SERVICE AGREEMENT

between

The Maryland Department of Information Technology and

The Customer

for

Data Management - PaaS
Accounts & Onboarding (Tyler Technologies Data & Insights)

This Service Agreement forms a part of the Memorandum of Understanding between the Maryland Department of Information Technology ("DoIT") and the Serviced Customer. The parties agree as follows:

I.   Service Description

This service delivers named user accounts to two platforms in one, a self-service platform for hosting and distributing datasets to the public through the State's Open Data Portal (ODP) and the State's Internal Data Portal (IDP), a FedRAMP Moderate accredited platform for inter- and intra- agency data collaboration, analysis and problem solving. Accounts come with access to online training provided from Tyler Technologies.

Account holders gain access to features and tools on the State's centrally managed, cloud-based, online data platform that promotes integration with third-party data sources, quickly deploys story pages to convey initiatives to executives, customers and the public and much more. Account holders are supported through the onboarding process by in-house staff and provided with access to online training courses to maximize the value of the account.

A. Standard Service:

The following components are included with the standard service:

1. Named user account for access to the centrally managed cloud-based data platform
2. Access to all the features, as indicated, in the table below:

Feature	Viewer	Editor
Create, upload and manage datasets		X
Create and publish derived views	X	X
Share private data assets with named users	X	X
Create story pages		X
Upload data from csv, xlsx, or other common formats		X
Manage and configure alerts and notifications		X
Publish data to the open data portal		X
Access data sources using natively supported OData		X
Public APIs for datasets, metadata and discovery	X	X

3. Deprovisioning of the account upon conclusion of the documented term
4. Secure authentication using Okta from within the MDGOV domain
5. Documentation and limited support for named user onboarding and startup
6. Access to self-paced online training from the vendor's learning platform
7. In-house technical support for standard platform usage and data connections
8. Limited vendor technical support for advanced platform expertise
9. Support for data connections to standard source systems
10. Proactive platform monitoring for security compliance and performance
11. Proactive operations and maintenance of the managed platform.
12. Product renewals with the vendor

B. <u>Service Exclusions:</u>

The following elements are excluded from the standard service offering:
1. Shared/Headless accounts;
2. Technical support for customer-developed online content (see Data Management - Accounts & Training Support);
3. Technical support for non-standard platform usage and data connections;
4. Data creation, preparation, remediation or maintenance;
5. Data analysis services;
6. Configuration of custom user roles;
7. Ad hoc and customized training;
8. Ad hoc usage statistics;
9. Recovery/Restoration of deleted items for online software;

10. Any Tyler Technologies products or platforms not listed above;
11. Non-english translations or components;

C. Optional Services

Auxiliary services may be available upon request from the Customer for an additional cost. These costs are not included in the budgeted services that DoIT provides and shall be the responsibility of the requesting agency. For any work requested in this area, DoIT will not be able to proceed until fully funded by the requester through a funds certification document.

The following services are add-ons that may be requested. Costs for these items are variable and will be clearly defined and agreed to before moving forward with the request.

1. Custom Extract, Transform, and Load (ETL) operations;
2. Support for non-standard data connections, and gateways;
3. Integration with Tyler Technologies Engagement Builder;
4. Custom content development and maintenance;
5. Ad hoc and custom training;

II.   Service Dependencies

To ensure the service described herein is delivered consistently and in accordance with state standards, the customer must meet the following requirements:

DoIT Services:	● Active subscription to Multi-Factor Authentication service (login.md.gov - Okta) for maryland.gov users.
Technical:	● Active State of Maryland government issued email address. ● Customer network has stable and reliable connections. ● Utilize a vendor-supported web browser (Chrome, Firefox, Edge or Safari)
Non-Technical:	● Understanding of data and metadata best practices. ● Complete an account request form with supervisor approval for named user account creation. ● Active employment or contract with the named supervisor's agency. ● Provide 24 x 7 x 365 points of contact (3) for coordinating outages, emergency maintenance/restoration (with appropriate application access to provide technical assistance), and change management

III. Responsibility Model

The following contains a non-exhaustive list that describes the responsibilities for both DoIT and the customer and may be updated periodically. Updates will be considered effective 14 calendar days from the posting date of the new service agreement.

