Service Level Agreement

In connection with all Services provided to County under the Agreement, Provider shall, at no additional cost to County, meet or exceed the requirements below, including, as applicable, as to Application Service Provider ("ASP") hosting or Software as a Service ("SaaS"). The standards set forth herein are intended to reflect the current industry best practices for the Services. If and to the extent industry best practices evolve to impose higher standards than set forth herein, this Service Level Agreement ("SLA") shall be deemed to impose the new, higher standards upon Provider. Provider shall notify County in writing of any material change to its standards. Any capitalized terms not defined herein refer to those defined terms in the Agreement.

Any item addressed in this SLA that requires approval by County must be approved in writing. The Contract Administrator and Director of County's Division of Enterprise Technology Services ("ETS") are authorized to approve those items on behalf of County.

1. Security

1.1 Provider will ensure that County has the ability to authenticate all access by username, password, or two-factor. Provider shall restrict access to County data to a specific source static IP address.

1.2 Provider will support encryption using at least Advanced Encryption Standard 256-bit encryption keys ("AES-256") or current industry security standards for the connection from County to Provider's production network.

1.3 If and to the extent Provider accepts, transmits or stores any credit cardholder data on behalf of the County, or if and to the extent that Provider or its Software or Services is reasonably determined by County to potentially impact the security of County's cardholder data environment (CDE), Provider shall comply with the most recent version of the Security Standards Council's Payment Card Industry ("PCI") Data Security Standard (PCI-DSS), including complying with the following requirements:

1.3.1 Prior to execution of this Agreement, after any significant change to the CDE, and annually Provider shall provide to County:

a) A copy of their Annual PCI DSS Attestation of Compliance (AOC);

b) A written acknowledgement of responsibility for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the County, or to the extent that the service provider could impact the security of the county's cardholder data environment.

c) A PCI DSS responsibility matrix that outlines the exact PCI DSS Controls are the responsibility of the service provider and which controls the service provider shares responsibility with the County.

d) If Provider subcontracts or in any way outsources the CDE processing, Provider is responsible for providing the AOC for the subcontractor or payment gateway to the County.

e) Provider agrees that it is responsible for the security of the County's cardholder data that it possesses, including the functions relating to storing, processing, and transmitting of the cardholder data.

f) Provider will immediately notify Agency if it learns that it is no longer PCI DSS compliant and will immediately provide Agency the steps being taken to remediate the non-compliance status. In no event should Vendor's notification to Agency be later than seven (7) calendar days after Vendor learns it is no longer PCI DSS complaint.

g) Provider acknowledges that any indemnification provided for under the referenced Contract applies to the failure of the Vendor to be and to remain PCI DSS compliant.

1.3.2 Provider shall enforce automatic disconnect of sessions for remote access technologies after a specific period of inactivity with regard to connectivity into the County infrastructure. (PCI 12.3.8)

1.3.3 Provider shall activate remote access from vendors and business partners into the County network only when needed by vendors and partners, with immediate deactivation after use. (PCI 12.3.9)

1.3.4 Provider shall implement two-factor authentication for securing remote access outside the network into the County's environment with access to any stored credit card data. (PCI 8.3)

1.3.5 Provider shall ensure all non-console administrative access to the SaaS System connecting to the County environment is encrypted. (PCI 2.3)

1.3.6 Provider shall maintain a file integrity monitoring program to ensure critical file system changes are monitored and approved with respect to County data. (PCI 10.5.5)

1.3.7 Provider shall ensure personal firewall software is installed on any mobile or employee- owned device that manages the County's Cardholder Data Environment ("CDE") and connects to the Internet when outside the network in accordance with PCI Standard. (PCI 1.4)

1.3.8 If software is a payment application which processes, stores, or transmits credit card data, the VISA Cardholder Information Security Program ("CISP") payment Application Best Practices and Audit Procedures shall be followed and current validation maintained.

1.4 Provider shall restrict inbound and outbound traffic to the County network to "deny all, permit by exception" configuration. (PCI 1.2.1)

1.5 Provider's wireless networks shall be configured using current industry security standards to encrypt and protect communications of County information.

