**ADDITIONAL TERMS FOR CLOUD SERVICES ENGAGEMENTS**

Exhibit 1 to Contract #\_\_\_\_\_\_\_\_

The words **“**Contract,” “Contractor,” “Form Contract,” and “State” have the same meanings in these Additional Terms for Cloud Services Engagements (these “Cloud Terms”) as they do in Contract #\_\_\_\_\_\_\_\_.

The purpose of these Cloud Terms is *EITHER* to establish terms for the provision of cloud services to the State if the Contractor has provided no such terms of its own *OR* to supplement, delete, and amend certain terms regarding the provision of cloud services in the Form Contract and any related documents that were provided to the State by the Contractor which have been incorporated into the Contract. For order-of-precedence purposes, these Cloud Terms shall be considered to be a part of the State’s Addendum or Professional Services Agreement rather than an attachment.

*These Cloud Terms call for at least one additional document to be attached to the Contract as an exhibit, a statement of work (the “SOW”).* The SOW should typically include a detailed description of the cloud services work that the Contractor will provide to the State in addition to (1) identifying the parties’ specific obligations to one another related to the Contractor’s provision of cloud services, (2) listing the service level minimums that the Contractor is to meet, (3) describing the manner and methods that the Contractor will use to meet those minimums, (4) defining the credits and any other remedies that are available to the State in the event that the Contractor fails to meet them, and (5) explaining how any such credits or other remedies are to be calculated and issued. *The parties understand and agree, however, that some of the aforementioned information may be provided in a separate service level agreement (an “SLA”). In that case, the SLA should be attached as an exhibit as well.*

1. **Definitions.**
2. “Agency Contacts” means any non-IOT personnel who have been identified as technical or security contacts by the State in the Contract, the SOW, or an SLA.
3. “Confidential Information” means any information that the State has identified as confidential or that, given the nature of the information or the circumstances surrounding its disclosure, reasonably should be considered as confidential. Confidential Information may include social security numbers, federal tax information, criminal justice information services data, protected health information, and other types of personally identifiable information that the State is required by law or contract to keep confidential.
4. “Data” means any data – including the selection, arrangement, and organization of such data – entered, uploaded, processed in an application or services, or otherwise provided to the Contractor by the State in connection with the Contract.
5. “Data Breach” means a situation where the Contractor knows, or should reasonably suspect, that unauthorized access to or acquisition of the Data has occurred.
6. “IOT” means the Indiana Office of Technology – *i.e.*, the state agency that is empowered to develop and maintain policies, procedures, and guidelines for the effective and secure use of information technology for the State, pursuant to IC § 4-13.1-2-2.
7. “ISF” means the “Information Security Framework” – *i.e.*, the document that contains the State’s information security policies and standards. The ISF was, or can be, provided to the Contractor by IOT following the Contractor’s execution of a nondisclosure agreement.
8. “Security Incident” means a situation where the Contractor knows, or should reasonably suspect, that unauthorized access to its environment has occurred which could lead to a Data Breach.
9. “Service” means the cloud services that the Contractor is providing to the State under the Contract.
10. **Data Ownership.** The State retains all rights, title, and interest in the Data.
11. **Service-Related Responsibilities.** 
    1. Of the Contractor.Except as is otherwise provided in the SOW or an SLA, the Contractor is responsible for the following responsibilities with regard to the Service:

(1) *Hardware, Software, and Network Support for the Service*. The Contractor shall acquire and operate all of the hardware, software, and network support that are necessary to provide the Service. The technical and professional activities required for establishing, managing, and maintaining the environments are likewise the responsibilities of the Contractor. The Contractor must allow the State to access and use the Service to perform synthetic transaction performance testing.

(2) *Unplanned Service Interruptions and Outages*. The Contractor shall ensure that the Service is available at all times, except during periods of excusable downtime – *i.e.*, those periods of time that are necessary to complete scheduled network, hardware, or service updates or upgrades. The Contractor shall investigate all unplanned interruptions or outages of the Service and provide detailed incident reports to IOT and any Agency Contacts within ten business days following restoration of service.

(3) *Updates, Upgrades, and Other Changes to the Service*. The Contractor must make network, hardware, and service updates and upgrades available to the State – at no additional cost – when the Contractor makes such updates and upgrades generally available to its own users. No update, upgrade, or other change to the Service may increase the cost of the Service to the State, decrease its functionality, or otherwise adversely affect the State’s use of it. The Contractor must notify IOT and any Agency Contacts of its intent to implement an update, upgrade, or other change to the Service at least two weeks before implementation. IOT and any Agency Contacts must be notified of emergency changes – *i.e.*, changes that are necessary due to an unexpected and pressing operational- or security-related need – within eight business hours or 24 total hours, whichever is less, after their implementation.