A. <u>DoIT Responsibilities for the Customer</u>
DoIT shall be responsible for the following activities in coordination with the Customer receiving DoIT enterprise managed services:

1. Account creation and deletion;
2. Platform administration and monitoring;
3. Password resets;
4. Platform governance;
5. Outage notifications;
6. Manage and monitor teams;
7. View activity log of site events;
8. Moderate community-submitted content suggestions;

B. <u>Customer Responsibilities</u>
The Customer shall be responsible for the following activities:

1. Prior to account creation, DoIT must receive confirmation from a supervisor of the requestor, who <u>must be</u> a State employee.
2. Follow the vendor user license agreement;
3. Submit a request to DoIT to offboard an account;
4. Users <u>must not</u> connect to any data source hosting data categorized as Personal Information (PI), confidential, sensitive, restricted access or similar within the platform;
5. Meet the minimum hardware specifications for use of online platform;

IV. Service Level Agreements (SLA's)

A. <u>Availability</u>
Service availability includes the duration of time the service is operational during a calendar month and the level at which the service functions. The table below further outlines DoIT's service targets. Status of the platform are reported by the vendor at status.socrata.com.

Category	Measure
Availability	99.9% uptime
Capacity	2 TBs

B. <u>Maintenance</u>

The State is subject to maintenance terms from the vendor as follows: The vendor will report scheduled maintenance windows, outages or other events affecting customers on the support site at https://support.socrata.com.

1. Scheduled Maintenance
Regular maintenance must be performed to maintain availability and reliability standards and includes replacing hardware, upgrading software, applying patches, and implementing bug fixes.
    a) Scheduled maintenance is automatic as this is an online service.

2. Unplanned Maintenance
    a) Unplanned maintenance is automatic as this is an online service.

C. Service Delivery
DoIT will deliver the requested services to the customer in a timely manner according to the following standards.

Category	Measure
Initial Ticket Response and Customer Contact	2 Business Days

V. Support and Service Management

A. Support
DoIT will provide support via telephone, email, or chat according to the SLA's outlined above.

1. DoIT Service Desk twenty-four (24) hours a day, seven (7) days a week.
2. DoIT Data Services Team during regular business hours (8 AM - 5 PM EST) Monday thru Friday, excluding weekends, state holidays and closings.
3. DoIT will serve as the primary support provider of the service outlined herein.

B. Incident Management
Incidents reported to the DoIT Service Desk will be triaged and managed based on priority as follows*:

This service is for a SaaS platform. All incidents are the responsibility of the vendor as agreed in the State's Enterprise License Agreement. DoIT will consult with the vendor conveying the details of the incident and monitor progress to resolution by the vendor.

Incident Owner: DoIT

Priority (P)	Description	Response Time	Resolution
P1	An incident that results in a total cessation of service across the platform	2 Hours	See Vendor SLAs
P2	An incident that results in a partial cessation or disruption of service, administrative access issues, or loss of other essential business functions.	4 Hours	See Vendor SLAs
P3	Disruption of service for non-essential functionality	2 Business Days	See Vendor SLAs
P3	Service questions and administrative requests such as account creation, deletion, and role changes	2 Business Days	5 Business Days
P4	Troubleshooting, account transfers, and account administration above and beyond account creation, deletion and role changes.	2 Business Days	10 Business Days
*Note: At times, it may be necessary to contact a vendor for assistance, thereby lengthening response times.			

Incident Owner: Vendor			
Priority (P)	Description	Response Time	Resolution
P1	An incident that results in a total cessation of service across the platform	2 Hours	N/A
P2	An incident that results in a partial cessation or disruption of service, administrative access issues, or loss of other essential business functions.	4 Hours	N/A
P3	Disruption of service for non-essential functionality	2 Business Days	N/A

C. Request Management
  Requests to move, add, or change service shall be handled as follows:

  1. New Service(s)
  Customers seeking to utilize the service or deploy optional services outlined herein must:

       a) Submit a request via email to doit.intake@maryland.gov explaining the business needs or challenges.
- DoIT will evaluate the request to ensure that the service meets the entity's business needs.

       b) Once the service is acquired for the agency, individuals will request accounts for the Internal Portal (data.maryland.gov) and Open Data Portal (opendata.maryland.gov) using the signup form.

2. Service Modifications

To increase, decrease, or alter existing service, the Customers must:

       a) Submit a request via email to doit.intake@maryland.gov
- Service modifications include increasing or decreasing the quantity of units or changing the user role of the account.
- DoIT will log the request and assign it to the appropriate team for fulfillment.
- Requests that involve increases to costs will result in billing changes to the agencies which will require a Statement of Work and fund certification to make the change.

