Fairfax County Project Proposal Matrix for Meeting Information Technology Security Policy Requirements

October 2017

Introduction

The Fairfax County Project Proposal Matrix for Meeting Information Technology Security Policy Requirements is required as an attachment for information technology responses to Request for Proposal (RFP) processes initiated by Fairfax County. It is intended to assist Fairfax County with soliciting vendor responses that identify the requirements of the Fairfax County Information Technology Security Policy. The clear identification of each element is required by Fairfax County in order to sustain and ensure a solid foundation for the development and implementation of secure information technology practices within Fairfax County Government. **Vendors with access to Fairfax County information resources are required to abide by all policies and procedures of Fairfax County Government.**

The RFP Security Matrix has been divided into four main sections. A response is required depending on the proposed solution/service provided by the vendor.

- ***Section A*** *is to provide basic information regarding the proposed solution*
- ***Section B*** *is relevant to Cloud/Hosted services, or hybrid Cloud services, in which solution will be located in non-County datacenters.*
- ***Section C*** *is applicable to traditional on-premises solutions which will be located in Fairfax County datacenters under control by Fairfax County personnel.*
- ***Section D*** *requires responses regardless if solution is a cloud/hosted solution or traditional on-premises solution. This section covers general functional security capabilities inherent to the solution.*

How to Use the Security Template

Each section has multiple columns:

1. Standard
This section includes the requirement that needs to be addressed. It can take the form of a question or a statement.

2. Compliance
The responder shall provide a high level response to the Standard. The answers can be YES, NO, And N/A. The responder should check one of the three boxes to indicate their solution's capability. Responders can provide a high level explanation of answers in the "Comments/Additional Information" section.

3. Comments/Additional Information
In this section the responder should provide any additional information required to answer the question.

References:
The Fairfax County Information Technology Security Policy and the HIPAA Security Standards. This vendor RFP template was based upon similar work approved for public distribution by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) in August 2003.

SECTION A: Please complete the following section for proposed CLOUD, HYBRID SERVICES, and ON-PREMISES SOLUTIONS

	DESCRIPTION OF PROPOSED SOLUTION	COMMENTS/ADDITIONAL INFORMATION
A.1	Requesting County Agency:	
A.2	System Name/Title:	
A.3	Vendor/Developer:	
A.4	RFP Reference Number (if Applicable):	
A.5	Is proposed application or service a cloud-based or on-premises solution?	☐ Vendor-hosted ☐ On-Premises ☐ BOTH:
A.6	Please identify **server application** components supported to include software, middleware, authentication and user directory options, and third party supporting software or middleware.	☐ Web application ☐ Database ☐ Active Directory Integration ☐ 3rd-party middleware ☐ Other Application ☐ Windows Server OS ☐ Unix/Linux Please provide additional information below:
A.7	Please describe any **client application** components to include client software, and any third party supporting software or middleware for solution to function.	☐ Client application ☐ Internet Explorer ☐ Third-party Plugins Please provide additional information below:
A.8	Please indicate which system development lifecycle and security standards your organization adheres to?	
A.9	Please specify any database versions that support the application.	☐ Oracle ☐ Microsoft SQL Server ☐ Other ☐ N/A Please specify supported release versions and other additional information below:
A.10	Please specify any user access directory and external authentication requirements to support the application.	☐ Local application user directory ☐ Active Directory ☐ Other LDAP ☐ N/A Please provide additional information below:

SECTION B: Please complete the following for proposed CLOUD/HOSTED OR HYBRID SERVICES

	STANDARDS	COMPLIANCE	COMMENTS/ADDITIONAL INFORMATION
B.1	Payment Card Industry Data Security Standard (PCI-DSS) If applicable, is your organization and the proposed solution compliant with PCI-DSS? Provide evidence of industry certification of compliance.	☐ Yes ☐ No ☐ N/A	Provide additional information below:
B.2	Health Insurance Portability and Accountability Act (HIPAA) If applicable, is your organization and the proposed solution compliant with HIPAA? Provide evidence of industry certification of compliance or other relevant documentation, if available.	☐ Yes ☐ No ☐ N/A	Provide additional information below:
B.3	Personally-Identifiable Information (PII) If applicable, is your organization and the proposed solution compliant with requirements to secure PII? Provide evidence of compliance, if applicable.	☐ Yes ☐ No ☐ N/A	Provide additional information below:
B.4	Does the organization maintain a formal information security program that identifies management, operational, and technical controls to ensure the confidentiality, integrity, and availability of information systems and data and validates those controls?	☐ Yes ☐ No	Provide additional information below:
B.5	Does organization maintain an active vulnerability management program to protect systems from known vulnerabilities?	☐ Yes ☐ No	Provide additional information below:
B.6	Does organization validate and test implemented security controls? Please describe methods whether through internal or third-party audits, vulnerability assessments, penetration testing, etc.?	☐ Yes ☐ No	Provide additional information below:

