AASHTOWare Project™ Hosting Services – Service Level Agreement

This Service Level Agreement ("SLA") between the licensing agency ("Agency") and the American Association of State Highway and Transportation Officials ("AASHTO") sets forth the service level terms and conditions under which AASHTO's service provider, Info[MS1] Tech, Inc. ("Service Provider") will provide the Agency with a hosted environment for the AASHTOWare Project™ software (collectively, the "Software"). The Service Provider agrees to provide the Agency with access and related hosting services ("Services") to the Software installed in the hosted environment, as more specifically described below.

Services provided

- **Hosted Environment**
    - Service Provider will provide a hosted environment, consisting of a development/test instance and a production instance that is completely isolated and dedicated to a single agency.
    - During the first year of hosting, the development/test instance is provided to the Agency for eleven (11) months after a one (1) month set-up period. Six (6) months after project start-up, the Service Provider will provide a hosted production instance to the Agency for the last six (6) months of first year.
    - The Service Provider hosts this production environment in Amazon Web Services (AWS) using a Virtual Private Cloud (VPC) computing environment within the continental United States
    - The Service Provider utilizes Amazon's Relational Database Service (Amazon RDS) to provide the database for the AASHTOWare Project applications.
    - The dev/test instance and the production instance will be available 24/7, excluding scheduled maintenance.
    - Service Provider will utilize cloud technologies to operate the installed software.
    - Service Provider provides all server system software.
    - User access to the applications will be available over the Internet only, using Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption.
    - User authentication will be provided with accounts maintained in an Active Directory in the VPC which the Agency manages through a web interface. The Agency may also chose to utilize their agency's Microsoft AD FS and/or Azure AD for user authentication to AASHTOWare Project. User authentication to AASHTOWare Project can be provided via an Agency's supported directory service over a Virtual Private Network (VPN) connection; however, this is not recommended for fault tolerance reasons.
    - The Agency can interface external Agency systems directly with the hosted database through a VPN tunnel setup between the Agency's network and the VPC. However, the existing API that utilizes the standard OData protocol is the preferred method for interfaces as it utilizes https and therefore can be performed over an internet connection as well as incorporates the business and security layers of the application.

- **Data Ownership, Protection, and Sovereignty**
    - Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Service Provider to ensure that there is no inappropriate or unauthorized use of information at any time.
    - Agency shall own all right, title and interest in its data that is related to the services provided.
    - Agency is responsible for ensuring that Agency is either the legal owner of or has the legal permissions to control all data hosted by Service Provider in connection with Service Provider's provision of Services.
    - Service Provider does not make any ownership claim to data hosted by Service Provider, and by using the Services, Agency expressly agrees to indemnify Service Provider against any action arising from facts or circumstances wherein ownership of data hosted by Service Provider under this Agreement is at issue.
    - All data will reside at rest in the United States.
    - All data stored at rest in the underlying storage is encrypted; the automated backups and snapshots are also encrypted at rest.
    - All data in transit between the application servers and databases and between the end users and applications is encrypted.
    - Agency data will be retained for 90 days after termination of this Agreement, unless earlier post-termination deletion is requested by Agency.
    - The Service Provider will not permit its personnel and contractors to access the software or data remotely except as required to provide support services or at the Agency's written request.
    - The Agency shall own all right, title and interest in its data that is related to the services provided. AASHTO retains all right, title, and interest in the application system related to the services provided. The Service Provider shall not access or make use of any Agency account or data except when expressly required to provide services or at the Agency's written request
    - All services shall remain in the United States, unless contractor and Agency otherwise explicitly agreed upon other terms. This includes backup data and disaster recovery locations.
    - Full data extracts are available for download by the Agency at any time in the form of the previous day's nightly database dump.
    - Service Provider will retain Agency data while Agency has an active Agreement. Service Provider will transfer and save the data that is within the Software and send the data to Agency in an industry standard electronic format upon termination of the Agreement.
    - In the event of termination of the contract, the Service Provider shall implement an orderly return of all data in a mutually agreeable format. The Service Provider shall guarantee the subsequent secure disposal of all data upon confirmation by the Agency.
- **Maintenance and Support Services**
    - Service Provider will apply all operating system upgrades, patches and antivirus updates. Service Provider and Agency will establish a scheduled maintenance window.