D. Outages

DoIT will communicate via X, formerly known as Twitter, @datamaryland of any outages or service degradation resulting from maintenance, fault isolation, or other disruptions. Status of the platform is found at https://support.socrata.com.

E. Support and Service Management Exclusions:

While DoIT strives to tailor support and maintenance activities to match the customer's mission, there may be limitations that hinder our ability to satisfy changing business needs. As such, support and service management activities do not include:

1. Shared/Headless accounts;
2. Technical support for customer-developed online content;
3. Technical support for non-standard platform usage and data connections;
4. Data creation, preparation, remediation or maintenance;
5. Data analysis services;
6. Configuration of custom user roles;
7. Ad hoc and onsite training;
8. Ad hoc usage statistics;
9. Recovery/Restoration of deleted items for online software;
10. Any Tyler Technologies products or platforms not listed above;
11. Non-english translations or components;
12. Development or management of customer applications;
13. Repairs or services for the customer's third-party technologies;
14. Spearheading customer initiatives;

15. Project management;

VI.   Costs for Service

DoIT provides this service via a shared service model, which allows the state to recognize reduced pricing based on economies of scale.

A. The Customer charges budgeted for the current fiscal year are outlined in the DoIT Shared Services Annual Invoice.
1. The unit of measure for which charges are derived for this service is per named user account.
2. Reference the current fiscal year Rate Sheet for additional information

B. All services delivered by DoIT under this agreement are done so on a 100% reimbursable model and therefore costs will be evaluated and adjusted annually to account for fluctuations in the number of shared services used and the underlying costs to deliver that service.

VII.   Termination of Service

This service will automatically be renewed unless the customer and DoIT mutually agree in writing to adjust or discontinue.

A. The customer must provide ninety (90) days advance written notice to terminate services. Due to the nature of the state financial system budgeting for IT services, terminations will only be effective at the end of the fiscal year following the conclusion of the ninety (90) day notice period.

VIII.   Warranty, Limitations, and Exclusions

A. Warranty
1. Account Management: Ensure accounts are set up, managed and deprecated based on the terms stated in this Service Agreement.
2. Platform Management: Proactively monitor the platform and notify customers of outages within a reasonable time frame and work directly with the vendor to troubleshoot issues, when applicable.
3. Named User Account Delivery: Provide the requested platform account within a reasonable timeframe and deliver onboarding guides and access to online training resources.
4. Technical Support: Assist with standard troubleshooting issues related to user account access, account management, or DoIT-managed aspects of the service.

B. Limitations

1. Since Non-enterprise Agencies are not using Okta, the Agency is responsible for managing user account access. The Agency must be aware that the account will be managed with a user account that consists solely of an email address (the user) and a user specified password. DoIT bears no responsibility for destruction of data caused by leaving accounts active after the account owners have left service. We recommend informing DoIT Data Services immediately with a request for account termination and transfer of data to an appropriate owner within your Agency.
2. Vendor licensing terms: DoIT serves as the primary customer to the vendor. All account users are subject to the terms and conditions in the vendor's customer agreement.
3. DoIT is not responsible for:
    a) Feature Availability: The vendor reserves the right to modify or discontinue, deprecate or otherwise, any platform feature without notice.
    b) Data Security and Privacy: The Customer is responsible for complying with all State and DoIT-specific data security and privacy policies while operating within the platform. The current platform is not regulated to protect data classified as confidential or restricted. The Customer is to self-monitor data loaded by the Customer's named account holders and take immediate and appropriate action to remove and discontinue the use of such data on the platform.
4. DoIT will discontinue any account that is found to be operating outside of the vendor's user license agreement or any statements in this agreement. DoIT will notify the named account holder and the identified manager of the action within a reasonable timeframe.
5. DoIT will remove any data classified as confidential or restricted if the named account holder has not removed the identified data within 30 days of notification. DoIT will notify the named account holder and the identified manager of the action within a reasonable timeframe.

C. Exclusions
    1. The Customer is solely responsible for ensuring the data in the Customer's named user accounts is complete, accurate, up-to-date, and complies with relevant government regulations and policies.
    2. DoIT is not responsible for customizations or modifications made to individual account environments beyond what is included in the service agreement.

3. DoIT is not liable for content loss due to unforeseen circumstances, platform errors, user error or misuse beyond reasonable control.