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 set forth in this Service Level Agreement ("SLA") for the duration of the Agreement. The standards set forth herein are intended to reflect the current industry best practices for the Application Service Provider ("ASP") hosting or Software as a Service ("SaaS") solution provided under this Agreement. If and to the extent industry best practices evolve to impose higher standards than set forth herein, SLA shall be deemed to impose the new, higher standards upon Provider. Provider shall promptly notify County in writing of any material change to its compliance with these standards. Any approval by County under this SLA may be approved in writing by the Contract Administrator or the Director of County's Division of Enterprise Technology Services ("ETS").

1. **Definitions**

1.1. "Provider Platform" means to the ASP or SaaS solution that constitutes the Services to the County, or otherwise stores, hosts, or transmits County Data. Provider shall maintain the same standards set forth herein for all of its data centers and facilities that store or host County data.

1.2. "County Data" means the data and information provided by County or its agents under this Agreement and all results derived therefrom through the use of the Provider's services, whether or not electronically retained and regardless of the retention media.

1.3. **Any other capitalized terms not defined herein refer to those defined terms in the Agreement.**

2. **Security**

2.1. **General**

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

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

2.1.3. Provider's procedures for the following must be documented and approved by County within 10 days of the Effective Date of the Agreement:

2.1.3.1. Evaluating security alerts and vulnerabilities;
2.1.3.2. Installing security patches and service packs;
2.1.3.3. Intrusion detection, incident response, and incident

escalation/investigation;

2.1.3.4. Access and authorization procedures and resetting access controls (e.g., password policy);

2.1.3.5. Risk analysis and assessment procedures;

2.1.3.6. User access and termination procedures;

2.1.3.7. Security log review;

2.1.3.8. Physical facility access controls; and

2.1.3.9. Change control procedures.

2.1.4. 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 SLA unless County, in writing, excuses specific compliance with any such term or condition. Provider shall provide County with a list of any such service providers, subconsultants or other third-parties on an annual basis, upon County's request, and promptly upon a material change in the composition of such entities.

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

2.1.6. Provider must mitigate critical or high risk vulnerabilities to the Provider Platform as defined by Common Vulnerability and Exposures (CVE) scoring system within 30 days of patch release. If Provider is unable to apply a patch to remedy the vulnerability, Provider must notify County of proposed mitigation steps to be taken and timeline for resolution.

2.2. **Controls**

2.2.1. Prior to the Effective Date of the Agreement, and at least once annually and upon request for the duration of this Agreement, Provider shall provide County with a copy of a current unqualified System and Organization Controls (SOC) 2 Type II, Report for the Provider, as well as any third party that provide hosting, SaaS, or data storage services for the Provider Platform, 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 implemented 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.

2.2.2. Provider shall maintain industry best practices for data privacy, security, and recovery measures including, but not limited to, disaster recovery programs, physical facilities security, server firewalls, virus scanning software, current security patches, user authentication, and intrusion detection and prevention. Unless otherwise provided in this

SLA, upon request by County, Provider shall provide documentation of such procedures and practices to County.

2.3. **Network Architecture/Security**

2.3.1. The Provider Platform 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 to the configuration diagram are subject to approval by County, which shall not be unreasonably withheld. Provider shall ensure that all database servers are protected behind a second set of internal firewalls.

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

2.3.3. Provider shall protect any Internet interfaces or web services 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.

2.3.4. Provider shall restrict inbound and outbound traffic to County network to "deny all, permit by exception" configuration.

2.3.5. Provider will support encryption using at a minimum Advanced Encryption Standard 256-bit encryption keys ("AES-256") or current industry security standards (whichever is higher) for the connection to the Provider Platform.

2.3.6. Provider's wireless networks connected to the Provider Platform shall be configured at a minimum using Wi-Fi Protected Access 2 (WPA2)-Enterprise, Advanced Encryption Standard (AES), and Protected Extensible Authentication Protocol (PEAP), current industry security standards (or whichever is higher) to secure and protect County data.

2.4. **Physical Architecture/Security**

2.4.1. Provider shall ensure the facilities that house the network infrastructure for the Provider Platform are physically secure against threats such as unauthorized access and natural and environmental hazards, and entry controls are in place to limit and monitor physical access to the Provider Platform.

2.4.2. Provider shall connect its hosting site for the Provider Platform through at least two (2) independent Internet Service Providers ("ISPs") with different Internet points of presence.

