Exhibit 1 – Hosting and/or Cloud Services and Security Standards ("Hosting Security Exhibit")

1. **Virtual Infrastructure/Cloud Services**. In addition to the Contractor responsibilities listed in the Agreement by and between the Parties, Contractor acknowledges and agrees to assume the following additional responsibilities:

   1.1. **Connectivity**. Contractor will provide the connectivity as described in in the Agreement.

   1.2. **Load Balancing**. Contractor will load balance the County applications to meet the needs of the County's operations, as may be further described in the County's system architecture specifications, or as mutually agreed to by the Parties.

   1.3. **Security**. Contractor will implement reasonable and appropriate systems and procedures sufficient to ensure the security and confidentiality of the County Data, as further specified herein. County Data is defined as the data described in the Data Practices section of this Professional Services Agreement.

   1.4. **SOC 2**. Contractor will provide the Services utilizing a SOC 2 compliant data center located in the continental United States. Contractor will perform periodic audits (SOC 2 or other industry equivalent standard mutually agreed to by the Parties) of Contractor's security controls (i.e., physical and logical security, network configuration, change/problem and vulnerability management and recovery services), and make available to the County a copy of such SOC 2 report and, upon the County's request, written reports regarding such audits. In the event of any qualified statements in such reports that materially impact the County, the County may immediately terminate the Agreement for material breach without further period to cure.

   1.5. **Back-up Services**. Contractor shall perform daily backups.
   Contractor will perform daily backups in accordance of section 16 below. The Contractor will retain backup data within a SOC 2 compliant environment within the continental United States for up to 2 years. Backups will be encrypted in storage. In addition, Contractor will fulfill restoration requests as directed by the County due to site failures. Restoration will be performed within the interval of two to four hours depending on the urgency of the request; and the agreed upon location of the desired back-up media; and if the location is expected to be down for more than 24 hours, Contractor will immediately transfer appropriate back-up data and re-establish all hosting operations in an appropriately functioning secondary server or location.

   1.6. **Anti-Virus Software**. Contractor will install and maintain industry standard anti-virus and anti-spyware software for all physical and virtual servers used to provide the Services.

   1.7. **Fix Errors**. Contractor will use Contractor's best efforts to promptly remedy any failure of the Services.

2. **Multi Factor Authentication**. Contractor will utilize a secure, multi-factor method of remote authentication and authorization to access the system(s).

3. **Monitoring Services.** Contractor will provide the following additional Services with respect to system monitoring:

3.1. Access. Contractor will provide access to Contractor's client portal, monitoring and alerting of the County's servers, as well as the processes and services being executed by such servers by Contractor's Network Operations Center on a 24 x 7 x 365 basis In addition, the County will be provided with access to Contractor's Network Operations Center, which allows for 24x7x365 access to support requests, open ticket status, reporting and a knowledge base of previous County issues and projects.

3.2. Monitoring and Detection. Contractor will provide monitoring and alerting by Contractor's Network Operations Center on a 5x8 basis with after hours alerting for critical events.

3.3. Equipment Monitored. The County requests that the Services be provided to cover the computer related items detailed on any network and infrastructure equipment inventory list maintained by Contractor in any County provided disaster recovery guidelines.

3.3.1 Additional Equipment. If the County has or purchases additional equipment, the monthly fee for Services will automatically be increased at the beginning of the following month to cover the additional equipment. Additional equipment must be inspected and certified as "fit for purpose" by Contractor before it is covered under this Hosting Security Exhibit.

3.3.2 Equipment Retirement. If the County retires equipment that is not replaced in kind, the monthly fee for Services will automatically be decreased at the beginning of the next month to account for the decrease in the need for support. The County must notify Contractor of the equipment retirement date via e-mail.

3.3.3. County To Provide Access. The County will provide full and complete access, including admin usernames and password, to all equipment covered under this Hosting Security Exhibit.

3.4. Notification. Contractor will notify the County of disruption in any Services for which Contractor is providing monitoring.

3.5. Fix Issues. Contractor will promptly apply a fix to any disruption in the Services.

3.6. Communication with Network Operations Center. The County may communicate with the Contractor's customer support center via telephone, email, or client portal ticket 24 hours a day, seven days a week and 365 days a year.

3.7. Initiation of Client Portal Tickets. Unless stated otherwise, client portal tickets are initiated or escalated within 2 hours receipt.

