Arlington County Information Governance Certification Requirements

Approved for Use
September 1, 2013
Revised September 28, 2018

Introduction

The Arlington County Project Proposal Matrix for Meeting Information Governance Policy Requirements is required as an attachment for information technology responses to Request for Proposal (RFP) or internal application development processes initiated by Arlington County Government. It is intended to assist Arlington County procurement with soliciting vendor responses that identify the requirements of the Arlington County Information Governance Policy. The clear identification of each element is required by Arlington County in order to sustain and ensure an adequate foundation for the development and implementation of secure information technology practices within Arlington County Government. Elements are included for issues relative to HIPAA Privacy, Security, and Records Management compliance in general.

This certification applies to all application data in transit, at rest, used and stored in support of government business. This certification also is required for any outsourced SaaS, CLOUD, or other off site data services in support of government business.

On-site vendors with access to Arlington County information resources are required to abide by all policies and procedures of Arlington County Government, Virginia.

How to Use the Security Template

The template is comprised of four sections:

1. Standard
This section includes the requirements to be addressed. Those requirements can take the form of a question or a statement.

2. Does Your System Comply?
The responder shall provide a high level response to the Standard. The answers can be YES, NO, or Alternative (ALT). The responder MUST check one of the three boxes to indicate their position or solution capability. If the ALT box is checked the responder must provide a high level explanation of the alternative in the "Comments/Plans for the Meeting Compliance" section. If there is supplemental information requested within the system compliance column, an answer MUST be provided.

3. Where in Your Proposal is the Solution Described?
In this section the responder shall insert the technical proposal reference to the details of the solution. It should be specific (e.g., volume, chapter/section, page and paragraph heading) as to where the answer can be found. Failure to provide the reference or an incorrect reference shall be considered a NO answer. The correct reference location will not be researched by the procurement office or other Arlington County Departments.

4. Comments/Plans for Meeting Compliance

In this section the responder may provide any high level comments that may clarify a response in the "Does System Comply" section. It is especially important for responders to use this section to explain alternative checked responses. An alternative response can include a statement of future development or a solution that addresses the requirement, however may not be a direct answer/solution to the requirement. This section MUST NOT be used for detailed descriptions of the response.

References:

. This template was based upon similar work approved for public distribution by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) in August 2003; modified for Arlington County Government, February 2013.

		STANDARDS	SYSTEM SPECIFICATIONS?	WHERE IN YOUR PROPOSAL IS THE SPECIFICATION DESCRIBED?
		A. Description		
A.1.		**System Name/Title:**		
A.2.		**Vendor/Developer:**		
A.3.		**RFP Reference Number:**		
A.4.		**Application Type:**	COTS:☐ Proprietary: ☐ ALT: ☐ .NET ☐ JAVA ☐ OTHER ☐ explain: _____ _____	
A.5.		**Provide a copy or statement about your software development life cycle standards and approach.**		
A.6.		**Database Requirements:**	Yes:☐ No: ☐ ALT: ☐ ☐ Oracle 10G or higher ☐ DB2 Release 7 ☐ Microsoft SQL Server 2016 SP1 ☐ Other	

A.7.		**User access controls are:**	☐ Built into the system
			(Must respond to Sections A, B, C, D, E, & F)
			
			☐ Standard operating system
			(Must respond to Sections A, C, D, E, & F)
			    ☐ Active Directory
			    ☐ LDAP
			    ☐ RACF
			
			☐ Database control
			(Must respond to Sections A, C, D, E, & F)
			    ☐ Oracle
			    ☐ DB2
			    ☐ SQL
			
			☐ Other
			(Must respond to Sections A, B, C, D, E, & F)	

A.8	**List all additional system components required to make the proposed solution work, including any applets and/or plug-ins.**		

