MaineHousing
MAINE STATE HOUSING AUTHORITY

2022 IFP for Website Hosting Solutions
Questions & Answers

Q: Could you share the Security Survey for us to review?
A: Sure thing. Please see the survey attached to this document.

Q: Are you looking for in-state bidders, or are you also open to bidders from other states?
A: Bidders from all states are welcome to submit bids to this RFP.

Q: Do you have any development or programming capabilities in-house?
A: Yes, we have an in-house webmaster that performs all development, code, and design needed for the site.

Q: What is the budget for this project?
A: We do not have a set budget for this project. We are paying around $15,000 per year for our current hosting services.

Q: We are an AWS Public Sector Partner for cloud hosting. Are you open to host the new website on AWS Cloud?
A: AWS would be a new service for us. This would depend on the level of support available.

Q: How do you keep the website secure? Do you have a security policy in place that we can look at?
A: We do not have a security policy in place. What security we do have is configured through EST File Security

Q: What is your current website hosting configuration with regards to Process Cores and Memory?
A: We are currently hosted on a Microsoft 2016 Server, Intel® Xeon ® 3.60GHz, quad-core with 16GB Ram.

Q: How are site backups currently taken?
A: Backups of the server are performed by our current host on a nightly basis.

Q: Will you require a new SSL Certificate for the website?
A: Our sites all require an SSL Certificate. We currently purchase the certificates and install them on the server ourselves.

Q: Do you currently have a security and disaster recovery plan in place?
A: We do not for this particular website and server.

Q: How often are security patches and updates currently applied to the server?
A: Security patches and updates are applied monthly.

Q: When do you expect to complete the hosting setup under this contract?
A: Our current contract expires in July. We would like to be able to move over to the new hosting environment by then.

Q: Do you currently use any tools to manage web accessibility?
A: We are using SiteImprove to identify areas of accessibility that need attention. We are not currently using a tool that allows users to manipulate accessibility settings on their end.

MAINEHOUSING
VENDOR SECURITY SURVEY

INSTRUCTIONS

This questionnaire is intended to be filled out by MaineHousing and vendor representatives. The General Information, Required Documentation, General Questions, and Technical Questions sections are intended to be filled out by the vendor and MaineHousing Information Technology (IT) staff.

The Findings and Risk Assessment section is to be used by MaineHousing IT only.

Once this document is submitted to MaineHousing IT, all contents of this document are considered confidential and not for release without prior approval from IT.

Please answer all questions completely on the following tabs. N/A is an acceptable response. If an answer is unknown, please state that so we can set up a call to discuss the question(s).

GENERAL INFORMATION (MAINEHOUSING TO FILL IN)

Date Survey Sent	
Vendor/Product	
Vendor Contact Name	
Vendor Contact Phone	
Vendor Contact Email	
MH IT Contact Name	
Other Involved MH Staff	
Which MH Departments use this solution?	
How many MH users?	
Is this a new, existing or replacement system?	

REQUIRED DOCUMENTATION

Document	Attached (Y/N)
SSAE16 SOC 2 Type II, FedRAMP or Other Attested Audit (These are 3rd party security audits completed to verify vendor security controls)	
Network infrastructure diagram(s) – vendor to provide if SAAS/PAAS/IAAS, MaineHousing otherwise	
Diagram showing data flow	
System Requirements Documentation and any other technical/security documentation	
Disaster Recovery and Business Continuity Documentation	
Certificate of Insurance & Cyber Insurance Policy	