4. Operating System Patch Services. Contractor will provide the following Services with respect to operating system Patches:

4.1. Patch Monitoring Services. Contractor will monitor recommendations from software vendors relating Patches (defined below) to software used in one or more Services.

4.2. Installation Services. Contractor will install Patches at a time appropriate to their risk level, which may include considering the following factors: any possible disruption to the Services, and the urgency of the need to install the Patch.

4.3. Notification. Contractor will notify and coordinate a maintenance window with the County for any Patch management installations that impact agreed upon SLAs

4.4. Definition of Patch. For the purposes of this Hosting Security Exhibit, the term "Patch" means platform and applications software security and anti-virus updates and other software fixes and updates issued by and recommended for installation by software vendors for Software used in one or more Services.

5. Security Standards. Contractor shall comply with all security measures and policies as outlined in the Agreement as well as Contractor's data privacy, security policies, client guide and/or Information Security Policy, and security procedures that apply to county data, which have been provided to the County and are herewith included herein by reference. In the event Contractor materially degrades the information security standard during any such modification, such degradation shall constitute a material breach by Contractor under the Agreement Contractor will comply with applicable U.S. laws and regulations concerning information security, the US-EU Privacy Shield Framework as established by the United States Department of Commerce and conduct SSAE 16 audits (or SOC 2) at least annually, or in the event it is superseded, the resultant SSAE 16 equivalent.

6. Security Program. Contractor agrees and represents that it currently maintains information protection practices and procedures ("Security Program") that complies with industry best practice and applicable privacy laws. Contractor's Security Program includes, at a minimum:

6.1. Appropriate administrative, technical, and physical safeguards and other security measures designed to ensure the security and confidentiality of County Data;

6.2. A security design intended to prevent any compromise of Contractor's own information systems, computer networks or data files by unauthorized users, viruses, or malicious computer programs which could in turn be propagated to County;

6.3. Appropriate internal practices including, but not limited to, encryption of data in transit and at rest; using appropriate firewall and antivirus software; maintaining these countermeasures, operation systems and other applications with up-to-date virus definitions and security patches so as to avoid any adverse impact to County's systems or information; appropriate logging and alerts to monitor access controls and assure data integrity and confidentiality; installing and operating security mechanisms in the manner intended sufficient to ensure County government operations must not be disrupted; permitting only authorized users access to systems and applications; and preventing unauthorized access to County systems via the Contractor's networks and access codes; and

6.4. All persons with authorized access to County Data must have a documented genuine need-to-know prior to access;

6.5. Contractor warrants that the services and deliverables will not contain, and Contractor, its employees or Contractor's Agents will not introduce through data transmission or any other means, any virus, ransomware, malware, spyware, bomb, worm, trap door, back door, Trojan horse, malicious logic, drop dead device, software lock, disabling code or any other contaminant, program routine or disabling device, including without limitation, any key, timer, clock, counter, local shared object/flash cookies or other self-

enacting device or limiting routines, codes, commands, or instructions or other feature that may have the effect or that could be used to access, track activity on, alter, delete, damage, deactivate, interfere with, disable or otherwise harm any service or deliverable or the County owned, licensed and/or leased computer hardware, software, code, systems, data, compilations of data, or other property.

7. Source Code Protection. Contractor will have in place and will maintain an industry standard security program which protects Contractor's source code from a compromise by Contractor's subcontractors or any other third party.

8. Audit. County may conduct a security review of Contractor's Security Program when determined as reasonably required by County. Contractor will provide County copies of its data privacy and security policies and procedures that apply to County Data. Subject to reasonable notice, Contractor shall provide County an opportunity to conduct a privacy and security audit of Contractor's Security Program and systems and procedures that are applicable to the Services provided by Contractor to County. Such audit may be conducted on-site by County personnel or County's contracted third party assessors or through surveys and interviews, at the option of County. In the event that Contractor has any security audits or review of its own systems performed by Contractor or a third party, including vulnerability and penetration assessments, it will give County notice of any current findings that are likely to adversely impact County Data and will keep County timely informed of its remediation efforts. If the audit reveals any vulnerability, Contractor shall correct such vulnerability at its sole cost and expense and shall certify the same in writing to County. Contractor shall use best efforts to correct all vulnerabilities and provide County a report explaining corrective actions immediately but no later than within thirty (30) days of completion of the audit, unless County agrees in writing otherwise. Contractor's failure to procure audits or to complete corrections in a timely manner will be a material breach of the Agreement.