	STANDARDS	DOES SYSTEM COMPLY?	WHERE IN YOUR PROPOSAL IS THE SOLUTION DESCRIBED?	COMMENTS/PLANS FOR MEETING COMPLIANCE
	B. Password controls			
B.1.	System enforced: specified strong password to include minimum length and combination of alpha and numeric characters	Yes:☐ No: ☐ ALT: ☐ Current Minimum: ___ Current Maximum: ___		
B.2.	System enforced: user passwords automatically changed or revoked after a user defined period has passed	Yes:☐ No: ☐ ALT: ☐ Current Change Interval: ___		
B.3.	System enforced: users required to change their passwords following the initial set up or resetting of the password	Yes:☐ No: ☐ ALT: ☐		
B.4.	System enforced: system administrators may not disable password controls	Yes:☐ No: ☐ ALT: ☐		
B.5.	System prevents auto logon, application remembering, embedded scripts, and hard-coded passwords in software	Yes:☐ No: ☐ ALT: ☐		
B.6.	History of previously used passwords is maintained by the system to prevent reuse	Yes:☐ No: ☐ ALT: ☐ Current Value: ___		
B.7.	Users are provided the capability to change their own passwords at their discretion	Yes:☐ No: ☐ ALT: ☐		
B.8.	User id's are disabled after a specified number of consecutive invalid login attempts	Yes:☐ No: ☐ ALT: ☐ Current # Attempts: ___		
B.9.	System automatically activates a password protected screensaver when units remain idle for determined period of time	Yes:☐ No: ☐ ALT: ☐		
B.10.	System automatically logs users off after a specified period of inactivity	Yes:☐ No: ☐ ALT: ☐ Current Auto logoff Time:___		
B.11.	Passwords entered in a non-display field	Yes:☐ No: ☐ ALT: ☐		
B.12.	Passwords encrypted when routed over a network	Yes:☐ No: ☐ ALT: ☐		
B.13.	Passwords are encrypted in storage	Yes:☐ No: ☐ ALT: ☐		

	STANDARDS	DOES SYSTEM COMPLY?	WHERE IN YOUR PROPOSAL IS THE SOLUTION DESCRIBED?	COMMENTS/PLANS FOR MEETING COMPLIANCE
	C. Security Administration			
C.1.	**System logs unauthorized access attempts by date, time, user id, device and location**	Yes:☐ No: ☐ ALT: ☐		
C.2.	**System maintains an audit trail of all security maintenance performed by date, time, user id, device and location and information is easily accessible**	Yes:☐ No: ☐ ALT: ☐		
C.3.	**System provides security reports of users and access levels**	Yes:☐ No: ☐ ALT: ☐		
C.4.	**System provides a field(s) for personal information to be used for verification of users' identities for password resets and other maintenance (i.e., Mother's Maiden Name, DOB, etc). Fields used would not be a requirement**	Yes:☐ No: ☐ ALT: ☐		
C.5.	**System provides varying levels of access within the security application (i.e. access to only password reset functions or access to password reset function +Access to add & update users)**	Yes:☐ No: ☐ ALT: ☐		
C.6.	**System permits the assignment of designated Access Control Administrators**	Yes:☐ No: ☐ ALT: ☐		
C.7.	**System provides varying levels of access within the application**	Yes:☐ No: ☐ ALT: ☐		
C.8.	**System uses groups and unique user ids to define levels of access**	Yes:☐ No: ☐ ALT: ☐		

