ATTACHMENT - CLOUD TERMS TABLE

The following terms shall apply to Cloud Solutions, which may include software and services, purchased by the Commonwealth. Bidder must provide a response indicating the manner in which the proposed Cloud Solution meets each term, or provide justification as to why a term is not applicable to the offered Cloud Solution. These terms may be negotiated between Agency and the awarded Bidder and shall take precedence over any conflicting terms provided by the Cloud Solution Provider.

Category	Term	Bidder's Response
Support and Training	Technical support must be provided via online helpdesk and toll-free phone number, during Business Hours (Monday through Friday from 8:00 a.m. to 6:00 p.m. Eastern Time) or 24x7x365.	
Service Level	Bidder must provide a Service Level Agreement (SLA) which includes (1) guaranteed uptime percentage or at least 99.00% and (2) definition of uptime and how it is calculated	
Service Level	Scheduled maintenance must be limited to ten (10) hours per month. Downtime must include the sum of unscheduled maintenance and scheduled maintenance if they exceed ten hours per month, combined.	
Service Level	Scheduled maintenance must occur with at least two (2) business days' advance notice, at agreed-upon times, and in no event during Business Hours.	
Service Level	The SLA must include: (1) response and resolution times, (2) multiple levels of defect classifications, and (3) other applicable metrics based on industry standards.	
Remedies	The SLA must include remedies for failure to meet guaranteed uptime, response and resolution time, and other metrics. Remedies may include fee reductions, credits, and extensions in service period at no cost.	
Remedies	Repeated or consistent failures to meet SLA metrics shall result in (1) a refund of all fees paid by Agency for the period in which failure occurred and (2) participation by the Cloud Solution Provider in a root cause analysis and corrective action plan at Agency's request.	
Remedies	If uptime is less than 98.0% three times during the Term, Agency may terminate the subscription and receive a pro-rated refund of all prepaid fees.	
Reports	Agency will be provided with a written report of performance metrics, including uptime percentage and service support requests, classifications, and response and resolution times, as requested by Agency. Agency may independently audit the report at Agency's expense.	
Reports	Cloud Solution Provider and Agency shall meet as often as reasonably requested by either party to review the performance of the Cloud Solution.	
Reports	Cloud Solution Provider will provide to Agency regular status reports during unscheduled downtime, at least once per day or upon Agency's request.	
Reports	Cloud Solution Provider will provide Agency with root cause analysis within thirty (30) days of unscheduled downtime.	
Changes	Cloud Solution Provider may not change the Cloud Solution during the agreed upon term or period of performance in any manner that adversely affects Agency or degrades the service levels applicable to Agency without Agency's written approval.	

Updates and upgrades	Cloud Solution Provider will make updates and upgrades available to Agency at no additional cost when solution provider makes such updates and upgrades generally available to its users.	
Updates and upgrades	Cloud Solution Provider will notify Agency at least sixty (60) days in advance prior to any major update or upgrade.	
Updates and upgrades	Cloud Solution Provider will notify Agency at least five (5) business days in advance prior to any minor update or upgrade, except in the case of an emergency such as a security breach.	
Updates and upgrades	No update, upgrade, or other change may decrease the Cloud Solution's functionality; or materially and adversely affect Agency's use of, or access to, the Cloud Solution; or increase the cost to Agency.	
Agency Data	Agency retains full right and title to data provided by Agency and any data derived therefrom, including metadata (collectively, the "Agency Data").	
Agency Data	Cloud Solution Provider shall not collect, access, or use user-specific Agency Data except as strictly necessary to provide the Cloud Solution to Agency. No information regarding Agency's use may be disclosed, provided, rented or sold to any third party for any reason unless required by law.	
Agency Data	Cloud Solution Provider shall not use any information collected in connection with the agreement, including the Agency Data, for any purpose other than fulfilling its obligations under the agreement.	
Agency Data	Agency Data must remain within the United States. Cloud Solution Provider must disclose to Agency the identity and location of any third-party host of Agency Data.	
Agency Data	Agency may export the Agency Data at any time during the Term or for up to three (3) months after the Term in an agreed-upon file format and medium.	
Agency Data	Three (3) months after the termination or expiration of the Term or upon Agency's earlier written request, solution provider shall at its own expense destroy and erase all Agency Data and Agency Confidential Information, unless otherwise required by law. Cloud Solution Provider shall, upon request, send a written certification to Agency certifying that it has destroyed the Agency Data and Confidential Information in compliance with this section.	
Data Privacy and Security	Cloud Solution Provider must comply with all applicable laws related to data privacy and security. Cloud Solution Provider must obtain FedRAMP certification for the Solution and maintain such certification for the duration of the agreement with Agency.	
Data Privacy and Security	Cloud Solution Provider shall not access Agency user accounts, or Agency Data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the agreement, or at Agency's written request.	
Data Privacy and Security	Cloud Solution Provider may not share Agency Data with its parent company, other affiliate, or any other third party without Agency's express written consent.	
Data Privacy and Security	Prior to contract execution, solution provider and Agency must identify whether the solution provider or the cloud solution will access sensitive data, including without limitation: Personal data under M.G.L. c. 66A Personal information under M. G. L. c. 93H and 201 CMR 17.00 Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 Records under the Federal Education Rights and Privacy Act of 1974 Federal Tax Information under IRS Pub. 1075	