MAINEHOUSING

VENDOR SECURITY SURVEY

GENERAL QUESTIONS		
#	**General Questions**	**Response**
G1	Describe the primary functions this solution provides.	
G2	Is this solution on premises or cloud based?	
G3	Will the vendor need to physically access or be on site at the MaineHousing office?	
G4	How will the system/application be accessed by the vendor, users, and IT staff?	
G5	Will the vendor require remote access?	
G6	Does the vendor use any sub-contractors?	
G8	What are the system requirements to integrate this system with Active Directory using LDAP or SSO?	
G9	Will the system store or transmit Protected Health Information (PHI)?	
G10	Will the system store or transmit Personal Identifiable Information (PII) i.e.. Social security, driver's license numbers?	
G11	Will the system store or transmit PCI (credit card) data?	
G12	Will the system store or transmit any financial data (e.g. loan numbers or payroll & HR information)?	
G13	Does the system have regulatory certification requirements (i.e. HUD)?	
G14	Are there any other legal stipulations that require attention? (Such as re-broadcasting TV/radio stations, online agreements, 3rd party software agreements, etc.)	
G15	Other than production, what environments will be implemented (e.g. testing, development, etc.), and of those environments, which will contain a copy of production data and test data (fake names, companies, etc.)?	

MAINEHOUSING

VENDOR SECURITY SURVEY

LEGAL & INSURANCE QUESTIONS

#	General Questions	Response
L1	Please describe your security incident management process.	
L2	Please describe any security breaches or issues you have experienced in the last five years.	
L3	Who would perform forensic analysis of a breach if one were to occur and are you able to collect evidence using proper chain-of-custody procedures?	
L4	Do you have a Cyber Insurance Policy? Do your sub-contractors if applicable?	
L5	Provide the Names, address, phone number, email address and titles of the primary and secondary IT security personnel that we would communicate with regarding a suspected Breach?	

MAINEHOUSING
VENDOR SECURITY SURVEY

TECHNICAL QUESTIONS						
		System Capabilities	**Application**	**Web Server**	**OS**	**Database**
Audit & Logging	AL1	Does the system generate audit logs of the following events? (provide answers for each component of the system being provided as represented in each column) - Failed logon attempts - Successful logons - Modification of settings - Shutdown/Startup - Administrative Account Management - Override functions executed by users - Reading of files - Modifying of files - Creating data or files - Deleting data or files - Transfer of data (send or receive)				
	AL2	Can the system archive audit log data and if so, describe how and where the archived logs will be kept?				
	AL3	Can the system provide user audit reports for the following? - Users and user access levels - Active vs Inactive Accounts - Administrative users - Last login				
Authentication & Access	AA1	What is the session/idle timeout and is it configurable?				
	AA2	What is the multi factor authentication solution provided for this system? Please describe the access verification process in detail.				
	AA3	Will authentication information be encrypted in transit? If so, explain the encryption method? (i.e. SSL, TLS 1.1, TLS 1.2, TLS 1.3)				
	AA4	Are interactive generic accounts required? These would be any shared logins used by users to access the system. If so, explain in detail what they will be used for.				
	AA5	Are service or resource accounts required? If so, explain in detail how they will be used.				
	AA6	Are users required to have Local Administrative privileges to run this product? If so, why?				
	AA7	Does the vendor utilize unique usernames and passwords for vendor workforce that will be accessing and supporting our data?				
	AA8	Does the application enforce password complexity controls for at least 3 of the 4 following characteristics: - Upper case - Lower Case - Numbers - Special Characters ($, #, *, spaces, etc.)				
	AA9	Will the application password controls enforce a 12 character user password minimum?				
	AA10	Describe the logical password controls available (length, forced changes, complexity, age, history, account lockouts etc.).				
	AA11	Are password policy settings customizable by MaineHousing staff?				