	STANDARDS	DOES SYSTEM COMPLY?	WHERE IN YOUR PROPOSAL IS THE SOLUTION DESCRIBED?	COMMENTS/PLANS FOR MEETING COMPLIANCE
	C. Security Administration (continued)			
C.9.	System provides the capability to place security controls on each system module and on confidential and critical levels within each module	Yes:☐ No: ☐ ALT: ☐		
C.10.	System provides capability to restrict access to particular records within the system, based on user id	Yes:☐ No: ☐ ALT: ☐		
C.11.	System provides capability of encryption of confidential or sensitive information stored locally on the device	Yes:☐ No: ☐ ALT: ☐		
C.12.	System provides capability of encryption of confidential or sensitive information transmitted over the network	Yes:☐ No: ☐ ALT: ☐		
C.13.	On-site training and sufficient supporting reference materials related to security administration for system administrators are provided prior to migration of product to production environment	Yes:☐ No: ☐ ALT: ☐		
C.14.	System provides centrally managed updates to protect against vulnerabilities	Yes:☐ No: ☐ ALT: ☐		
C.15	System will operate as described in conjunction with the County's chosen Anti-virus, anti-malware, and anti-spam protection software.	Yes:☐ No: ☐ ALT: ☐		
C.16	If this system stores PII, PPI or HIPAA data has the County Privacy Officer (HR Director) approved the Business Associate Agreement (BAA)?	Yes:☐ No: ☐ ALT: ☐		

	STANDARDS	DOES SYSTEM COMPLY?	WHERE IN YOUR PROPOSAL IS THE SOLUTION DESCRIBED?	COMMENTS/PLANS FOR MEETING COMPLIANCE
	D. Activity Logging			
D.1.	**System logs unauthorized access attempts by date, time, user id, device and location**	Yes:☐ No: ☐ ALT: ☐		
D.2.	**System maintains an audit trail of all security maintenance performed by date, time, user id, device and location and information is easily accessible**	Yes:☐ No: ☐ ALT: ☐ Number of days kept: ___		
D.3.	**System logs all inquiry accesses to data**	Yes:☐ No: ☐ ALT: ☐		
D.4.	**System logs all modification accesses to data**	Yes:☐ No: ☐ ALT: ☐		
D.5.	**System has auditing capabilities for both online or batch reporting. Can also be exported into County standard databases**	Yes:☐ No: ☐ ALT: ☐		
D.6.	**Can logs be archived and recalled as needed?**	Yes:☐ No: ☐ ALT: ☐ Archive methods: ☐ Tape ☐ Disk ☐ Other		

	STANDARDS	DOES SYSTEM COMPLY?	WHERE IN YOUR PROPOSAL IS THE SOLUTION DESCRIBED?	COMMENTS/PLANS FOR MEETING COMPLIANCE
	E. Networking and Compatibilities			
E.1.	**Provide a diagram of the recommended network connectivity, interfaces, and data exchanges required for the proposed solution. Include a description and any additional explanation necessary to explain the method of interaction (e.g., read/write, synchronous/ asynchronous).**			
E.2.	**System configuration/architecture (i.e., hardware, wiring, display, network, and interface) is documented and included in proposal.**	Yes:☐ No: ☐ ALT: ☐		
E.3.	**Does your solution support external data transmission? Please indicate the method(s) supported.**	Yes:☐ No: ☐ ALT: ☐ Methods: ☐ Secure FTP ☐ Fax ☐ Email ☐ File Copies (CD, Diskette, etc) ☐ Browser applications ☐ Tape media ☐ Web services ☐ Other:		
E.4.	**For externally electronically transmitted information, can the solution support encryption and data protection?**	Encryption: Yes:☐ No: ☐ ALT: ☐ Data Protection: Yes:☐ No: ☐ ALT: ☐		
E.5.	**For wireless transmission of data, does the system support the Arlington County wireless standards?**	Yes:☐ No: ☐ ALT: ☐		

	STANDARDS	DOES SYSTEM COMPLY?	WHERE IN YOUR PROPOSAL IS THE SOLUTION DESCRIBED?	COMMENTS/PLANS FOR MEETING COMPLIANCE
	E. Networking and Compatibilities (continued)			
E.6.	**Can the system be accessed remotely (i.e., , Internet, etc.). If applicable, provide an explanation of your wireless transmission requirements for the proposed solution.**	Yes:☐ No: ☐ ALT: ☐ Methods: ☐ Dialup ☐ Internet ☐ Internet VPN ☐ Wireless		
E.7.	**For management and vendor support can the system support secure remote access (VPN/Dual Factor Authentication)?**	Yes:☐ No: ☐ ALT: ☐ Methods: ☐ Security tokens that provide one-time password authentication ☐ Public/Private keys with strong pass phrases ☐ Citrix		
E.8.	**What anti-virus and end-point security software is the proposed solution compatible with? Provide version details with answer.**			