2.4.3. Provider shall ensure adequate background checks have been performed on any personnel having access to County data. To the extent permitted by such checks, Provider shall not knowingly allow convicted felons or other persons deemed by Provider to be a security risk to access County data. Provider shall provide privacy and information security training to its employees upon hire and at least once annually.

2.5. **Disaster Recovery**

2.5.1. Provider shall maintain a disaster recovery plan for the Provider Platform 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.

2.5.2. Provider shall conduct a disaster recovery test of Provider's hosted or SaaS system that comprises the Provider Platform under this Agreement on at least an annual basis, and shall notify County at least ten (10) days in advance of each such test. In addition, Provider shall conduct a disaster recovery test specific to the County, including County's data and utilization of the Provider Platform and County's network and data, in coordination with County at least once per year; the timing and duration of the County-specific test is subject to the approval of County.

2.6. **Incident Response**

2.6.1. If any unauthorized party is successful in accessing any information technology component related to the Provider Platform, including but not limited to servers or fail-over servers where County's data or files exist or are housed, Provider shall report to County within twenty-four (24) hours of becoming aware of such breach. 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. Provider shall not release County data or copies of County data without the advance written consent of County.

2.6.2. 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.

2.7. **County Data**

2.7.1. Provider shall maintain controls that ensure separation of County Data. Provider agrees to provide at a minimum Advanced Encryption Standard 256-bit encryption keys ("AES-256") or current industry security standards (or whichever is higher) 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.

2.7.2. Any County Data must be available to County upon request within one (1) business day, in any format reasonably requested by County, including, without limitation, Extensible Markup Language ("XML") and Structured Query Language ("SQL"), or in another format as may be mutually agreed to by County and Provider.

2.7.3. Upon termination or expiration of this Agreement or end of serviceable life of any media used in connection with this Agreement, and upon written notification from County that the applicable County Data is currently maintained by County or otherwise securely stored, Provider shall, at County's option, (a) securely destroy all media (including media used for backups) containing any County Data on all decommissioned hard drives or storage media to National Institute of Standards and Technology ("NIST") standards and provide to County a signed certificate of destruction within ten (10) business days, or (b) return to County all County Data and provide a signed certification within two (2) business days documenting that no County Data is retained by Provider in any format or media.

2.7.4. County Data is the property solely of County and may not be reproduced or used by Provider with the prior written consent of County. Provider and its subcontractors will not publish, transmit, release, sell, or disclose any County Data to any third party without County's prior written consent.

2.7.5. County shall have the right to use the Services to provide public access to County Data as County deems appropriate or as otherwise required by law.

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

3. **Compliance**

3.1. Provider shall cooperate and provide any information requested by County relating to compliance and regulatory requirements. A request for information or review by

County may include, but is not limited to, the following:

3.1.1. Vulnerability scans of authenticated and unauthenticated operating systems/networks, web applications, and database applications;

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

3.1.3. 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 monthly or periodic network traffic and firewall activity logs; and

3.1.4. Physical inspection of Provider's facilities by County or its representatives.

3.2. Provider shall provide County with the ability to generate account reports consisting of the account holder's name and application access rights.

3.3. 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.

3.4. 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.

3.5. Upon request by County, Provider shall promptly 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), time-stamped application and platform environment change control logs, and time-stamped data backup logs indicating the backup type (e.g., full, incremental, etc.).

3.6. 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.

4. Service Availability

4.1. System Availability

4.1.1. Provider guarantees that the Network Uptime (as defined herein) 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 is the time that the System and Services are functioning optimally and fully operational, and requires proper functioning of all network infrastructure, including routers, switches, and cabling, affecting a user's ability to reliably transmit or receive data; Network Downtime is the remainder of time that is not included in Network Uptime, and is measured from the time the trouble ticket is opened to the time the network is fully restored. As long as the System is available over the Internet to at least two other comparable non-County customers (i.e., the System is functioning properly and there are no technical issues with Provider or the Provider Platform), any inability on the part of County to access the System as a result of a general Internet outage will not be counted toward Network Downtime. System unavailability 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 Downtime. System unavailability due to Provider's equipment failure constitutes Network Downtime.

4.1.2. 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 Network Downtime in excess of that permitted under the Network Uptime Guarantee (up to 100% of County's monthly or pro rata 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 or future invoice.

4.1.3. 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 without advance notice only with 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 effects 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.

4.1.4. 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) = %).