1.6 Provider agrees to achieve the Statement on Standards for Attestation Engagement No. 16 ("SSAE 16") criteria for security, availability, and confidentiality for the Services, the Software, and the System. All servers that Provider uses to provide Services under the Agreement shall be protected behind a layer of firewalls, the initial configuration diagram of which must be approved by County prior to Final Acceptance. Any subsequent changes are subject to approval by County, which shall not be unreasonably withheld. All database servers will be protected behind a second set of internal firewalls in compliance with Section 1.14 below.

1.7 Provider shall ensure that facilities that house the network infrastructure which hosts County data are physically secure against threats such as unauthorized access and natural and environmental hazards.

1.8 Provider shall ensure entry controls are in place to limit and monitor physical access to systems housing the County environment.

1.9 Provider shall ensure that separation of duties and least privilege are enforced for privileged or administrative access to County's data and systems.

1.10 Provider's procedures for the following must be documented and approved by County within 10 days of the execution date of this Agreement:

1.10.1 Evaluating security alerts and vulnerabilities;
1.10.2 Installing security patches and service packs;
1.10.3 Intrusion detection, incident response, and incident escalation/investigation;
1.10.4 Access and authorization procedures and resetting access controls (i.e., password policy);
1.10.5 Risk analysis and assessment procedures;
1.10.6 User access and termination procedures;
1.10.7 Security log review
1.10.8 Physical/facility access controls; and
1.10.9 Change control procedures.

1.11 Prior to the Effective Date of the Agreement, and at least annually for the duration of this Agreement, Provider shall provide County with a copy of a current, annual, unqualified SOC 2 Type II, Report, inclusive of all five Trust Service Principles (Security, Availability, Processing Integrity, Confidentiality, and Privacy), unless the County's Chief Information Officer in his or her sole discretion approves other documentation of appropriate security controls by Provider. If the audit opinion in the SOC 2, Type II report is qualified in any way, Provider shall provide sufficient documentation to demonstrate remediation of the issue(s) to the satisfaction of the County's Chief Information Officer.

1.12 Provider shall maintain a disaster recovery plan with mirrored sites geographically separated by at least 250 miles, with a Recovery Time Objective ("RTO") of a maximum of eight (8) hours and a Recovery Point Objective ("RPO") of a maximum of four (4) hours from the incident.

1.13 Provider shall conduct a disaster recovery test in coordination with County at least once per year. The timing and duration of the test will be subject to the approval of County, and shall be coordinated and timed so as to cause minimal or no disruption to the Services or the regular business of County.

1.14 Provider shall maintain controls that ensure separation of County data, confidential information, and security information from that of Provider's other clients. Provider agrees to provide at least AES-256 data encryption for Social Security Numbers, Taxpayer Identification Numbers, Employer Identification Numbers, bank account numbers, passwords, cardholder data, and any other data such as Protected Health Information ("PHI") and Personally Identifiable Information ("PII") or as otherwise directed by County on all copies of such data stored, transmitted, or processed, at no additional charge to County, and shall classify such data internally at its highest confidentiality level. Provider shall also ensure that the encryption key(s) are not stored with the encrypted data and are secured by a Hardware Security Module ("HSM"). Provider shall immediately notify County of any compromise of the encryption keys. Provider shall provide a copy of County's encryption key(s) at County's request. Provider shall prohibit the use of unencrypted protocols such as FTP and Telnet for the data defined in this paragraph.

1.15 Provider shall maintain industry best practices for data privacy, security, and recovery measures including disaster recovery programs, physical facilities security, server firewalls, virus scanning software, current security patches, user authentication, and intrusion detection and prevention. Provider shall maintain the same standards set forth herein regardless of whether the County data is stored at any primary or other location. Upon request (or as otherwise provided in this SLA), Provider shall provide documentation of such procedures and practices to County. In addition, Provider agrees not to allow Peer to Peer Software ("P2P") to be installed onto any network where County data/files reside unless County specifically permits it in writing on a case-by-case basis.

1.16 Provider shall report to County within twenty-four (24) hours of becoming aware of the incident if any unauthorized party is successful in accessing any information technology component related to the County within Provider's responsibility, including but not limited to servers or fail-over servers where County's data or files exist or are housed. Provider shall provide County with a detailed incident report within five (5) days of the breach, including remedial measures instituted and any law enforcement involvement. Provider shall fully cooperate with County on incident response, forensics, and investigations that involve the Provider's infrastructure relating to any County data or County applications.