		STANDARDS	DOES SYSTEM COMPLY?	WHERE IN YOUR PROPOSAL IS THE SOLUTION DESCRIBED?	COMMENTS/PLANS FOR MEETING COMPLIANCE
	F. Contingency, Continuity, & Back-up				
F.1.	**What is your back up policy for the proposed solution?**				
F.2.	**For vendor supported, maintained, and managed solutions is there a Business Continuity Plan and a Disaster Recovery Plan?**	Yes:☐ No: ☐ ALT: ☐ ☐ Not applicable, County supported			
F.3.	**Does your solution automatically monitor database capacity requirements to reduce the risk of system overload? If yes, is a warning alert provided to the system administrator?**	Yes:☐ No: ☐ ALT: ☐ ☐ Warning alert provided ☐ Not applicable, County supported			
F.4.	**In the event of an identified vulnerability to or within the system, are there designated technical support personnel available to assist Arlington County with eliminating or mitigation of the vulnerability?**	Yes:☐ No: ☐ ALT: ☐ ☐ Not applicable, County supported			
F.5.	**In the event of an identified vulnerability will there be a zero-day vendor response team assigned to provide support to Arlington County IT administrator(s)?**	Yes:☐ No: ☐ ALT: ☐			
F.6	**In the event of an incident or hardware/software fault does the application support redundant auto-failure, i.e. seamlessly transition the application to the redundant platform?**	Yes:☐ No: ☐ ALT: ☐			
	G. Records Retention				
G.1.	**Please describe (in detail) the type of information to be stored in the proposed system**	Yes:☐ No: ☐ ALT: ☐			
G.2.	**Are you aware of existing records retention requirements for the content (See Virginia Records Retention Requirements**	Yes:☐ No: ☐ ALT: ☐			

	If yes, please state the requirements.			
G.3.	Are you proposing to store any Personally Identifying Information in the system (SSN, Drivers License, financial information, etc.)? If so, please describe the business need and safeguards in place to secure the information.	Yes:☐ No: ☐ ALT: ☐		
G.4.	Does the system allow for records to be protected from unauthorized modification or deletion?	Yes:☐ No: ☐ ALT: ☐		
G.5.	Does the system allow for records to be tagged (classified) and assigned a retention policy/schedule ensuring that the record is retained pursuant to the policy?	Yes:☐ No: ☐ ALT: ☐		
G.6.	Does the system allow for automated destruction/deletion of records that have met or exceeded the required retention schedule?	Yes:☐ No: ☐ ALT: ☐		
G.7.	Does the system allow for automated destruction to be suspended in the event of anticipated litigation and/or investigation (legal hold)?	Yes:☐ No: ☐ ALT: ☐		
G.8.	Does the system allow for retrieval and production of information for e-discovery and FOIA compliance?	Yes:☐ No: ☐ ALT: ☐		
G.9.	If the system does not contain any of the required functions identified in G.4. – G.8., have you ensured that it integrates with county systems that do contain the required functionality? If yes, please describe your solution.	Yes:☐ No: ☐ ALT: ☐		

	H. Data Security/Privacy			
H.1.	If this system stores HIPAA or PII data is the data secured through encryption?	Yes:☐ No: ☐ ALT: ☐		
H.2.	If this system is capable of utilizing GPS for tracking purposes has Terms and Conditions of use language been prepared?	Yes:☐ No: ☐ ALT: ☐		
H.3.	If this is a public facing application and GPS is potentially part of the offering has a straw man education and promotion package been prepared?	Yes:☐ No: ☐ ALT: ☐		