Data Security. With respect to the System and environment the Contractor uses to provide services, including those for data storage and transmission, the Contractor agrees as follows:

1. ADA Requirements. The Contractor agrees to comply with all aspects of both the Americans with Disabilities Act (ADA) and the Web Content Accessibility Guidelines (WCAG) 2.1, Level AA. The Contractor shall ensure that all web-based software solutions, websites, and mobile applications provided under this contract are fully and readily accessible to individuals with disabilities and provide reasonable accommodations. This includes, but is not limited to, providing alternative text for images, ensuring that all interactive elements are navigable via keyboard, and providing captions for all video content. The Contractor shall also ensure that any updates or modifications to the software, websites, or applications continue to meet these accessibility standards and comply with the ADA and WCAG. Failure to comply with the ADA, WCAG, and these requirements may result in the termination of this contract and the Contractor being held liable for any damages or costs incurred by the County as a result of non-compliance.
2. Ownership of County Data. Lake County is the owner of its data, data compilations and reports or compilations of its data generated from use of the Licensed System (“County Data”). Notwithstanding anything to the contrary contained in the contract, the County will have the right to use the Contractor's Licensed System to access and have unfettered use of such data, reports, compilations, or information derived from or resulting from the use of the Licensed System or to generate reports from such data, files, or information. Contractor acknowledges and agrees that the County is the owner and custodian of the data, compilations, and information, whether or not such is electronically retained and regardless of the retention media and that the use of the Licensed System in relation to such information or data does not in any way restrict County in the County's rights of disclosure of its data and information.
3. County Proprietary Information. The Contractor shall take necessary security measures to ensure that the County proprietary information cannot be downloaded to or printed from any devices that its employees, contractors, or subcontractors use, including, and without limitation, desktops, laptops, and USB flash drives.
4. County Data. In storing or processing the County Data, the Contractor shall not comingle the County Data with any data from Contractor’s other clients.
5. Security Operating Protocols. The successful proposer’s cloud service product offering(s) that collect, process, store, maintain, transmit, dispose, and/or could impact government data must demonstrate compliance with National Institute of Standards and Technology (NIST) Special Publication 800- 53 (revision 5 or latest version) at the Impact Level specified below or be enrolled in the GovRAMP Progressing Snapshot Program until the product achieves GovRAMP Authorized status at a Public Control Baseline of Moderate. Contractors not enrolled with GovRAMP, shall provide independent verification of systems and security controls (e.g. SOC 2, Type II report) on an annual basis. The Contractor shall provide the most recent independent verification for review to the County prior to contact execution.
	1. GovRamp Continuous Monitoring. Products utilizing a GovRAMP security status to satisfy this cybersecurity standard, must maintain its status for the duration of the contract and must grant visibility and access through GovRAMP for continuous monitoring as requested.
6. Hosting Provider. The Contractor shall only use servers located in secure facilities in the U.S. and administered by a third-party hosting provider (“Hosting Provider”) to provide services to the County. The Contractor represents and warrants that each Hosting Provider used by the Contractor will cause to be conducted, on at least an annual basis, an SSAE 16 Type II (or equivalent) security audit by a reputable security specialist who must identify in a written report (a copy of which must be promptly delivered to the County upon request and which must be the Contractor’s Proprietary Information) any readily identifiable security vulnerabilities in connection with the applicable Hosting Provider’s services that the Contractor uses and the operating environment.
7. County Data Location. Except for sending the County Data to the County, the Contractor shall keep the County Data solely in its Hosting Provider’s facility or facilities located in the United States and shall not allow such data to leave such facility or facilities in any form.
8. Confidentiality of Data.  All County and County employee data encountered in the course of this project and in administration of the plan is strictly confidential.  All Administrator staff, including any sub-contractors, who may have access to or potential access to any confidential County data must protect this data from unauthorized access.  Under no circumstances may County employee data be disclosed to parties outside the contract or used for purposes other than the fulfillment of the contract.
9. Backup Materials. Licensor shall maintain backup servers as well as a complete and current backup copy of the System that the Licensor uses to provide services to the Licensee and the data processed through the System (“Backup Materials”). Backup Materials must be maintained at a separate physical location in the United States. If access or use of the service is interrupted, the appropriate backup must be activated within four (4) hours to minimize disruptions.
10. Security Breach Notification. Contractor shall have policies and procedures in place for the effective management of Security Breaches, as defined below. In the event of any actual, attempted, suspected, threatened, or reasonably foreseeable circumstance Contractor experiences or learns of that either compromises or could reasonably be expected to comprise County data through unauthorized use, disclosure, or acquisition of County data (“Security Breach”), Contractor shall immediately notify County of its discovery. After such notification, Contractor shall, at its own expense, immediately:
* Investigate to determine the nature and extent of the Security Breach.
* Contain the incident by taking necessary action, including, but not limited to, attempting to recover records, revoking access, and/or correcting weaknesses in security.
* Report to County the nature of the Security Breach, the County data used or disclosed, the person who made the unauthorized use or received the unauthorized disclosure, what Contractor has done or will do to mitigate any harmful effect of the unauthorized use or disclosure, and the corrective action Contractor has taken or will take to prevent future similar unauthorized use or disclosure.