(4) *Business Continuity and Disaster Recovery*. The Contractor shall ensure that the Service provides and maintains a backup of the Data that can be recovered in an orderly and timely manner within a predefined period of time that is consistent with recovery time and point objectives in the SOW or an SLA. The backup shall be stored at least once daily in an off-site secure data center that is located within the continental United States. The Contractor shall implement a contingency plan for disaster recovery purposes that is designed to maintain the State’s access to the Service and prevent the loss of the Data. At the request of the State, the Contractor shall perform an annual disaster recovery test and take action to correct any issues that are detected within the timeframe that the parties have agreed to in the SOW or an SLA. The Contractor shall provide a report to IOT and any Agency Contacts that identifies the issues that were addressed and the extent to which time objectives were achieved.

(5) *Annual Resource Utilization Assessment*. The Contractor shall provide an annual resource utilization assessment to IOT and the Agency Contacts that details the composition of the Data. This assessment must include the volume of the Data, the file formats, and license utilization.

(6) *Providing a Secure Means to Import and Export the Data*. The Contractor shall provide a secure means for importing and exporting the Data. The State – with the reasonable assistance of the Contractor – must be able to import or export the Data to or from the Service to or from any other entity, in a timely and orderly fashion, in an industry-standard format that provides for interoperability and portability and is accessible without the Contractor’s application.

In no case shall the Contractor take any action that results in loss of the Data until the Contractor has received notice from the State that the Data has been successfully exported. After receiving such notice, the Contractor shall permanently remove or delete all copies of the Data from its environment in accordance with NIST 800-88 standards within 30 days – unless it is legally prohibited from doing so – and provide a certificate of destruction to IOT and any Agency Contacts. The Contractor shall be reimbursed for all reasonably-incurred costs associated with exporting the Data.

* 1. Of the State. The State is responsible for the following responsibilities with regard to the Service:

(1) *Inputting the Data*. The State shall be responsible for inputting the Data into the Contractor’s system and for keeping it current and accurate, unless otherwise stated in the SOW or an SLA.

(2) *Confidential Treatment of the Contractor’s Trade Secrets*. The State shall consider the trade secrets and security-related plans, test results, audit reports, other assessments, and related documents that are provided to it in connection with the Service to be confidential and shall not disclose them to third parties that are not affiliated with the State, consistent with the terms of the Indiana Access to Public Records Act, IC 5-14-3-4(a)(4) and (b)(10), unless required to do so by law.

(3) *State User Compliance*. The State shall use commercially-reasonable efforts to ensure that its users comply with all of the terms and conditions of the Contract.

(4) *No Reverse Engineering*. The State shall not reverse engineer, decompile, disassemble, or otherwise attempt to derive source code or other trade secrets from any of the software or applications that the Contractor provides to the State in association with the Service.

1. **Data Privacy and Security.** The Contractor understands that it is responsible for ensuring the confidentiality and integrity of the Data. To this end, the Contractor agrees to the following, except as is otherwise provided in the SOW or an SLA:
   1. Encryption. The Contractor shall ensure that industry-standard encryption techniques are used to protect the Data to a degree that meets or exceeds the standards which are required by the ISF – including IOT’s data encryption standard, IOT-CS-SEC-003 – with the State maintaining exclusive control of all encryption keying material.
   2. Location. The Data shall be stored, processed, and maintained on secure servers in locked data cabinets in secure facilities that are located within the continental United States. The Data shall not be stored on portable devices – including smartphones, tablets, laptops, and desktop computers. Support for the Service shall be provided from locations within the continental United States by citizens of the United States.
   3. No Use for Nonstate Purposes. The Data may not be copied, disclosed, retained, produced, or sold by the Contractor, without the State’s prior written consent, for use in transactions that do not involve the State. The Contractor must not use any information collected in connection with the Service for any purpose other than fulfilling its obligations under the Contract. If the Contractor receives a legal or investigative demand calling for production of the Data, the Contractor shall provide prompt written notice to the state contacts who are identified in the Contract and cooperate with the State’s efforts to obtain an appropriate protective order or other reasonable assurance that the Data will be afforded confidential treatment.
   4. Limited Access and Use. Access to the Data shall be restricted to those employees and agents of the Contractor who have a need for access in connection with the operation or support of the Service. These individuals shall not access the Data, except (1) as is necessary to provide the Service, (2) in response to service-related or technical issues, or (3) at the State’s written request. The Contractor shall maintain multi-factor identification and other appropriate identification-and-access controls that limit access to the Data, in accordance with the principles of least privilege and least function. The Data shall not be accessed remotely by the employees and agents of the Contractor, except to provide technical support to the State.