1.17 Provider shall protect any Internet interfaces provided under this Agreement using a security certificate from a certification authority ("CA") that meets or exceeds the CA/Browser Forum's latest Secure Sockets Layer ("SSL") Baseline Requirements and Network and Certificate Systems Security Requirements.

1.18 Provider shall connect its hosting site through at least two (2) independent Internet Service Providers ("ISPs") with different Internet Points-of-Presence.

1.19 Provider shall ensure adequate background checks have been performed on any personnel having access to County data/files. To the extent permitted by such checks, Provider shall not knowingly allow access to any County data/files to convicted felons or other persons deemed by Provider to be a security risk.

1.20 Provider shall ensure that its service providers, subconsultants, and any third parties performing any Services relating to this Agreement shall comply with all terms and conditions specified in this Agreement unless County, in writing, excuses specific compliance with any such term or condition. Provider shall provide County annually, or more frequently at County's request, with a list of any service providers, subconsultants or other third-parties that Provider utilizes to provide Services to County.

1.21 Provider shall cooperate and provide any requested information during the term of the Agreement in connection with County's initial and on-going review and inspection relating to compliance and regulatory requirements. Request for information or review by County may include, but is not be limited to, the following:

a) Vulnerability scans of authenticated and unauthenticated operating systems/networks, web applications, and/or database applications;

b) Automated scans and penetration ("Pen") tests performed by County personnel or agents designated by County;

c) Review of requested documents, including without limitation, Provider's architecture documents, external audits of Provider's information security policies and procedures, Pen- test documentation, security incident reports, environment logs, virtual private network ("VPN") access logs to terminal services, network traffic and firewall activity logs, Intrusion Detection System ("IDS") attack alerts and anomalies, enterprise password management activity, server and application logs, and/or monthly or periodic network traffic and firewall activity logs; and

d) Physical inspection of Provider's facilities by the County or its officially designated representative.

1.22 If new or unanticipated threats or hazards are discovered by either County or Provider, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

1.23 Provider must mitigate critical or high risk vulnerabilities immediately after critical or high risk vulnerabilities are formally identified.

1.24 Provider shall provide County with the names and contact information for a security point of contact and a backup security point of contact to assist County with security incidents prior to the Effective Date of this Agreement.

1.25 Provider shall not release County data or copies of County data without the advance written consent of County.

1.26 County data or copies of County data must be available to County upon request within one (1) business day in the then-current format or any other format as may reasonably be requested by County.

1.27 Upon termination or expiration of this Agreement, after written confirmation by County that the applicable County data is currently maintained by County or otherwise securely stored, Provider shall securely erase all County data on all decommissioned hard drives or storage media to National Institute of Standards and Technology ("NIST") standards.

1.28 Provider shall provide privacy and information security training to its employees upon hire and at least annually.

1.29 Provider shall submit a network architecture diagram of the County's stored and transmitted data, to include location of data center and connectivity from all third parties who have access to County's data.

2. Compliance

2.1 For the duration of the Agreement, Provider shall provide County with the ability to generate account reports consisting of the account holder's name and application access rights.

2.2 For the duration of the Agreement, Provider shall provide County with the ability to generate account management reports showing new users, access rights changes, and account termination with the associated time stamp information.

2.3 For the duration of the Agreement, Provider shall provide County with the ability to generate time-stamped user and administrator access (login/logout) and a list of activities performed by administrators, privileged users, or third party contractors while using the System.

2.4 Promptly upon request, Provider shall provide County with access to time-stamped data transfer logs including the account, a description of the data transferred and its size, and the user and account names for forensic purposes.

2.5 Promptly upon request, Provider shall provide County with access to the time-stamped application and platform environment change control logs.

2.6 Promptly upon request, Provider shall provide County with access to the time-stamped data backup logs indicating the backup type (e.g., full, incremental, etc.).

3. Service Availability

3.1 System Availability

3.1.1 Provider guarantees that the network uptime will be 99.99% of Prime Time (defined as County business days from 7 a.m. – 7 p.m. Eastern Time) and 98.00% of non-Prime Time for each calendar month during the term of the Agreement, excluding Scheduled Maintenance as defined herein (collectively, the "Network Uptime Guarantee"). Network uptime requires proper functioning of all network infrastructure, including routers, switches, and cabling, affecting County's ability to reliably transmit or receive data. Network downtime is measured from the time the trouble ticket is opened to the time the network uptime is fully restored. As long as the System is available over the Internet to at least two other comparable customers (i.e., the System is functioning properly and there are no technical issues with Provider or its ISP's hardware or software), any inability on the part of County to access the System as a result of a general Internet outage will not be counted toward any unavailability time period.

