Maynard Partners LLC

Vendor Assessment Questionnaire

Note: For all questions below, please answer with consideration only for the in-scope data and systems that pertain to the services provided to and applicable to <District Name Here>, unless the question specifically refers to your organization as a whole. In-scope systems include any systems, technologies and infrastructure that collect, store, or process data for services provided to <District Name Here>.

			To be completed by Third Party/Vendor		*To be completed by <District Name Here>*
Question	**Domain Area**	**Assessed Control**	**Answer Choice (Yes/No or Text)**	**Additional Comments (to support answer choice)**	**Verified? (Yes/No)**
1	Compliance	Does a formal information system/security assessment program exists that defines requirements for auditing in-scope information systems to determine their continued compliance with organizational policies, standards, and applicable regulations. (SOX, HIPPA, FISMA, GDPR, PCI DSS) Does the organization have documentation readily available for <District Name Here> to demonstrate compliance?	To be completed by Third Party/Vendor		
2	Compliance	Has the organization had an independent audit attestation (e.g., SOC1/SOC2) or security review within the last 12 months? Upon request, can compliance be demonstrated?	To be completed by Third Party/Vendor		
3	Security Governance	How do you ensure that the company policies, standards and procedures are up to date?	Please explain		
4	Security	Has your organization aligned to a security framework ? (e.g. NIST, ISO 27001)	To be completed by Third Party/Vendor		
5	Security	Do you currently conduct security assessments, such as penetration tests on an annual basis?	To be completed by Third Party/Vendor		
6	Security	What security controls do you have in place to govern and manage third parties or outsourced operations?	Please explain		
7	Security	How are incidents, threats & vulnerabilities managed?	Please explain		
8	Security	Does the organization have documented access management controls in place?	To be completed by Third Party/Vendor		
9	Security	Does the organization deploy encryption at rest and in transit for all <District Name Here> related data?	To be completed by Third Party/Vendor		
10	Operations	Does the organization have a process is in place to perform background screening of individuals (e.g. criminal records, referencing), prior to authorizi access to any of the in-scope systems, data, and/or facilities?	To be completed by Third Party/Vendor		
11	Operations	In the event of a breach, does the organization have processes in place to assist <District Name Here> in complying with the breach notification requirements?	To be completed by Third Party/Vendor		
12	Privacy	What types of data elements are being transferred or collected from <Distric Name Here> as a part of the service or product provided? Are they stored within the organization's environment?"	Please explain		
13	Privacy	Does the organization have an implemented Data Privacy Program?	To be completed by Third Party/Vendor		
14	Privacy	Can your organization demonstrate adherence to applicable privacy laws (i.e CCPA, GDPR)?	To be completed by Third Party/Vendor		