Before providing the Service to the State, the Contractor shall provide a list to IOT and any Agency Contacts that identifies those of its employees and agents who will have access to the Data, or the ability to service the systems that maintain the Data, by name and IP address. After it has begun to provide the Service, the Contractor shall update the list every 90 days. In addition to identifying employees and agents, the updated lists shall include access histories and security logs for the Data.

* 1. Nondisclosure Agreements, Background Checks, and Security Awareness Training. The Contractor shall not permit its employees and agents to have access to the Data before they have (1) signed commercially-reasonable nondisclosure agreements, (2) undergone the same level of background checks that the State requires of its own employees and agents who have access to the Data, and (3) received industry-standard annual security awareness training as well as any other training that the State requires of its own employees and agents who have access to the Data.
  2. Subcontractors and Other Agents. The Contractor agrees that it is responsible for the acts and omissions of any subcontractors and other agents that may be involved in the provision of the Service – including business partners or other entities or individuals that may be a party to a joint venture or similar agreement with the Contractor or that may be involved in any application development or operations.
  3. Vulnerability Scans and Malware Protection. The Contractor shall ensure that the systems, middleware, applications, and interfaces on which the Service operates are scanned for vulnerabilities at regular intervals as required by the ISF – including IOT’s configuration management standard and its system and information integrity standard, IOT-CS-SEC-140 and IOT-CS-SEC-148 – and that all necessary security updates are applied as soon as possible and no later than is warranted by industry-standard best practices. The Contractor shall conduct monthly vulnerability scans of any public-facing interfaces with access to the Data. The Contractor shall utilize industry-standard malware protection, incorporating both signature- and nonsignature-based detection mechanisms, on all systems with access to the Data.
  4. Firewalls. The Service must utilize industry-standard firewalls regulating all data entering the internal data network from any external source that will enforce secure connections between internal and external systems and will only permit authorized data to pass through, and the Contractor shall ensure that external connections incorporated into the Service have appropriate security controls – including industry-standard intrusion detection and countermeasures that will detect and terminate any unauthorized activity prior to entering the firewall maintained by the Contractor.
  5. System Security Plans. The Contractor must provide sufficient information to IOT and any Agency Contacts on an annual basis – in the form of its nonproprietary system security plans, security processes, and technical limitations – for the parties to determine what their individual roles and responsibilities are with regard to safeguarding the Data and keeping it confidential.
  6. Incident Response Plan. The Contractor shall have an incident response plan that establishes how the Contractor will address Security Incidents and Data Breaches – including preparation, detection and analysis, containment, eradication, and recovery processes. The Contractor shall fully cooperate with the State’s security resources and law enforcement personnel in the handling of Security Incidents and Data Breaches.
  7. Other Security Standards. The Contractor shall maintain all other industry-standard administrative, technical, and organizational security measures that are necessary to safeguard against unauthorized access to or acquisition of the Data. These measures must be compatible with the standards required by the ISF – including IOT’s cloud product and service agreements standard, IOT-CS-SEC-010.

1. **Audits.**
2. Contract Audit. Upon (30) thirty days notice the State shall be permitted to conduct audits to confirm that the Contractor is adhering to the terms of the Contract – including these Cloud Terms, the SOW, and an SLA – at the State’s discretion and expense. The audits may be conducted by the State or by a third party. Such audits are limited to once in a twelve month period.

.

1. **Special Security Incident and Data Breach Considerations.**
   1. Need to Report Security Incidents and Data Breaches without Unreasonable Delay. The Contractor shall report all Security Incidents and Data Breaches to IOT and any Agency Contacts, without unreasonable delay, no matter what type of information is contained within the Data. The Contractor acknowledges that the State’s need to learn of Security Incidents and Data Breaches will be more urgent, however, if the Data contains Confidential Information. The Contractor understands that, in such cases, the State may be required by law (including IC 4-1-10, IC 4-1-11, and 10 IAC 5-4-1), or by contract, to provide notice to various third parties within prescribed time frames – two days or less in some cases.