B.7	Does the organization's solution use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, etc.) to safeguard information data during transmission between networks?	☐ Yes ☐ No	Provide additional information below:
B.8	Does the organization's proposed solution maintain a defense-in-depth security architecture incorporating intrusion detection, firewalls, and other network security monitoring and access control mechanisms?	☐ Yes ☐ No	Provide additional information below:
B.9	Does the organization provide adequate controls to protect against malicious code in hosted environment?	☐ Yes ☐ No	Please describe controls.
B.10	Does the organization protect data by implementing access control mechanisms to limit access to data to personnel whose job requires such access?	☐ Yes ☐ No ☐ ALT	Provide additional information below:
B.11	Does the proposed solution uniquely identify and authenticate all users?	☐ Yes ☐ No	Provide additional information below:
B.12	Does the organization protect data by implementing an auditing and systems monitoring program to identify and alert of unauthorized access or transactions?	☐ Yes ☐ No	Provide additional information below:
B.13	Does the organization restrict physical access to systems housing customer data and is the access audited?	☐ Yes ☐ No	Provide additional information below:

B.14	Will County data be encrypted at rest in the proposed solution?	☐ Yes ☐ No	Provide additional information below:
B.15	Has the organization implemented data retention and disposal policies, procedures and processes to limit data storage amount and retention time to that which is required for legal, regulatory, and business requirements?	☐ Yes ☐ No	Provide additional information below:
B.16	Does the organization maintain formal electronic data destruction procedures in the event of customer termination of contract?	☐ Yes ☐ No	Provide additional information below:
B.17	Are the data centers in which County data would reside located only in United States or its territories? If no, please explain.	☐ Yes ☐ No	Provide additional information below:
B.18	Are the organization's hosted application or resources maintained in a multi-tenant environment or platform in which County data is co-mingled with other entities, or dedicated infrastructure for County-specific resources?	☐ Yes ☐ No	Provide additional information below:
B.19	Does the organization maintain high availability of resources available to customers and document and define specific service availability level agreements?	☐ Yes ☐ No	Provide additional information below:
B.20	Does the organization maintain an incident response plan including strategy for notifying customers in the event of a breach and compromise of customer information? Is this incident response plan regularly tested?	☐ Yes ☐ No	Provide additional information below:

B.21	Does the organization maintain a formal Business Continuity/Disaster Recovery Plan? Does organization perform regular exercises to test the effectiveness of the plan?	☐ Yes ☐ No	Provide additional information below
B.22	Does the organization maintain disaster recovery procedures to assist in preventing interruption of system use?	☐ Yes ☐ No	Provide additional information below:
B.23	Does the organization maintain cyber security risk insurance?	☐ Yes ☐ No	Provide additional information below
B.24	Is the organization compliant with legal restrictions on the use of copyright material, ensuring that only software developed by the organization, or licensed or provided by the developer to the organization, is used?	☐ Yes ☐ No	Provide additional information below
B.25	Do all vendor employees and sub-contractors successfully complete a background investigation upon hire?	☐ Yes ☐ No	Provide additional information below

SECTION C: Please complete the following for proposed ON-PREMISES SYSTEMS

	STANDARDS	COMPLIANCE	COMMENTS/ADDITIONAL INFORMATION
C.1	Payment Card Industry Data Security Standard (PCI-DSS) If applicable, is the solution compliant with PCI-DSS? Please provide evidence of industry certification of compliance.	☐ Yes ☐ No ☐ N/A	Provide additional information below:
C.2	Health Insurance Portability and Accountability Act (HIPAA) If applicable, is the solution compliant with HIPAA? Please provide evidence of industry certification of compliance.	☐ Yes ☐ No ☐ N/A	Provide additional information below:
C.3	Personally-Identifiable Information (PII) If applicable, is the solution compliant with requirements to secure PII? Provide evidence of compliance, if applicable.	☐ Yes ☐ No ☐ N/A	Provide additional information below:
C.4	Does the organization maintain an active vulnerability management program to identify and remediate vulnerabilities in the system/application which is implicated throughout the product lifecycle?	☐ Yes ☐ No	Provide additional information below:
C.5	Does the organization test and validate security controls implemented within the system/application? Please describe methods whether through internal or third-party audits, vulnerability assessments, penetration testing, etc.?	☐ Yes ☐ No	Provide additional information below:
C.6	Does the organization's application/system use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, etc.) to safeguard information data during transmission?	☐ Yes ☐ No	Provide additional information below:
C.7	Does the proposed solution uniquely identify and authenticate all users (no anonymous access)?	☐ Yes ☐ No	Provide additional information below:
C.8	Will County data be encrypted at rest in the proposed solution?	☐ Yes ☐ No	Provide additional information below:

