NON-PUBLIC DATA OWNED BY THE STATE OF MISSISSIPPI

Per rule 1.4 of the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy, each agency must ensure that new contracts and amendments include the terms and conditions approved by ITS. The terms and conditions provided below are applicable for State of Mississippi data that the agency has categorized as ***non-public*** data.

Data Ownership: The State of Mississippi ("State") shall own all right, title and interest in all data used by, resulting from, and collected using the services provided. The Service Provider shall not access State User accounts, or State Data, except (i) in the course of data center operation related to this solution; (ii) response to service or technical issues; (iii) as required by the express terms of this service; or (iv) at State 's written request.

Data Protection: 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 State information at any time. To this end, the Service Provider shall safeguard the confidentiality, integrity, and availability of State information and comply with the following conditions:

a) All information obtained by the Service Provider under this contract shall become and remain property of the State.

b) At no time shall any data or processes which either belongs to or are intended for the use of State or its officers, agents, or employees be copied, disclosed, or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction that does not include the State .

Data Location: The Service Provider shall not store or transfer State data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State data remotely only as required to provide technical support.

Encryption:

a) The Service Provider shall encrypt all non-public data in transit regardless of the transit mechanism.

b) For engagements where the Service Provider stores non-public data, the data shall be **encrypted at rest**. The key location and other key management details will be discussed and negotiated by both parties. Where encryption of data at rest is not possible, the Service Provider must describe existing security measures that provide a similar level of protection. Additionally, when the Service Provider cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. The policy shall comply with the following requirements:

- The policy shall be issued by an insurance company acceptable to the State and valid for the entire term of the contract, inclusive of any term extension(s).
- The Service Provider and the State shall reach agreement on the level of liability insurance coverage required.

- The policy shall include, but not be limited to, coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, and liability assumed under an insured contract.
- At a minimum, the policy shall include third party coverage for credit monitoring. notification costs to data breach victims; and regulatory penalties and fines.
- The policy shall apply separately to each insured against whom claim is made or suit is brought subject to the Service Provider's limit of liability.
- The policy shall include a provision requiring that the policy cannot be cancelled without thirty (30) days written notice.
- The Service Provider shall be responsible for any deductible or self-insured retention contained in the insurance policy.
- The coverage under the policy shall be primary and not in excess to any other insurance carried by the Service Provider.
- In the event the Service Provider fails to keep in effect at all times the insurance coverage required by this provision, the State may, in addition to any other remedies it may have, terminate the contract upon the occurrence of such event, subject to the provisions of the contract.

Breach Notification and Recovery: Unauthorized access or disclosure of non-public data is considered to be a security breach. The Service Provider will provide immediate notification and all communication shall be coordinated with the State. When the Service Provider or their sub-contractors are liable for the loss, the Service Provider shall bear all costs associated with the investigation, response and recovery from the breach including but not limited to credit monitoring services with a term of at least 3 years, mailing costs, website, and toll free telephone call center services. The State shall not agree to any limitation on liability that relieves a Contractor from its own negligence or to the extent that it creates an obligation on the part of the State to hold a Contractor harmless.

Notification of Legal Requests: The Service Provider shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Service Provider shall not respond to subpoenas, service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

Termination and Suspension of Service: In the event of termination of the contract, the Service Provider shall implement an orderly return of State data in CSV or XML or another mutually agreeable format. The Service Provider shall guarantee the subsequent secure disposal of State data.

a) Suspension of services: During any period of suspension of this Agreement, for whatever reason, the Service Provider shall not take any action to intentionally erase any State data.

b) Termination of any services or agreement in entirety: In the event of termination of any services or of the agreement in its entirety, the Service Provider shall maintain the existing level of security as stipulated in the agreement and shall not take any action to intentionally erase any State 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 State data and shall thereafter, unless legally prohibited, dispose of all State data in its systems or otherwise in its possession or under its control as specified in section 7(d) below. Within this 90 day

timeframe, Service Provider will continue to secure and back up State data covered under the contract.

c) Post-Termination Assistance: The State 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.

d) Secure Data Disposal: When requested by the State, the provider shall destroy all requested data in all of its 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 (NIST) approved methods. Certificates of destruction shall be provided to the State.

Background Checks: The Service Provider shall conduct criminal background checks and not utilize any staff, including sub-contractors, to fulfill the obligations of the contract who has been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for a minimum of one (1) year is an authorized penalty. The Service Provider shall promote and maintain an awareness of the importance of securing the State's information among the Service Provider's employees and agents.

Security Logs and Reports: The Service Provider shall allow the State access to system security logs that affect this engagement, its data, and/or processes. This includes the ability to request a report of the activities that a specific user or administrator accessed over a specified period of time as well as the ability for an agency customer to request reports of activities of a specific user associated with that agency.

- These mechanisms should be defined up front and be available for the entire length of the agreement with the Service Provider.

Contract Audit: The Service Provider shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State’s expense.

Sub-contractor Disclosure: The Service Provider shall identify all of its strategic business partners related to services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Service Provider, who will be involved in any application development and/or operations.

Sub-contractor Compliance: Service Provider must ensure that any agent, including a Service Provider or subcontractor, to whom the Service Provider provides access agrees to the same restrictions and conditions that apply through this Agreement.

Processes and Procedures: The Service Provider shall disclose its non-proprietary security processes and technical limitations to the State so that the State can determine if and how adequate protection and flexibility can be attained between the State and the Service Provider. For example: virus checking and port sniffing — the State and the Service Provider shall understand each other’s roles and responsibilities.

Operational Metrics: The Service Provider and the State shall reach agreement on operational metrics and document said metrics in the Service Level Agreement. At a minimum the SLA shall include:

a) Advance notice and change control for major upgrades and system changes

b) System availability/uptime guarantee/agreed-upon maintenance downtime

c) Recovery Time Objective/Recovery Point Objective

d) Security Vulnerability Scanning