Security Assurances for Cloud Computing:

1) Vendor shall use its reasonable best efforts to ensure that the Software is developed and deployed using secure coding practices and business processes in a manner that minimizes security flaws within the Software. Vendor will notify Arvada in the event that Vendor makes material changes in those practices and processes.

2) Vendor will maintain and enforce safety and security procedures with respect to its access and maintenance of Client Data (i) that are at least equal to industry standards for such types of locations, (ii) that are in accordance with reasonable Arvada security requirements, and (iii) that provide reasonable appropriate technical and organizational safeguards against accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of Client Data accessible by Vendor. Vendor will not be responsible for the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of Client Data by Arvada or its service providers.

3) All Client Data must be stored in a secure environment that protects the Client Data from unauthorized access, modification, theft, misuse, and destruction whether it resides in a repository or while in transit over networks.

4) All Client Data shall be stored in the United States at all times.

5) At the time of signing an Agreement with Arvada, Vendor shall provide the name and address of the third party host who will be storing Client Data, and Vendor shall provide Arvada at least thirty (30) days' prior written notice of a change of the third party host of the Client Data, unless an emergency requires otherwise.

6) Vendor shall notify Arvada within twenty-four (24) hours of any breach of security (whether physical, data, or network) that results in the unauthorized access to Client Data.

7) Vendor shall notify Arvada within seventy-two (72) hours of any dispute between Vendor and its third party host.

8) During the term of any Agreement between Arvada and Vendor, Arvada may, but is not obligated to, perform audits of the Vendor environment, including unannounced penetration and security tests, as it relates to the receipt, maintenance, use, or retention of Client Data. Arvada agrees to give Vendor twenty-four (24) hours prior notice of any such audit. The security audit may include, but not be limited to, the use of third party commercially available software security testing tools. If, based on the security audit, the software is determined to be insecure, then upon written notice of such non-secure status, Vendor, at its cost and expense, shall use its commercially reasonable best efforts to remedy the security flaws by modifying or replacing the software within thirty (30) days of receipt of such written notice (the "Security Remedy Period"). Upon receipt of revised software and notice from Vendor that the security flaws have been remedied prior to the end of the Security Remedy Period, the software shall again be subject to a security audit at Vendor's expense. Notwithstanding any provision of the Proposal to the contrary, if the software is determined to be insecure and remains insecure at the end of the Security Remedy Period, Arvada shall be deemed to have not accepted the software under the terms of any Agreement unless Arvada in its sole discretion otherwise expressly agrees in writing to accept the software notwithstanding that it is deemed to be insecure in accordance with this paragraph. With respect to any Agreement between Proposer and Arvada, Vendor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits with reasonable timeframes.

9) Vendor agrees to only use Client Data for its intended use under executed Contract Documents, and not to "mine" any of the Client Data for any purpose.

10) Services provided by Vendor and any associated cloud service provider must comply with the requirements of the most current Criminal Justice Information Services ("CJIS") Security Policy.

11) Vendor and any associated cloud service provider must ensure that Client Data is portable to other systems and interoperable with other operating systems to an extent that does not compromise the security and integrity of the Client Data.