9. Mobility and Transfer of Data. No Confidential Information, CPI, CPM or County Data shall be stored, transported, or kept on a laptop or any other mobile device or storage media, including USB, "thumb drives," DVDs, CDs, unless encrypted using an encryption methodology approved in writing by County. All electronic data transfers of County Data must be via secure FTP or other County approved protocol and/or in approved encrypted form. Any physical removal or transfer of County Data from County's or Contractor's facilities shall be conducted only according to controls developed or approved by County.

10. Security Certification. Contractor must maintain a level of security certification or assessment consistent with best practices and by a qualified third party reasonably acceptable to County. Such certifications shall be provided to County as reasonably requested by County.

11. Segmentation. Contractor warrants that all County Data is maintained so as to preserve segmentation of County Data from data of others.

12. Controls. The County agrees that Contractor is solely responsible for all testing and auditing, including port scanning and penetration testing, of Contractor security controls. Contractor shall provide results of such testing as requested by the County.

13. Penetration Testing. Penetration testing of the Contractor's architecture is included at a frequency of one per year at no additional cost. Contractor will coordinate with the current

Contractor penetration testing vendor and shall use best efforts to remedy any critical issues identified immediately but no later than within thirty (30) days of reporting. At the County's request Contractor will provide a sanitized final report to the County once it has been verified it does not contain information related to any other clients. Contractor's failure to remedy and report the remedy in a timely manner will be a material breach of the Agreement. Additional penetration tests or the County specific penetration tests will be at the expense of the County and will be arranged through Contractor's vendor for penetration testing.

14.Security Policies. Contractor's security policy is as identified in its SOC 2 report and is made up of the following documents:

- Acceptable use
- Access control
- Backup and restoration
- Business continuity and disaster recovery
- Change management
- Corporate ethics
- Customer support and SLA
- Data retention and disposal
- Disciplinary
- Incident management
- Information security
- Key management and cryptography
- Network security
- Personnel security
- Privacy policy for websites
- Risk assessment
- Server Security
- Serverless security
- Software development
- Vendor management
- Vulnerability and penetration testing management
- Workstation and mobile device

15. Hosting Security Standards. The hosting security standards for the Contractor or Contractor's Agent's data center(s) (the "Data Center") include:

- Physical Security
    1. Video cameras
    2. Motion sensors
    3. Fire sensors
    4. Locked doors with controlled access
    5. Manned reception area
    6. Visitor log

There are no external windows in the Data Center. In the Data Center, all physical equipment is owned or leased by Contractor and/or Contractor's Agent and is subject to terms herein for all

such hosting services including without limitation the secure management and monitoring of all components of the Services provided. Exterior perimeter walls, doors, windows and the main interior entry door to the raised floor environment are constructed of materials that afford UL rated ballistic protection. Vegetation and other objects within the Data Center are maintained such that an intruder would not be concealed.

Physical access mechanisms (e.g. access cards, biometric devices, man-traps and portals) have been implemented and are administered by local operations staff to help ensure that only authorized individuals have the ability to access the Data Center. Portals and Tdar man-traps have been installed as an anti-tailgating measure in the Data Center lobby. All access into and out of the Data Center is through either a portal or Tdar man-trap. The portal/man-trap bypass doors are only to be used in the event an individual is unable to use the portal or. man-trap. Examples include handicap, phobia or other restrictions on a case-by-case basis. Tours and emergency Data Center security operations crews will be permitted to use the Portal bypass door, when necessary. All security systems have dedicated 24x7 UPS systems and standby emergency power support.

The Data Center incorporates video cameras, motion sensors, fire sensors, locked doors with controlled access, manned reception area, visitor log, and glass break sensors in the Data Center. There are no external windows in the Data Center. Video cameras are used in the front entrances, emergency exits, secure areas, main lobby, elevators, general employee areas, within the Data Center and monitoring the grounds and parking lots around the Data Center. Security monitoring is recorded to digital files with a 90 day retention. Tapes are rotated every 30 days and are stored offsite. Motion sensors are located on the roof and are armed 24x7. The Data Center utilizes on-site and remote monitoring centers and both are manned 24x7.