- Service Provider provides phone support for any issues with the service during the normal AASHTO support hours of 8:30 AM to 5:30 PM Eastern Standard Time Monday through Friday, holidays excluded. The response time for issues received during these hours is fifteen (15) minutes, with an issue resolution time of less than an hour.
- Service Provider provides email support outside of the normal customer support hours listed above with a response time of the next business day and an issue resolution time of less than an hour after the response has been acknowledged.

- **Minimum Security Standards**
  - Systems are probed quarterly by Info Tech personnel using the Nessus scanning tool. These results are then analyzed, and corrective action is taken where needed. A third-party security assessment is also performed annually.
  - Antivirus protection is included on all Windows systems within the environment.
  - All data will be encrypted at rest and in transit.
  - Access to the hosted environment will be strictly limited through protocol, port, and endpoint firewalls.
  - Direct database access is only provided through the VPN tunnel to the Agency's internal network.
  - In an effort to minimize the attack surface area, Service Provider will set up the hosted environment to have the minimum number of resources accessible from the Internet, when possible done via a reverse proxy type resource.
  - All Server instances will be behind a firewall. Additional system hardening is done on the server side in order to reduce the attack surface and lower the potential for compromise.
  - For user accounts maintained in an Active Directory in the VPC, the service provider uses no global or general accounts; all accounts belong to an individual. Password strength is enforced automatically. Passwords have a 90-day lifespan. Should the Agency require stronger passwords and a shorter lifespan, this requirement is incorporated into the design.
  - Security controls and processes are in place for the information and the system as categorized as moderate based on the mappings below.
    - Confidentiality: The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
    - Integrity: The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
    - Availability: The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- **Availability and Performance**
  - Applications and their dependencies are hosted in a fault tolerant, highly available environment.
  - The service is continuously monitored for availability and performance. Metrics are monitored and alerts generated as described below:
    - Availability: Server unavailable

        - CPU utilization: Average CPU utilization above 75% for 2 consecutive periods of 5 minutes
        - Available Memory: Minimum available memory below 0.5GB for 2 consecutive periods of 5 minutes
        - Available Storage:
            - Database Servers: Minimum available storage space below 5GB for 1 consecutive period of 5 minutes
            - Non-Database Servers: Minimum available storage space below 10% of total volume for 1 consecutive period of 5 minutes
    - Servers will be scaled up or down based on the monitored performance metrics listed above.
    - Service Provider shall provide the Agency with a performance and availability dashboard allowing the Agency an on-demand, automated way of accessing availability and performance metrics.
    - The Services will be operational 24x7 and available to the Agency at least 99% of any calendar month (Uptime Warranty), excluding scheduled maintenance.
    - Downtime: "Downtime" shall mean any complete interruption in the availability of access to the Production Instance to Agency that Service Provider cannot or does not restore within sixty (60) minutes that was not a direct result of agency actions. Downtime begins upon Agency notification to Service Provider of the interruption, either by speaking directly with a Service Provider Agency service representative or recording a voice mail message in the Service Provider Agency service voice mail box. Downtime does not include a scheduled maintenance window for upgrades or to address any issues or requirements by Service Provider or the Agency.
- **Backup Mechanisms**
    - Any data hosted by the Service Provider will be backed up following the backup policies listed below.
        - Automated full daily backups will be performed and kept for a minimum of thirty days, unless otherwise defined by the Agency.
        - Point in time recovery (down to the second) to any point in time during the backup retention period is available.
        - Automated database dump backups will be performed daily with a fourteen-day retention period. These are stored in both another region and the most recent backup stored at another cloud provider to minimize data loss under the most extreme failure scenarios of full region and full AWS failures respectively.
        - Server backups will include automated snapshots taken nightly with a fourteen-day retention period with the most recent snapshot stored in another region.
- **Recovery Mechanisms**
    - **Server failure recovery**
        - Without any manual interaction a server that becomes impaired due to an underlying hardware failure or a problem will be automatically recovered. A recovered Server is identical to the original Server, including the instance ID, IP addresses, and all Server metadata. No manual intervention is required.