4.1.5. Provider guarantees the functioning of all equipment components necessary for Provider to provide the Services, the Provider Platform, and meet System availability requirements stated in this SLA.

4.2. **Infrastructure Management**

4.2.1. During Prime Time, Provider shall ensure packet loss of less than one percent (1%) and less than sixty (60) milliseconds domestic latency within the Provider Platform. Provider shall maintain sufficient bandwidth to the Provider Platform and ensure the server processing time (or CPU processing capacity) 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.

4.2.2. To the extent the Provider Platform provides or supports public access to users in Broward County or through the County's web pages, Provider's Services shall support up to 500,000 site hits per calendar day and capture the number of site hits by page for performance to standards reporting.

4.2.3. Provider shall ensure that an unlimited number of transactions may be processed to County production database. Subject to County approval, 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 this SLA.

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

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

4.2.6. To the extent the Provider Platform includes an ad-hoc reporting tool 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.

4.2.7. 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 County 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 as part of Provider's required Services under this Agreement. Upon County's request, Provider shall also provide restoration of individual file(s).

4.2.8. A development and test system, which shall mirror the production system, shall be made available for use by County for testing or training 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. County may control data that is populated on the demonstration and training system by requesting that Provider perform any or all of the following:

4.2.8.1. periodically refresh data from production;
4.2.8.2. perform an ad-hoc refresh of data from production;
4.2.8.3. not refresh data from production until further notice from County; or
4.2.8.4. refresh data on an ad hoc basis with training data supplied by County.

4.3. **Performance Monitoring and Hosting Capacity Increases**

4.3.1. If requested by County, Provider shall provide standard reporting metrics of the Provider Platform to County on a monthly basis which shall include: traffic patterns by user and by time; server load, including central processing unit load, virtual memory, disk and input/output channel utilization; transmission control protocol 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.

4.3.2. 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.

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:

5.1.1. 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 equipment configurations;

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

5.1.3. 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;

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

5.1.5. 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;

5.1.6. 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, in accordance with 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

5.1.7. 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.

6. Payment Card Industry (PCI) Compliance

If and to the extent the Provider Platform accepts, transmits or stores any credit cardholder data County or is reasonably determined by County to potentially impact the security of County's cardholder data environment ("CDE"), the following provisions shall apply:

6.1. Provider shall comply with the most recent version of the Security Standards Council's Payment Card Industry ("PCI") Data Security Standard ("DSS").

6.2. Prior to the Effective Date, after any significant change to the CDE, and annually Provider shall provide to County:

6.2.1. A copy of their Annual PCI DSS Attestation of Compliance ("AOC");

6.2.2. 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.

6.2.3. 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.

6.3. Provider shall follow the VISA Cardholder Information Security Program ("CISP") payment Application Best Practices and Audit Procedures and maintain current validation.

6.4. If Provider subcontracts or in any way outsources the CDE processing, or provides an API which redirects or transmits County Data to a payment gateway, Provider is responsible for maintaining PCI compliance for their API and providing the AOC for the subcontractor or payment gateway to the County.

6.5. Mobile payment application providers must follow industry best practices such as VISA Cardholder Information Security Program ("CISP") or OWASP for secure coding and transmission of payment card data.

6.6. 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.

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

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

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

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

6.11. 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)

6.12. All inbound and outbound connections to County's CDE must use Transport Layer Security (TLS) 1.2 or current industry equivalent (whichever is higher).

7. Managed Services/Professional Services (IT)/Third-Party Vendors

7.1. Provider shall immediately notify County of any terminations or separations of Provider's employees who performed Services to County under the Agreement or who had access to the County's Data and must ensure such employees' access to County Data and network is promptly disabled.

7.2. Provider shall ensure all Provider's employees with access to County environment have signed County's Information Resources User Acknowledgement form prior to accessing County network environment.

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

8. **Software Installed in County Environment**

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

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

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

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

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

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

9. **Equipment Leased or Purchased from Provider**

9.1. Provider shall ensure that physical security features are included in the Equipment acquired under this Agreement to prevent tampering. Provider shall ensure security measures are followed during the manufacture of the Equipment provided under this Agreement. Any Equipment provided under this Agreement shall not contain any embedded remote control features unless approved in writing by County's Contract Administrator.

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

9.3. Provider shall regularly provide County with end-of-life-schedules for all applicable Equipment.

9.4. Provider shall support electronic delivery of digitally signed upgrades of any applicable Equipment firmware from Provider or supplier website.