	Criminal Justice Information Criminal Offender Record Information If the Cloud Solution will store, use, access, or obtain potential access to, sensitive data, solution provider and Agency must document any additional specifications and/or requirements pertaining to the Cloud Solution and Cloud Solution Provider.	
Data Privacy and Security	Cloud Solution Provider shall provide a secure environment for Agency Data, and any hardware and software, including servers, network and data components provided by solution provider as part of its performance, in order to protect, and prevent unauthorized access to and use or modification of, the Cloud Solution and Agency Data.	
Data Privacy and Security	Cloud Solution Provider will encrypt personal and non-public Agency Data in transit and at rest.	
Data Privacy and Security	Agency Data must be partitioned from other data in such a manner that access to it will not be impacted or forfeited due to e-discovery, search and seizure or other actions by third parties obtaining or attempting to obtain solution provider's records, information or data for reasons or activities that are not directly related to Agency's business.	
Data Privacy and Security	In the event of any breach of security that adversely affects Agency Data or solution provider's obligations, or any evidence that leads Cloud Solution Provider to believe that such a breach is imminent, Cloud Solution Provider shall promptly (and in no event more than twenty-four hours after discovering such breach) notify Agency. Cloud Solution Provider shall identify the affected Agency Data and inform Agency of the actions it is taking or will take to reduce the risk of further loss to Agency. Cloud Solution Provider shall provide Agency the opportunity to participate in the investigation of the breach and to exercise control over reporting the unauthorized disclosure, to the extent permitted by law.	
Data Privacy and Security	If sensitive data is compromised, Cloud Solution Provider shall be responsible for providing breach notification to data owners in coordination with Agency and the Commonwealth as required by M.G.L. ch. 93H or other applicable law or Commonwealth policy. The solution provider shall not send any breach notification notices to Commonwealth's data owners without receiving prior written approval of the Commonwealth.	
Data Privacy and Security	Cloud Solution Provider shall indemnify, defend, and hold Agency harmless from and against any and all fines, criminal or civil penalties, judgments, damages and assessments, including reasonable expenses suffered by, accrued against, charged to or recoverable from the Commonwealth, on account of the failure of Cloud Solution Provider to perform its "Data Privacy and Security" obligations.	
Disaster Recovery	Cloud Solution Provider will maintain and follow a disaster recovery plan designed to maintain Agency access to the cloud solution, and to prevent the unintended destruction or loss of Agency Data. In no event shall the Cloud Solution be unavailable for a period in excess of twenty-four (24) hours.	
Disaster Recovery	Cloud Solution Provider shall review and test the disaster recovery plan regularly, at minimum twice annually. Cloud Solution Provider shall back up Agency Data in an off-site "hardened" facility located within the United States. In the event of service failure, Cloud Solution Provider shall be able to restore the Cloud Solution, including Agency Data, with loss of no more than twelve (12) hours of Agency Data and transactions prior to failure.	

Records and Audit	Cloud Solution Provider shall maintain accurate, reasonably detailed records pertaining to: (1) substantiation of claims for payment, (2) service levels, including service availability and downtime.	
Records and Audit	Cloud Solution Provider shall keep such records for a minimum of six (6) years from the date of creation.	
Records and Audit	Agency or its designated agent shall have the right, upon reasonable notice to solution provider, to audit, review, and copy all records collected by Cloud Solution Provider that may reasonably relate to Agency's use of the cloud solution. Such records will be made available to Agency or Agency's agent at no cost to Agency.	
Transition Assistance	Cloud Solution Provider shall reasonably cooperate with Agency and other parties in connection with all cloud solution to be delivered under the agreement. Cloud Solution Provider shall assist Agency in exporting and extracting the Agency Data, in a format usable without the use of the cloud solution and as agreed to by Agency.	
Transition Assistance	If Agency determines that a documented transition plan is necessary, Cloud Solution Provider shall reasonably cooperate with Agency to document such transition plan no later than sixty (60) days prior to termination or expiration of the agreement.	