The Data Center requires a key-card for entry. Only three designated employees are permitted to open the door to accept shipments or greet visitors. The Data Center is staffed from 6 a.m. to 7 p.m. weekdays. Security guards patrol the building during unstaffed hours. Video cameras are positioned in the areas surrounding the Data Center. All visitors must sign in and be escorted at all times.

All persons requesting access into the Data Center must be positively identified. This process requires the requesting person to submit valid (unexpired) Government issued photographic ID at the desk and sign in and out of the Data Center. Visitors must be approved by Contractor's personnel prior to arriving at the Data Center. The Data Center incorporates secure badges, secure visitor badges, and biometrics. All visits must be arranged in advanced, and all visitors are escorted at all times.

- Network Security

    1. Every connection to an external network is terminated at a firewall.
    2. Network devices are configured to prevent communications from unapproved networks.
    3. Network devices deny all access by default.
    4. Security patches are regularly reviewed and applied to network devices.
    5. Contractor follows a strict change management process which incorporates Change Advisory Board review and approvals.

6. Communication through a network device is controlled at both the port and IP address level.
7. There is a documented standard for the ports allowed through the network devices.
8. Contractor prevents unauthorized devices from physically connecting to the internal network.
9. There is an approval process to allow the implementation of extranet connections.
10. Contractor manages a SIEM (Security Information and Event Management) tool to review any potential security, infrastructure and vulnerabilities.
11. Contractor subscribes to Contractor's Agent's dedicated NIDS service and 24 x 7 incident response to monitor and respond to intrusion attempts.
12. The Data Center is compliant with SOC-1 and SOC-2.

16. Backup. Contractor uses daily on-site backups that are maintained within cloud-based storage solutions. All of the County Data will be contained in a distinct database that will follow the backup process set forth in the Agreement. Some systems are not backed up because they do not contain any useful data and the recovery process is to rebuild these systems.

- Full backups of the County's repositories are performed daily.
- Incremental backups are performed every hour.

17. Disaster Recovery. Contractor's Disaster Recovery plan is structured in a recovery team format. This format increases the efficiency by allowing departments to be recovered concurrently. The plan provides critical recovery solutions, information and specific steps required to be followed by each team member to ensure successful recovery. Contractor has a Crisis Manager and leadership identified with responsibilities clearly assigned. Alternates for each critical team member are identified to be involved in the event that the team member is not available. The Disaster Recovery Plan is tested and updated at least annually or when major changes warrant updating. A report of each Disaster Recovery test is completed and any identified gaps and lessons learned are shared with leadership. Any major gaps are prioritized and mitigated where ever possible.

Contractor also includes Business Continuity Plans (BCP) as part the annual testing efforts. This includes a full BCP tabletop exercise with leadership engagement. A report of the annual BCP test is generated and reviewed with leadership. Any gaps identified are prioritized by leadership and are assigned and mitigated where ever possible before the next BCP test if not before.

18. County Data. The Contractor shall provide the County with all County Data upon termination or at any earlier time in the format reasonably requested by the County at no additional cost to the County. In addition, to the extent the County requests Transition Services, the Contractor will provide such Transition Services as provided below. The return of the County Data will either be provided once Transition Services are completed, or earlier, as requested by the County. The Contractor shall not destroy the County Data until such time as the County has confirmed successful access to the returned County Data.

18.1. "Transition Services" means those Services that are provided by Contractor to County at the time of expiration or termination of the Agreement, Service Order, SOW, or any other

termination of Services, along with any new services that County may require to transfer County Data, and the affected Services to County or to any third party designated and authorized by County.

18.2. "Transition Services Period" means a period of six (6) months, or as otherwise described in the Agreement, Service Order or SOW, for the orderly transition of Services and transfer of any County Data to County or another service provider, beginning upon the expiration of the Agreement, Service Order, SOW, or other termination of Services.

18.3. "Transition Services Plan" is the written methodology and approach, including Deliverables and timelines that Contractor will use to deliver the Transition Services during the Transition Services Period.

