**Attachment N**

**Infrastructure Overview**

The State strongly prefers a cloud-based service offering within a state-owned cloud tenant. However alternative solutions may be considered if they demonstrate significant value. This section provides details on infrastructure and support requirements, outlining the State’s minimum requirements.

**Solution Categories**

The vendor must propose one of the following hosting solutions:

1. **State-Owned Cloud Tenant (Preferred Cloud Solution)**

**Definition:** A vendor hosted solution deployed within a cloud environment owned and managed by the State. This environment is provisioned in either Microsoft Azure or Amazon Web Services (AWS) under the State’s enterprise agreements. The Indiana Office of Technology will set up a cloud tenant that the vendor will use to support all aspects of the solution with oversight and minimal support from the Indiana Office of Technology.

**Minimum Requirements**

* **Tenant Ownership and Access:**
* The State retains full ownership and administrative control over the tenant.
* The vendor shall be granted access only to the resources necessary for the deployment, configuration, and maintenance of the solution, as explicitly authorized by the State.
* The State owns the financial consumption charges within the State-Owned cloud tenant.
* **Data Residency and Compliance:**
* All data associated with the solution must reside within the State-owned tenant.
* The vendor must ensure compliance with all applicable State and federal regulations, including but not limited to data security, privacy, and sovereignty requirements.
* **Deployment and Management:**
* The vendor is expected to install, update, and manage the application and other unique aspects of the solution during the project to meet the requirements and as part of Day 2 support / Maintenance and Operations.
* <https://www.in.gov/iot/iot-vendor-engagement/ht>The vendor must utilize state approved tenant specific native tools and services for monitoring, backup, and disaster recovery, as specified by the State.
* **Security and Access Controls:**
* The vendor shall implement robust security measures, including role-based access control, encryption, and multi-factor authentication, in alignment with [Information Security Framework](https://www.in.gov/iot/iot-vendor-engagement/) (<https://www.in.gov/iot/iot-vendor-engagement/>).
* Security documentation and audit logs must be provided to the State regularly.
* Security assessments, including vulnerability scans, must be conducted and reported to the State.
* **Exit Strategy:**
* Upon contract expiration or termination, the vendor shall ensure a seamless transition of all resources, configurations, and data back to the State, without disruption to ongoing operations.
* A detailed exit plan must be submitted within 120 days of contract expiration or termination, including but not limited to timelines and responsibilities, to facilitate this transition.

1. **Vendor Hosted Cloud Tenant (Exception Based Cloud Solution)**

**Definition**: A vendor managed cloud environment outside of the State’s enterprise agreements.

**Justification and Minimum Requirements**:

Exceptions to the requirement of utilizing a state-owned cloud tenant will only be considered if there are compelling reasons and justifications as to why hosting in a State-owned cloud tenant is not feasible. The State will evaluate these justifications but is not obligated to agree with any external cloud hosting options and the associated scoring will reflect that.

If proposing a hosted solution that does not use a State-owned cloud tenant, your company is required to, at a minimum:

* Provide a clear justification for why hosting within a state-owned cloud tenant is not feasible.
* Demonstrate independently verified compliance with NIST 800-53, Revision 5 (or the most current version at the time of proposed solution go-live).
* Alternatively, provide a detailed plan that includes independent verification of your company's path toward achieving compliance with NIST 800-53, Revision 5 (or the current version at the time of proposed solution go-live).
* Must adhere to the applicable security standards, policies and requirements as outlined by the IOT Cloud Provider Questionnaire, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) Terms outlined within this procurement.

1. **On-Premises Solutions - Vendor Provided Hardware (Preferred On-Premises Solution)**

**Definition:** A vendor provided hardware solution deployed within the States data center.

**Minimum Requirements**

* The vendor is responsible for procuring, deploying, and maintaining hardware hosted within the State of Indiana datacenters.
* Ensuring that all hardware aligns with the State’s standards and specifications, as outlined the State’s established policies and enterprise standards that collectively constitute the [Information Security Framework](https://www.in.gov/iot/iot-vendor-engagement/) (<https://www.in.gov/iot/iot-vendor-engagement/>).
* Meeting the service levels, security protocols, and cost expectations detailed in the "Hosting" section of the [IOT-Services-Catalog.pdf](https://www.in.gov/iot/files/IOT-Services-Catalog.pdf).
* Providing full documentation of hardware lifecycle management, including installation, updates, maintenance, and upgrades as needed.
* Ensuring compatibility with existing state systems and providing any necessary adjustments for seamless integration.
* Delivering comprehensive reporting on hardware usage, performance metrics, and any troubleshooting activities during the contract period.

1. **On-Premises Solutions – State Owned Hardware (Exception Based On-Premises Solution)**

**Definition**: A vendor managed solution operating on state owned infrastructure.

**Minimum Requirements**:

* Collaborating with the State to ensure a seamless initial setup, including installation, configuration, and integration with the State’s systems.
* Adhering to the service levels, security requirements, and cost structures outlined in the "Hosting" section of the [IOT-Services-Catalog.pdf](https://www.in.gov/iot/files/IOT-Services-Catalog.pdf) and as outlined within the [Information Security Framework](https://www.in.gov/iot/iot-vendor-engagement/) (<https://www.in.gov/iot/iot-vendor-engagement/>).
* Provide ongoing monitoring, performance optimization, data backup, and disaster recovery services to ensure system reliability and availability.
* Coordinating with the State on any necessary warranty claims or hardware replacements, including detailed reporting and documentation of hardware issues and resolutions.
* Transferring knowledge, if applicable, to the State to facilitate collaboration and long-term operational continuity.