3.1.2 Provider will refund to County five percent (5%) of the monthly fees (or monthly pro rata equivalent, if recurring fees under the Agreement are charged other than monthly) under the Agreement for each thirty (30) minutes of System unavailability/network downtime in excess of that permitted under the Network Uptime Guarantee (up to 100% of County's monthly fee), measured on a calendar month basis. Such refunds will be paid within ten (10) days of the applicable monthly report or, at County's option, may be credited against amounts due under any unpaid invoice.

3.1.3 Normal availability of the System shall be twenty-four (24) hours per day, seven (7) days per week. Planned downtime (i.e., taking the System offline such that it is not accessible to County) ("Scheduled Maintenance") shall occur during non-Prime Time and with at least five (5) business days' advance written notice to County. Provider may conduct Scheduled Maintenance at other times and upon less notice upon written consent from County, which consent will not be unreasonably withheld. During non-Prime Time, Provider may perform routine maintenance operations that do not require the System to be taken offline but may have immaterial effect on System performance and response time without any notice to County. Such degradation in performance and response time shall not be deemed network downtime. All changes that are expected to take more than four (4) hours to implement or are likely to impact user workflow require County's prior written approval, which will not be unreasonably withheld.

3.1.4 By the tenth day of each calendar month, Provider shall provide to County a report detailing Provider's performance under this SLA for the prior calendar month. To the extent the performance fails to meet the Network Uptime Guarantee, the report shall calculate: the total number of minutes of uptime for each of Prime Time and non-Prime Time; the total number of minutes for each of Prime Time and non-Prime Time minus any applicable Scheduled Maintenance, respectively; and the percentage of uptime versus total time minus Scheduled Maintenance for each (e.g., monthly minutes of non-Prime Time

network uptime / (Total minutes of non-Prime Time – Minutes of Scheduled Maintenance) = %).

3.1.5 Provider guarantees the functioning of all hardware components necessary for Provider to provide the Services and Service Availability herein, and will replace any failed or defective component at no cost to County. Downtime for the purpose of building redundancy or other recovery systems that is approved by County in advance shall not be charged as downtime in computing the Network Uptime Guarantee. Network downtime due to hardware failure is subject to the Network Uptime Guarantee.

3.2 Infrastructure Management

3.2.1 During Prime Time, Provider shall ensure packet loss of less than one percent (1%) and less than sixty (60) milliseconds domestic latency within Provider's network. Provider shall maintain sufficient bandwidth to the hosting sites and ensure the server processing time to provide millisecond response times from the server. County and Provider recognize that end user response times are dependent on intermittent ISP network connectivity, and in the case of County's users, dependent on County's internal network health.

3.2.2 Provider's Services shall support up to 500,000 site hits per calendar day to County's web pages and capture the number of site hits by page for performance to standards reporting.

3.2.3 Provider's Services shall ensure that an unlimited number of transactions may be processed to County production database, but Provider may recommend that non-routine reports and queries be limited to certain timeframes, quantities or other specifications if Provider determines that such reports and queries cause degradation to response times affecting performance levels established in the SLA.

3.2.4 Provider will retain all database records regardless of number or size.

3.2.5 Provider shall routinely apply upgrades, new releases, and enhancements to the System as they become available after prior, written approval by the County and shall ensure that these changes will not adversely affect the System.

3.2.6 To the extent Provider's System includes an ad-hoc reporting tool and/or standard reports, Provider agrees to provide unlimited access to such functionality to County. Provider agrees to support an unlimited number of queries and reports against County's data. County agrees that Provider may put reasonable size limits on queries and reports to maintain System performance, provided such limits do not materially impact County's regular business operations.

3.2.7 Provider shall conduct full, encrypted System backups (including System and user data) weekly and shall conduct incremental, encrypted backups daily. Encrypted backups will be written to a backup device with sufficient capacity to handle the data.

Provider shall maintain a complete current set of encrypted backups for County's System, including data, at a remote, off-site "hardened" facility from which data can be retrieved within one (1) business day at any point in time. Full System restoration performed as a recovery procedure after a natural disaster is included in Provider's Services under this Agreement. Upon County's request, Provider shall also provide restoration of individual file(s). Provider agrees that County may extract all County Data (as defined below) from Provider's database at will.