C.9	Does the proposed system/application maintain built-in high-availability features?	☐ Yes ☐ No	Provide additional information below:
C.10	Does organization's proposed solution include disaster recovery features and recommended practices specific to the solution to allow for the continuation of operations in the event of a disaster?	☐ Yes ☐ No	Provide additional information below:
C.11	Is the organization compliant with legal restrictions on the use of copyright material, ensuring that only software developed by the organization, or licensed or provided by the developer to the organization is used for customer's systems?	☐ Yes ☐ No	Provide additional information below:

SECTION D: Vendors must complete the following section for both CLOUD and ON-PREMISES SOLUTIONS

	GENERAL FUNCTIONAL SECURITY	COMPLIANCE	COMMENTS/ADDITIONAL INFORMATION
	Password Controls		
D.1	Does the system enforce strong passwords to include minimum length and combination of alpha and numeric characters?	☐ Yes ☐ No	Current Minimum: ___ Current Maximum: ___
D.2	Can user passwords be automatically changed or account disabled after a period of inactivity has passed?	☐ Yes ☐ No	Current Change Interval: ___
D.3	Can system force users to change default passwords following the initial set up or resetting of the password?	☐ Yes ☐ No	Provide additional information below:
D.4	Can the system prevent auto logon, application remembering, embedded scripts, and hard-coded passwords in software?	☐ Yes ☐ No	Provide additional information below:
D.5	Does system maintain a history of previously used passwords to prevent reuse?	☐ Yes ☐ No	Current Value: ___
D.6	Does the system allow for users to change their own passwords at their discretion?	☐ Yes ☐ No	Provide additional information below:
D.7	Does the system disable accounts after a specified number of consecutive invalid login attempts?	☐ Yes ☐ No	Current # Attempts: ___
D.8	Does system automatically activate a session termination or lock if user remains idle or inactive for a determined period of time?	☐ Yes ☐ No	Default Auto logoff Time:___
D.9	Are passwords entered in a non-display field to access application/system?	☐ Yes ☐ No	Provide additional information below:

D.10	Are passwords encrypted in storage and transmission? Please identify strategy to secure passwords to include encryption algorithm, key size, and use of salted and password hashing.	☐ Yes ☐ No	Provide additional information below:
D.11	Does system supports multi-factor authentication?	☐ Yes ☐ No	Provide additional information below:

	APPLICATION TECHNICAL CONTROLS	COMPLIANCE	COMMENTS/PLANS FOR MEETING COMPLIANCE
	Security Administration		
D.12	Does system log unauthorized access attempts by date, time, User ID, device and location?	☐ Yes ☐ No	Provide additional information below:
D.13	Does system maintain an audit trail of all security maintenance performed by date, time, User ID, device and location and information is easily accessible?	☐ Yes ☐ No	Provide additional information below:
D.14	Does system provide security reports of users and access levels?	☐ Yes ☐ No	Provide additional information below:
D.15	Does system maintain role-based group and user access control based on business functional requirements?	☐ Yes ☐ No	Provide additional information below:
D.16	Does system provide the capability to place security controls on each system module and on confidential and critical levels within each module?	☐ Yes ☐ No	Provide additional information below:
D.17	Does system provide capability to restrict access to particular records within the system, based on User ID and groups?	☐ Yes ☐ No	Provide additional information below:
D.18	Is on-site training and sufficient supporting reference materials related to security administration available to provide to County if solution is selected?	☐ Yes ☐ No	Provide additional information below:
D.19	Can system and security logs be archived and recalled as needed?	☐ Yes ☐ No	Provide additional information below:

	APPLICATION TECHNICAL CONTROLS	COMPLIANCE	COMMENTS/ADDITIONAL INFORMATION
	Networking		
D.20	Has the System configuration/architecture (i.e., hardware, wiring, display, network, and interface) been documented in proposal?	☐ Yes ☐ No	Provide additional information below:
D.21	Does your solution require data transmission between multiple solution provider networks? For example, data transmission requirements between Fairfax County networks and vendor-controlled networks, or vendor and sub-contractor networks?	☐ Yes ☐ No	Describe methodology and requirements
D.22	Is there a requirement for vendor to access system remotely from the internet?	☐ Yes ☐ No	Please describe remote access requirements and any built-in features.
D.23	For management and vendor support, can the system support secure remote access such as multi-factor authentication?	☐ Yes ☐ No	Provide additional information below:
D.24	Is the system compatible with mainstream anti-virus and endpoint protection software?	☐ Yes ☐ No	Please specify compatible products:
D.25	For web application security, has the vendor implemented controls in the proposed solution to protect against SQL injection, cross-site scripting, and other common attacks?	☐ Yes ☐ No	Provide additional information below:

I certify that the above responses are true and accurate.

NAME OF OFFEROR:_____

_____
Typed Name and Title

_____ _____
Signature Date of Submission