tools were used to scan for vulnerabilities?

What was the date of your last external assessment?

Can we review the results of security scans, such as ISS, Nessus, AppScan, etc.?

PCI DSS

Does the application store, process, or transmit credit card data?

Are you PCI DSS compliant?

Do you have a certificate of compliance?

Is the certificate of compliance current? Issued within the last calendar year?

Are you classified as a service provider?

Are you on the list of VISA approved service providers?

Are you classified as a merchant? If so, what level (1,2,3,4).

Describe the architecture employed by the system to verify and authorize credit card transactions. What payment processors/gateways does the system support?

Can the application be installed in a PCI DSS compliant manner?

Is the application listed as an approved PA-DSS (**Payment Application Data Security Standard**) application?

Include documentation describing the systems' abilities to comply with Payment Card Industry Data Security Standards (PCI DSS) and any features or capabilities of the system that must be added or changed