3.2.8 A development and test system, which shall mirror the production system, shall be made available for use by County for testing purposes upon two (2) business days' request, including without limitation, upon request for County's testing of application upgrades and fixes prior to installation in the production environment.

3.2.9 A demonstration/training system will be available for use by County upon two (2) business days' request. County may control data that is populated on the demonstration/training system by requesting that Provider:

a) periodically refresh data from production;
b) perform an ad-hoc refresh of data from production;
c) not refresh data from production until further notice from County; or
d) refresh data on an ad hoc basis with training data supplied by County.

3.3 Performance Monitoring and Hosting Capacity Increases

3.3.1 If requested by County, Provider shall provide standard reporting metrics to County on a monthly basis which shall include: traffic patterns by user and by time; server load, including Central Processing Unit ("CPU") load, virtual memory, disk and input/output ("I/O") channel utilization; Transmission Control Protocol ("TCP") load for each server allocated in part or in full to County System; and system errors in System, database, operating system, and each server allocated in part or in full to System.

3.3.2 In the event County anticipates an increase in transaction volume or seeks to expand capacity beyond the limitations, if any, provided under the Agreement, Provider will provide timeline and cost estimates to upgrade existing servers or deploy additional servers dedicated to County's System within fifteen (15) calendar days of written notice by County. Any incremental or additional costs shall be handled pursuant to the "Change of Scope" procedures in the Agreement.

4. Data

4.1 County shall also have the right to use the Services to provide public access to the data, files, or information derived from the use of the System, to generate reports from such data, files, or information, and to provide such data, files, or information on electronic media to the public where required or allowed by applicable law.

4.2 All data and information provided by County or its agents under this Agreement and

all results derived therefrom through the use of the System, whether or not electronically retained and regardless of the retention media (collectively "County Data"), are the property solely of County and may not be reproduced or used with the prior written consent of County. Provider and its subcontractors will not publish, transmit, release, sell, or disclose any County Data to any other person without County's prior written consent. The provisions of this Section 4.2 shall survive the termination or expiration of the Agreement.

4.3 In the event of any impermissible disclosure, loss or destruction of County Data, Provider must immediately notify County and take all reasonable and necessary steps to mitigate any potential harm or further disclosure, loss or destruction.

4.4 County shall have the option of receiving County Data at any time in any format, including, without limitation, Extensible Markup Language ("XML"), Structured Query Language ("SQL"), or in another format as may be mutually agreed to by County and Provider.

4.5 Upon the termination of this Agreement or the end of serviceable life of any media used in connection with this Agreement, Provider shall, at County's option, (a) securely destroy all media (including media used for backups) containing any County Data and County information and provide to County a signed certificate of destruction within ten (10) business days, and/or (b) return to County all County Data and provide a signed certification within two (2) business days, documenting that no County Data or information is retained by Provider in any format or media.

5. Transition/Disentanglement

5.1 Provider will complete the transition of any terminated Services to County and any replacement providers that County designates (collectively, the "Transferee"), without causing any unnecessary interruption of, or adverse impact on, the Services ("Disentanglement"). Provider will work in good faith (including, upon request, with the Transferee) at no additional cost to County to develop an orderly Disentanglement plan that documents the tasks required to accomplish an orderly transition with minimal business interruption or expense for County. Upon request by County, Provider shall cooperate, take any necessary additional action, and perform such additional tasks that County may reasonably request to ensure timely and orderly Disentanglement, which shall be provided at the rate(s) specified in the Agreement or, if no applicable rate is specified, at a reasonable additional fee upon written approval by the County. Specifically, and without limiting the foregoing, Provider shall:

a) Promptly provide the Transferee with all nonproprietary information needed to perform the Disentanglement, including, without limitation, data conversions, interface specifications, data about related professional services, and complete documentation of all relevant software and hardware configurations;

b) Promptly and orderly conclude all work in progress or provide documentation of work in progress to Transferee, as County may direct;

c) Not, without County's prior written consent, transfer, reassign or otherwise redeploy any of Provider's personnel during the Disentanglement period from performing Provider's obligations under this Agreement;

d) If applicable, with reasonable prior written notice to County, remove its assets and equipment from County facilities;

