

## **Service Level Agreement**

In connection with all Services provided to County under the applicable contract (the "Agreement"), Contractor 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 Contractor Platform provided by Contractor under this Agreement. If and to the extent industry best practices evolve to impose higher standards than set forth herein, this SLA shall be deemed to impose the new, higher standards upon Contractor. Contractor shall promptly notify County in writing of any material change to its compliance with these standards. Any approval required by County under this SLA may be issued in writing by the Contract Administrator or the Broward County Chief Information Officer ("CIO").

Sections 1-5 of this SLA apply to all aspects of the Contractor Platform. In addition, Sections 6 and 7 of this SLA apply to any Software as a Service ("SaaS") or web hosting services provided to County under the Contractor Platform.

### **1. Definitions**

1.1. Contractor Platform means any and all SaaS or web hosting to be provided by Contractor under the Agreement, including any system or other solution that stores, hosts, or transmits County Data. Contractor shall maintain the same standards set forth herein for its data centers and facilities that store or host County Data.

1.2. County Data means the data and information (including text, pictures, sound, graphics, video and other medium) relating to County or its employees or agents, or made available or provided by County or its agents to Contractor, for or in the performance of this Agreement, including all derivative data and results derived therefrom, whether or not derived through the use of the Contractor's services, whether or not electronically retained, and regardless of the retention media.

Any other capitalized terms not defined herein refer to those terms as defined in the Agreement, if so defined; if not defined in the Agreement, any other capitalized terms shall have their plain language meaning as used in the applicable context.

### **2. Security**

#### **2.1. General**

2.1.1. Contractor will ensure that County can authenticate all access by username/password and Multi-Factor Authentication (MFA). Upon request, Contractor shall restrict access to County Data to a specific source static IP address. Contractor shall ensure that separation of duties and least privilege access are enforced for privileged or administrative access to County Data and the Contractor

Platform. Contractor's procedures for the following must be documented and made available upon request by County, including:

- 2.1.1.1. Evaluating security alerts and vulnerabilities;
- 2.1.1.2. Installing security patches and service packs;
- 2.1.1.3. Intrusion detection, incident response, and incident escalation/investigation;
- 2.1.1.4. Access and authorization procedures and resetting access controls (e.g., password policy);
- 2.1.1.5. Risk analysis and assessment procedures;
- 2.1.1.6. User access and termination procedures;
- 2.1.1.7. Security log review;
- 2.1.1.8. Physical facility access controls; and
- 2.1.1.9. Change control procedures.

2.1.2. Contractor shall ensure that its service providers, Subcontractors, and any third parties, including any data hosting providers, performing any Services related 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. Contractor shall provide County with a list of any such service providers, Subcontractors or other third parties on an annual basis, upon County's request, and promptly upon a material change in the composition of such entities.

2.1.3. If a new or unanticipated vulnerability to the Contractor Platform is discovered by either County or Contractor, or if existing technical controls have ceased to function properly, the discovering party shall immediately notify the other party.

2.1.4. When technically feasible, for all software used, furnished, or supported under the Agreement, Contractor shall review such software to find and remediate security vulnerabilities during initial implementation and upon any significant modifications and updates to same.

2.1.5. Contractor must mitigate critical or high-risk vulnerabilities (as defined by Common Vulnerability and Exposures scoring system) to the Contractor Platform within 30 days after patch release. If Contractor is unable to apply a patch to remedy the vulnerability, Contractor must promptly notify County of proposed mitigation steps to be taken and develop and implement an appropriate 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, Contractor shall provide County with a copy of a current unqualified System and Organization Controls (SOC) 2 Type II,

Report for Contractor's Organization or application, as well as any third party that provide hosting, SaaS, or data storage services for the Contractor Platform, inclusive of all five Trust Service Principles (Security, Availability, Processing Integrity, Confidentiality, and Privacy), unless the County's Chief Information Officer in their sole discretion approves other documentation of appropriate security controls implemented by Contractor. If the audit opinion in the SOC 2, Type II report is qualified in any way, Contractor shall provide sufficient documentation to demonstrate remediation of the issue(s) to the satisfaction of the County's Chief Information Officer.

2.2.2. Contractor 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. Upon request by County, Contractor shall provide documentation of such procedures and practices to County. Contractor shall utilize industry standard security measures to safeguard against unauthorized access to the Contractor Platform.

2.2.3. Contractor shall utilize antivirus protection software, updated and currently supported operating systems, firmware, third party and open source application patches, and firewalls to protect against unauthorized access to the Contractor Platform. Contractor shall conduct penetration testing internally and externally at least annually and after any significant infrastructure or application upgrade or modification to the Contractor Platform. Upon request, provide a letter attesting that Contractor performed the penetration testing and findings, if any, were remediated.

### 2.3. Network Architecture/Security

2.3.1. Contractor 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. Contractor 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 between any user or County network to the Contractor Platform.