So that the State can comply with any such contractual or legal obligations, if the Data contains Confidential Information, the Contractor agrees to report Security Incidents and Data Breaches to IOT and any Agency Contacts, without unreasonable delay, as if the Contractor were itself bound by the same contractual or legal obligations. Notice requirements may be further defined and clarified in the SOW or an SLA.

* 1. Need for Additional Action following Data Breaches. Following a Data Breach, the Contractor shall (1) investigate the Data Breach and identify the threat that caused it and level of exposure, (2) contain and remediate the threat in order to prevent further immediate harm to the State, (3) implement measures that are designed to prevent the same or a similar threat from affecting the Data again in the future, and (4) document the additional action steps taken – as outlined here – and provide a summary of the same to IOT and any Agency Contacts.

If the Data Breach is the result of the Contractor’s or its agents’ failure to adhere to its data privacy and security obligations under Section 4, above, the Contractor shall cover the costs that the State incurs associated with providing notice of the Data Breach to affected individuals, regulators, and others; with providing credit-monitoring services for affected individuals; and with providing a website, a toll-free telephone number, and a call center for affected individuals to contact.

1. **Warranties.** 
   * + 1. The Service. With respect to the Service, the Contractor shall pass through all standard warranties and guarantees which warrants as follows:
2. If the Service was offered to the State by the Contractor as a result of a special procurement request or a request for proposal, the Service shall be fit for the particular purposes specified in the request. The Contractor possesses superior knowledge, with respect to the Service, and is aware that the State is relying on its skill and judgment in providing the Service.
3. The Service shall be performed in a professional and workmanlike manner and shall not infringe any third-party proprietary rights – including any trademark, trade name, trade secret, copyright, moral rights, patents, or similar intellectual property rights.
4. The Service shall conform in all material respects to the requirements set forth in the Contract. All updates, changes, alterations or modifications to the Service shall be compatible with, and shall not materially diminish, the features or functionality of the Service.
5. Any documentation that the Contractor is required to provide under this Contract shall be sufficient in detail and content to allow a user to understand and fully utilize the Service without reference to any other materials or information.
   1. Privacy and Security. With respect to privacy and security, the Contractor warrants that the Service and any related deliverables do not include any degradation, known security vulnerabilities, or breaches of privacy or security.
   2. Supportability. With respect to supportability, the Contractor warrants that the Service and any deliverables do not have dependencies on operating systems or software that are no longer supported by the Contractor, or its subcontractors, partners or third-party providers.
   3. Access. With respect to access, the Contractor warrants that the State shall receive commercially-reasonable uninterrupted access to the Service.
6. **Liability.**
7. Limitation. The Contractor’s per-event liability under the Contract shall not exceed the total amount of fees actually paid or payable by the State to the Contractor for the Service, under this Contract for the year previous to the incident which gave cause for such liability, with the understanding that multiple losses stemming from the same root cause shall constitute a single event. FOR ALL OTHER CONTRACTUAL CLAIMS, IN NO EVENT SHALL EITHER PARTY BE liable for any indirect, incidental, consequential, or punitive damages – including loss of profit, income, or savings – even if advised of the possibility thereof, except when such damages are caused by the gross negligence or willful misconduct of the party, its employees, agents, or subcontractors.
8. Exclusion. The limitation described above does not apply with respect to (1) any intentional or willful misconduct or negligence of any employee, agent, or subcontractor of the Contractor; (2) any act or omission of any employee, agent, or subcontractor of the Contractor; (3) claims for bodily injury, death, or real and tangible property damage; (4) the Contractor’s indemnification obligations; (5) the Contractor’s data privacy obligations; (6) the Contractor’s data security obligations; and (7) the Contractor’s data availability obligations. The Contractor acknowledges and agrees that it is fully responsible for all acts and omissions of its employees, agents, and subcontractors – including their gross negligence or willful misconduct.
9. **Notice and Other Required Communications with IOT.** The Contractor shall use the following email addresses when it is required to provide notice or otherwise communicate with IOT under these Cloud Terms:
   1. Section 3. Notice and other communications that are required under Section 3 of these Cloud Terms shall be sent to [*notifyoperations@iot.in.gov*](mailto:notifyoperations@iot.in.gov).
   2. Sections 4, 5, and 6. Notice and other communications that are required under Section 4, 5, and 6 of these Cloud Terms shall be sent to [*notifysecurity@iot.in.gov*](mailto:notifysecurity@iot.in.gov).
10. **Alterations, Modifications, Changes, Deletions.** The provisions of these Cloud Terms have not been altered, modified, changed, or deleted in any way, except in the following paragraphs: \_\_\_\_\_\_\_\_.