e) If County requests, and to the extent permitted under the applicable agreements, assign to the Transferee (or use its best efforts to obtain consent to such assignment where required) all contracts including third-party licenses and maintenance and support agreements, used by Provider exclusively in connection with the Services. Provider shall perform all of its obligations under such contracts at all times prior to the date of assignment, and Provider shall reimburse County for any losses resulting from any failure to perform any such obligations;

f) Deliver to Transferee all current, nonproprietary documentation and data related to County- owned assets and infrastructure. After confirming in writing with County that the applicable County data is received intact or otherwise securely stored by County, Provider shall securely erase all County data, including on any hard drives and backup media, to NIST standards. Upon written consent from County, Provider may retain one copy of documentation to the extent required for Provider's archival purposes or warranty support; and

g) To the extent requested by County, provide to County a list with current valuation based on net book value of any Provider-owned tangible assets used primarily by Provider in connection with the Services. County shall have the right to acquire any or all such assets for net book value. If County elects to acquire such assets for the net book value, any and all related warranties will transfer along with those assets.

For each section below that is checked (☒), Provider shall comply with the requirements of that section. If the section is not checked, those items are not applicable to Provider under this Agreement.

☐ **6. Managed Services/Professional Services (IT)/Third-Party Vendors**

6.1 Provider shall immediately notify the County of any terminations/separations of employees performing services under the Agreement or who had access to the County's network in order to disable such employees' access to County systems.

6.2 Provider shall ensure all Provider employees have signed County's Information Security Policy Acknowledgement form prior to accessing County network environment. (PCI 12.3.5)

6.3 Provider shall perform privacy and information security training to its employees with access to the sensitive County environment upon hire and at least annually. (PCI 12.6.1)

☐ **7. Software**

7.1. Provider must provide a security plan or secure configuration guide for Software installed in the County environment by the Provider.

7.2. Provider shall advise of any third party software (e.g., Java, Adobe Reader/Flash, Silverlight) required to be installed and version supported. Provider shall support updates for critical vulnerabilities discovered in the versions of third party software installed.

7.3. Provider shall ensure that the Software is developed based on industry standards/and or best practices, including following secure programming techniques and incorporating security throughout the software-development life cycle.

7.4. Provider shall ensure the Software has a security patch issued for newly identified vulnerabilities within 30 days for all critical or high security vulnerabilities.

7.5. Provider shall ensure the Software provides for role-based access controls.

7.6. Provider shall support electronic delivery of digitally signed upgrades from Provider or supplier website.

7.7. Provider shall enable auditing by default in software for any privileged access or changes.

7.8. If the Software is a payment application which processes, stores, or transmits credit card data, the VISA Cardholder Information Security Program ("CISP") payment Application Best Practices and Audit Procedures will be followed and current validation maintained.

7.9. Provider shall regularly provide County with end-of-life-schedules for all applicable Software.

☐ **8. Hardware Leased or Purchased from Vendor**

8.1 Provider shall ensure that physical security features are included in the Hardware acquired under this Agreement to prevent tampering.

8.2 Provider shall ensure security measures are followed during the manufacture of the Hardware acquired under this Agreement.

8.3 Any Hardware provided under this Agreement shall not contain any embedded remote control features unless approved in writing by County's Contract Administrator.

8.4 Provider shall disclose any default accounts or backdoors which exist for access to County's network.

8.5 If a new critical or high security vulnerability is identified, Provider shall supply a patch, firmware update or workaround approved in writing by County's Contract Administrator within 30 calendar days from identification of vulnerability.

8.6 Provider shall make available, upon County's request, any required certifications as may be applicable and required (e.g., Common Criteria ("CC"), Federal Information Processing Standard 140 ("FIPS 140)).

8.7 Provider shall regularly provide County with end-of-life-schedules for all applicable Hardware and Software.

8.8 Provider shall support electronic delivery of digitally signed upgrades from Provider or supplier website.

8.9 Upon County's request, Provider shall make available to the County proof of Provider's compliance with all applicable federal, state, and local laws, codes, ordinances, rules, and regulations in performing under this Agreement, including but not limited to: HIPAA compliance; Provider's latest compliance reports (e.g., PCI Compliance report, SSAE 16 report, International Organization for Standardization 27001 (ISO 27001) certification); and any other proof of compliance as may be required from time to time.