### 2.4. Physical Architecture/Security

2.4.1. Contractor shall ensure the facilities that house the network infrastructure for the Contractor 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 Contractor Platform. Contractor shall ensure adequate background checks are routinely performed on any personnel with access to County Data. Contractor shall not knowingly allow convicted felons or

other persons deemed by Contractor to be a security risk to access County Data. Contractor shall provide privacy and cybersecurity training to its employees upon hire and at least once annually.

## 2.5. Incident Response

2.5.1. Contractor shall report any cybersecurity incident or random incident (as those terms are defined in Section 282.0041, Florida Statutes) impacting or relating to County Data (including but not limited to servers or fail-over servers) to County, including the details required by Section 282.3185(5)(a), in sufficient time to reasonably permit County to timely comply with any required reporting under Section 282.3185(b) and no later than twenty-four (24) hours after becoming aware of such breach (or such shorter time period as may be required under applicable law), unless an extension is granted by County's CIO. Contractor shall provide County with a detailed incident report within five (5) days after becoming aware of the breach, including remedial measures instituted and any law enforcement involvement. Contractor shall fully cooperate with County on incident response, forensics, and investigations into Contractor's infrastructure as it relates to any County Data or County applications.

2.5.2. Prior to the Effective Date of this Agreement, Contractor 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 cybersecurity incidents. Upon request by County, Contractor shall deliver to County in electronic form the website application activity such as logs of visits and user logins and logoffs by or on behalf of County on the Contractor Platform. County may, at its sole discretion, terminate all access to the Contractor Platform.

## 2.6. County Data

2.6.1. Contractor shall maintain controls that ensure logical separation of County Data from non-County data. Contractor agrees to provide at a minimum Advanced Encryption Standard 256-bit encryption ("AES-256") or current industry security standards (or whichever is higher) for all County Data that includes employee information, financial information, social security numbers, bank account numbers, username with passwords or security questions, cardholder data, or any other protected data such as Protected Health Information ("PHI") and Personally Identifiable Information ("PII"), and any other data as may be directed by County, and 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. Contractor shall also ensure that the encryption key(s) are not stored with the encrypted data and are secured by a Hardware Security Module ("HSM"). Contractor shall immediately notify County of any compromise of any encryption key. Contractor shall provide a copy of County's encryption key(s) at County's request. Contractor shall

prohibit the use of unencrypted protocols such as FTP and Telnet for the data identified in this paragraph.

2.6.2. 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, Contractor 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 thereafter documenting that no County Data is retained by Contractor in any format or media.

2.6.3. County shall have the right to use the Products and Services and the Contractor Platform to provide public access to County Data as County deems appropriate or as otherwise required by law. County Data is the property solely of County and may not be reproduced or used by Contractor without County's prior written consent. Contractor and its Subcontractors will not publish, transmit, release, sell, or disclose any County Data to any third party without County's prior written consent. Contractor shall not modify or alter County Data (other than modifications strictly necessary to upload County Data to the Contractor Platform) without County's prior written consent. In the event of any impermissible disclosure, loss, or destruction of County Data caused in whole or in part by any action or omission of Contractor, Contractor must immediately notify County and take all reasonable and necessary steps to mitigate any potential harm, further disclosure, loss, and destruction.

### 3. Compliance

3.1. Contractor shall cooperate and provide any information requested by County relating to compliance and regulatory requirements, and will, upon request:

3.3.1. Provide a letter attesting that the Contractor performed vulnerability scans of authenticated and unauthenticated operating systems/networks, web applications, database applications, and the Contractor Platform;

3.3.2. Provide Contractor's architecture documents, cybersecurity policies and procedures (redacted, if necessary), and general network security controls documentation such as firewalls, Intrusion Detection System ("IDS"); and

3.3.3. Permit County to conduct a physical inspection of Contractor's facilities, but only to the extent such inspection is related to the security of and access to County Data or the Contractor Platform.

3.2. Contractor shall provide County with the ability to generate: account reports consisting of the account holder's name and application access rights; account management reports showing new users, access rights changes, and account termination with the associated time stamp information; and 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. Upon request by County, Contractor 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.).

3.3. Upon County's request, Contractor shall make available to County proof of Contractor'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; Contractor'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. Infrastructure Management

Contractor shall ensure that an unlimited number of transactions may be processed to the County production database. Subject to County approval, Contractor may recommend that non-routine reports and queries be limited to certain timeframes, quantities, or other specifications, if Contractor determines that such reports and queries cause degradation to response times affecting performance levels established in this SLA. Contractor shall routinely apply upgrades, new releases, and enhancements to the Contractor Platform as they become available and shall ensure that these changes will not adversely affect the Contractor Platform or County Data. A development and test system, which shall mirror the production system, shall be made available for use by County for testing or training purposes, including without limitation, 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 Contractor perform any or all of the following: periodically refresh data from production; perform an ad-hoc refresh of data from production; not refresh data from production until further notice from County; or refresh data on an ad hoc basis with training data supplied by County.