        - The method for recovering a server not handled automatically as described above is to create a volume from the most recent snapshot and associate the restored volume to the problematic server or a newly launched server.
    - **Data failure recovery**
        - The three scenarios in which the database will need to be recovered are when the instance (server), the availability zone (data center), or the region fails.
        - For Production deployments, only a region failure will necessitate a manual intervention. If a production database instance becomes unavailable, the hot standby instance will automatically take its place. This results in essentially zero data loss.
        - Non-production Instance (server) failure: Perform a point in time recovery and terminate the problematic instance. This results in essentially zero data loss.
        - Non-production availability zone (data center) failure: Perform a point in time recovery and terminate the problematic instance. This results in essentially zero data loss.
        - Region failure: Replacement instances will be launched in another region using the most recent backup stored in that region. This type of failure is highly unlikely and results in a maximum data loss of 24 hours.
        - A data recovery plan is also in place for the extraordinarily unlikely event of a complete AWS failure. The database dump backups that are stored in another cloud provider allow the Service Provider to recover the data so another solution with a maximum data loss of 24 hours.
    - Testing of the server and data recovery methods is performed and logged annually at a minimum.
    - The Recovery Point Objective is the maximum targeted period in which data might be lost due to a major incident.
        - The three scenarios in which the data will need to be recovered are when the instance (server), the availability zone (data center), or the region fails. For Production deployments, only a region failure will necessitate a manual intervention. If a production database instance becomes unavailable, the hot standby instance will automatically take its place. This results in essentially zero data loss for both server or data center failures. The RPO for an entire region failure is 24 hours or less as it depends on the time gap between the nightly database dump that's copied to another region and the incident. This type of failure is highly unlikely and results in a maximum data loss of 24 hours.
        - A data recovery plan is also in place for the extraordinarily unlikely event of a complete AWS failure. The database dump backups that are stored in another cloud provider allow the Service Provider to recover the data so another solution with a maximum data loss of 24 hours.
    - The Recovery Time Objective is the targeted duration of time within which services must be restored after a disaster.
        - The recovery time objective is 1 hour for all failure scenarios except an entire region failure or AWS failure. In the highly unlikely scenario of an entire region failure the RTO is 12 hours. In the extraordinarily unlikely event of a complete AWS failure the RTO is 48 hours.

- **Configuration/Change Management**
    - Any changes to the configuration of the hosted environment as it relates to user accessed applications including agency developed customizations must be requested/approved by the agency EUD. These will be applied to the Test instance first when applicable with the EUD providing written approval to apply to production following thorough agency testing.

- **Audit and Logging**
    - With web-based AASHTOWare Project 4.2 and later the Service Provider will record and retain audit-logging information from the Software. The Software should provide sufficient logging to answer the following questions:
        - What activity was performed?
        - Who performed the activity?
        - Where was the activity performed?
        - When was the activity performed?
        - What was the status, outcome, or result of the activity?
    - Logs shall be kept for a minimum of six months and made available to Agency on-demand.
- **Security Incident Response**
    - Service Provider will immediately report any breach of security, including but not limited to unlawful accesses, theft, or other actions that compromise the security of information technology resources owned or hosted by the service provider.
    - Service Provider will cooperate with the Agency during investigations of suspected computer security incidents by providing all requested information to the Agency.
    - Service Provider will work with the Agency to establish any additional security controls that are deemed necessary and reasonable by the Agency.

Remedies

- In the event that, as a direct result of Service Provider's actions or omissions with respect to its performance of the Services, the Agency experiences Downtime in any calendar month in excess of Downtime permitted by the Uptime Warranty stated above, as the sole and exclusive remedy hereunder and at the Agency's request, the Agency shall receive $500.00 for the first hour of Downtime and $500.00 for each hour thereafter missed, up to limit of $5,000.00 per month. The total shall not exceed more than $5,000.00 per month.

Termination

In the event of termination of the contract, the Service Provider shall implement an orderly return of all data in an industry standard electronic format. The Service Provider shall guarantee the subsequent secure disposal of all data upon confirmation by the Agency.

- Suspension of services: During any period of suspension or contract negotiation or disputes, the Service Provider shall not take any action to intentionally erase any Agency data.

- Termination of any services or agreement in entirety: In the event of termination of any services or agreement in entirety, the Service Provider shall not take any action to intentionally erase any Agency data for a period of 90 days after the effective date of the termination. After such 90-day period, the Service Provider shall have no obligation to maintain or provide any Agency data and shall thereafter, unless legally prohibited, dispose of all Agency data in its systems or otherwise in its possession or under its control as specified below. Within this 90-day timeframe, Service Provider will continue to secure and back up Agency data covered under the contract.
- Post-termination assistance: Agency shall be entitled to any post-termination assistance generally made available with respect to the services unless a unique data retrieval arrangement has been established as part of the Service Level Agreement.
- Secure data disposal: When requested by the Agency, the Service Provider shall destroy all requested data in all forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology approved methods and certificates of destruction shall be provided to the Agency.