18.4. Transition Services. In connection with the expiration or termination of the Agreement, any Service Order, or SOW, for any reason, and notwithstanding any dispute between the Parties, Contractor will provide Transition Services for the Transition Services Period, or as otherwise agreed upon between the Parties as follows: (i) Applicable Requirements and Access. At no additional cost Contractor will provide County and any designated Third Party Service Provider in writing, to the extent applicable, applicable standards, policies, operating procedures, and other Documentation relating to the affected Services; (ii) Development of Transition Services Plan. If requested by County, at Contractor's expense, Contractor will assist County and its designated Third Party Service Provider in developing a Transition Services Plan; (iii) Comparable Fees. Contractor shall provide the Transition Services during the Transition Service Period at fees that are no greater than fees charged County for comparable services prior to termination or if comparable services were not performed for County prior to termination or expiration, then at fees no greater than the fees charged by Contractor to other similarly situated customers or fair market value, whichever amount is less; (iv) Post Transition Services Period. For up to three (3) months after the Transition Services Period, at no cost to County, Contractor will answer all reasonable and pertinent verbal or written questions from County regarding the Services on an "as needed" basis as agreed to by the Parties, and deliver to the County any County owned reports materials and information including without limitation any Confidential Information, CPI, CPM, and County Data that might still be in the possession of Contractor; and (v) Absolute Obligation. Contractor agrees that it has an absolute and unconditional obligation to provide County with Transition Services and Contractor's quality and level of performance during the Transition Service Period will continue to adhere to all requirements of the Agreement.

19. Data Retention. Contractor may continue to keep or maintain any County Data obtained in the course of performance of the Services so long as the Agreement and the relevant Service Order or SOW remains in effect and such use shall not extend beyond the termination of the Agreement or the relevant Service Order or SOW except with respect to providing Transition Services, provided that Contractor will provide a copy of the County Data upon termination or expiration of the Agreement in accordance with Section 15 of the Service and Software Subscription or at any time requested by County.

20. Warranties.

20.1. Contractor warrants that the Services and Deliverables will not contain, and Contractor, its employees or Contractor's Agents will not introduce through data transmission or any other means, any virus, ransomware, malware, spyware, bomb, worm, trap door, back door, Trojan horse, malicious logic, drop dead device, software lock, disabling code or any other contaminant, program routine or disabling device, including without limitation, any key, timer, clock, counter, local shared object/flash cookies or other self-enacting device or limiting routines, codes, commands, or instructions or other feature that may have the effect or that could be used to access, track activity on, alter, delete, damage, deactivate, interfere with, disable or otherwise harm any Service or Deliverable or the County owned, licensed and/or leased computer hardware, software, code, systems, data, compilations of data, or other property.

20.2. Contractor warrants that (a) all Services and Deliverables will strictly comply, function and perform in accordance with the functional requirements and specifications of County or as otherwise identified in any and all specifications, criteria, requirements and documentation specified or referred to in the applicable Service Order(s) and/or SOW(s), (b) the Documentation, if any is to be provided, will be accurate, complete and sufficient in detail to enable the End Users to use all of the functionality of the Services and Deliverables without assistance from Contractor or any third party, (c) no information transferred through or stored in or on the Services or Deliverables, while in the possession or under the control of Contractor, will be subject to any loss of accuracy or integrity or corruption, and (d) all Services or Deliverables will comply, function and perform in accordance with all applicable laws and regulations. In the event that the County discovers that any Services or Deliverables do not conform to and perform in accordance with the specifications and requirements of the County, the County shall promptly notify Contractor in writing of such nonconformance, and Contractor shall, at Contractor's sole cost and expense, promptly re-perform Services to modify such Services or Deliverable to make it conform, time being of the essence. In the event Contractor is unable to qualitatively and functionally re-perform the Services or correct a Deliverable within five (5) business days of County notice of the nonconforming Service or Deliverable, County may seek and obtain a refund for the defective Services or Deliverable. Contractor's failure to properly remedy any failed warranty outlined above shall not preclude County from exercising any other remedies available to it under the Agreement or at law or equity.

20.3. Contractor represents and warrants that all third party materials required to operate and fully utilize the Services or Deliverables will be fully disclosed to the County and are commercially available to the County and unless otherwise identified in a Service Order or SOW, no additional license fee or other costs will be incurred by County for use of the Services. Contractor shall and hereby does assign and pass through to the County all warranties, representations and indemnities granted to Contractor by third parties in and with respect to such third party materials, or any component thereof, and all remedies for breach of such warranties, representations and indemnities.