#### 5. Transition/Disentanglement

5.1. Contractor will complete the transition of any terminated Services or Support and Maintenance to County and any replacement provider(s) that County designates (collectively, the "Transferee"), without causing any unnecessary interruption of, or adverse impact on, the Services, County Data, or the ongoing business operation of County ("Disentanglement"). Contractor 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, Contractor 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 County.

Specifically, and without limiting the foregoing, Contractor 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. Refrain, without County's prior written consent, from transferring, reassigning, or otherwise redeploying any of Contractor's personnel during the Disentanglement period to the extent such action would impede performance of Contractor's obligations under the 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 Contractor exclusively in connection with the Services or Support and Maintenance.

5.1.6. Deliver to Transferee all current, nonproprietary documentation and data related to County-owned assets and infrastructure; and

5.1.7. To the extent requested by County, provide County a list with current valuation based on net book value of any Contractor-owned tangible assets required to make the Contractor Platform available to County. 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, Contractor shall use best efforts to ensure that any and all related warranties will transfer along with those assets.

## 6. Network Architecture/Security

### 6.1. Network Architecture

6.1.1. The Contractor Platform shall be protected behind a layer of firewalls utilizing a high-availability (HA) design. At County's request, Contractor shall submit a network architecture diagram of County's stored and transmitted data, including the location of the data center and details of connectivity for all third parties who have access to County Data. Any network security changes implemented by Contractor must not compromise the security of County Data. Using a tiered design, Contractor shall ensure that all database servers are protected behind a second set of internal firewalls. Contractor shall restrict inbound and outbound traffic to County's network to "deny all, permit by exception" configuration.

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

## 6.2. Disaster Recovery

6.2.1. Contractor shall maintain a disaster recovery plan for the Contractor 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. Contractor shall conduct a disaster recovery test of the hosted or SaaS system that is utilized by or comprises the Contractor Platform on at least an annual basis, and shall notify County at least ten (10) days in advance of each such test. In addition, Contractor shall conduct a disaster recovery test specific to County in accordance with a documented procedure (runbook), including testing County Data and all elements of the Contractor Platform, 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.

## 6.3. County Data.

6.3.1. Contractor shall make any County Data available to County upon request within one (1) business day and 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 by County and Contractor.

## 7. Service Availability

### 7.1. System Availability

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



7.1.2. Contractor 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 Contractor Platform and System are functioning optimally and fully operational, and requires proper functioning of all network infrastructure, including firewalls, 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 Contractor Platform and System are 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 Contractor or the Contractor Platform), any inability on the part of County to access the System as a result of a general documented 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. Contractor Platform or System unavailability due to Contractor’s equipment failure constitutes Network Downtime.

7.1.3. Contractor 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 after the applicable monthly report or, at County’s option, may be credited against amounts due under any unpaid invoice or future invoice. If the Agreement provides for other credit or compensation due to County for an event that also constitutes Network Downtime, the greater of the two amounts shall apply.

7.1.4. Normal availability of the Contractor Platform and 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. Contractor 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, Contractor may perform routine maintenance operations that do not require the Contractor Platform or System to be taken offline but may have immaterial effects on performance and response time without any notice to County. Such immaterial 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.

7.1.5. By the tenth day of each calendar month, Contractor shall provide County a report detailing Contractor'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) = \_\_%).

## 7.2. Infrastructure Management

7.2.1. During Prime Time, Contractor shall ensure packet loss of less than one percent (1%) and less than sixty (60) milliseconds domestic latency within the Contractor Platform. Contractor shall maintain sufficient bandwidth to the Contractor Platform and ensure the average response time of the platform from the server remains between 200 millisecond and one second. County and Contractor 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.

7.2.2. To the extent the Contractor Platform provides or supports public access to users in Broward County or through the County's web pages, the Contractor Platform 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. Contractor will retain all County-related database records regardless of number or size.

7.2.3. To the extent the Contractor Platform includes an ad-hoc reporting tool or standard reports, Contractor agrees to provide unlimited access to such functionality to County. Contractor agrees to support an unlimited number of queries and reports against County Data. County agrees that Contractor 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.

7.2.4. Contractor shall conduct full, encrypted 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. Contractor shall retain a complete current set of encrypted backups for County's System, including County Data, with a retention period of at least 30 days, 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 the required performance by Contractor under this Agreement. Upon County's request, Contractor shall also provide restoration of individual file(s).

### 7.3. Performance Monitoring and Hosting Capacity Increases

7.3.1. If requested by County, Contractor shall provide standard reporting metrics of the Contractor 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 the System, database, operating system, and each server allocated in part or in full to the System.

7.3.2. If County anticipates an increase in transaction volume or seeks to expand capacity beyond the limitations, if any, provided under the Agreement, Contractor will provide timeline and cost estimates to upgrade existing servers or deploy additional servers dedicated to County's System within fifteen (15) calendar days after written notice by County.