MAINEHOUSING
VENDOR SECURITY SURVEY

	AA12	If the system has a default administrative account, can it be renamed or disabled?				
	AA13	Does the system support role based access?				
	AA14	Who will be responsible for user and administrative access administration? If it's not MaineHousing, explain the account creation process				
Business Continuity	BC1	Please explain how your solution provides redundancy for business continuity?				
	BC2	What data integrity check mechanisms are in place?				
	BC3	What is the contracted service level agreement (SLA)?				
	BC4	Are there alternate method(s) to provide vendor and IT support to the application if internet connectivity is unavailable?				
	BC5	Describe how data will be accessed in the event of an emergency if not hosted by MaineHousing?				
	BC6	Explain in detail, the backup plan to include frequency, method (i.e. full, incremental, etc.), and media used.				
	BC7	Are there any special retention requirements for backups?				
Configuration Management	CM1	Can MaineHousing specify the Network Time Protocol (NTP) server used with this system?				
	CM2	What Microsoft products are used by this system and which versions are supported? Are those licenses provided with the software or purchased separately by MaineHousing?				
	CM3	Can this system be placed on the MaineHousing domain?				
	CM4	Does the vendor uninstall or disable unnecessary system applications and services not required for the functioning of the application?				
	CM5	Does the primary application require additional software to be authorized under our application control?				
	CM6	If there are additional storage requirements what are the IO demands?				
	CM7	If new servers are required, does the system support virtualization?				
	CM8	What web browser is recommended to ensure the best performance for this solution?				
	CM9	Will the application be presented through Citrix and if so how many concurrent users are expected?				
	CM10	Are there any connections to external websites?				
	CM11	Is any there any transfer or storage of data required internal or external to the solution?				
	CM12	What is the required operating system(s)? If an unsupported operating system is required explain why? (i.e Windows XP)				
	CM13	Are shared directories/folders required for the system to operate? If yes, explain what directory/folder and why.				
Connectivity	CN1	Does this system use wireless connections (Wi-Fi, Bluetooth, NFC, RFID, etc.)?				
	CN2	Does the system use any external connections from MaineHousing? If so, describe the connection (type, from, to, and what is being transmitted/received) in detail.				

MAINEHOUSING
VENDOR SECURITY SURVEY

	CN3	Can Citrix Storefront be used for remote access to the MaineHousing network?				
	CN4	Does the solution require new networking equipment, drops, or jacks?				
Encryption	EN1	Describe encryption details for data at rest.				
	EN2	Describe encryption details for backups.				
	EN3	Are any or all data communication transmissions encrypted? If so, what type is used (SSL, TLS 1.0, TLS 1.1, TLS 1.2)?				
Endpoint	EP1	What antivirus solution is compatible with this system?				
	EP2	Can the endpoint solution be configured for weekly scans?				
	EP3	Document all the exclusions (path and reason) for endpoint protection.				
Vendor Capabilities	VC1	Does the documentation include contact information, instructions for receiving support, contract number, service agreement number, and any other required support information?				
	VC2	Are patches for vulnerabilities and security updates provided at no charge to MaineHousing?				
	VC3	If product uses a third party software, does vendor certify patches from third party vendor (My SQL, Cache, etc.)?				
	VC4	Does the vendor provide documented processes and procedures for provisioning and de-provisioning vendor's user/system accounts?				
	VC5	Is the operating system, application, and any third party software currently supported by the original manufacturer?				
	VC6	What mechanisms do you have in place to protect your software supply chain?				
Vulnerability Management	VM1	Will the system be fully updated with all certified service packs and patches prior to deployment?				
	VM2	Is the system currently supported and capable of maintaining regular updates and patches?				
	VM3	Does the system have documented instructions for patching?				

MAINEHOUSING

VENDOR SECURITY SURVEY

FINDINGS AND RISK ASSESSMENT

OVERALL RECOMMENDATION Choose an item.

OVERALL RISK: Choose an item.		
SECTION	**RISK**	**EXPLANATION**
General	Choose an item.	
Legal	Choose an item.	
Audit/Logging	Choose an item.	
Access/Auth	Choose an item.	
Busn. Cont.	Choose an item.	
Configuration	Choose an item.	
Connectivity	Choose an item.	
Encryption	Choose an item.	
Endpoint	Choose an item.	
Vendor Capabilities	Choose an item.	
Vulnerablity Mngmt.	Choose an item.	