Oversight Systems
Master Agreement

This Master Agreement (the "**Agreement**") is effective on the Effective Date indicated below between Oversight Systems, Inc., a Delaware corporation ("**Oversigh**t") and the client identified below ("**Client**").

Contact Information:

Client: **_____** **_____** **Attention: _____** **Telephone: _____** **Email: _____**	**Oversight:** **Oversight Systems, Inc.** **360 Interstate North Pkwy SE, Suite 300** **Atlanta, GA 30339** **Attention: Finance** **Telephone: (770) 984-4650** **Email: Finance@OversightSystems.com**

This Agreement consists of this cover page, the attached Terms and Conditions, and any Orders executed under this Agreement. This Agreement constitutes the entire agreement between the parties on the subject matter of this Agreement and supersedes all prior or contemporaneous agreements, negotiations, representations and proposals with respect to the subject matter of this Agreement. To the extent the terms, conditions, or definitions set forth in a purchase order or similar document submitted by Client differ or conflict with the terms and conditions of this Agreement, the terms of this Agreement control. This Agreement may not be modified or amended except in writing signed by both parties. By signing below, the parties acknowledge that they have read, understand and agree to be bound by this Agreement, and that the individual signing below is authorized to execute this Agreement on behalf of the party.

Effective Date: _____

<Client Name>	**Oversight Systems, Inc.**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

TERMS AND CONDITIONS

1. DEFINITIONS.

In addition to other terms defined elsewhere, the following terms have the following meanings:

"**Affiliates**" means any entity that a party, directly or indirectly, controls, an entity that controls a party or an entity that is under common control with a party. For purposes of this provision, control means (i) ownership of at least fifty percent (50%) of the outstanding voting shares of the entity or (ii) the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of such entity, whether through the ownership of voting securities, by contract or otherwise.

"**Documentation**" means the supporting documentation and materials embedded in the Service.

"**Order**" means the document executed by the parties under this Agreement by which Client procures Services. Each Order will set forth the applicable Term (as defined on the applicable Order) and the Service Fees (as defined in Section 4 below). Each Order shall constitute a separate and independent contractual obligation between the parties.

"**Services**" means Oversight's Software-as-a-Service provided to Client under this Agreement and as described more specifically on the applicable Order.

2. SERVICES.

2.1. Right to Use the Service. Subject to payment of the applicable Service Fees, Oversight will provide the Services described in the applicable Order and in accordance with the Hosting Guide attached to this Agreement as Exhibit 1. Oversight grants Client, and Client accepts from Oversight, a non-exclusive, non-transferable, right to use the Services during the Term. The Services will be used subject to limitations set forth on the applicable Order. Client is responsible for the use of the Services by any person to whom Client has given access to the Services, and any person who gains access to the Data (as defined in Section 7.2 below) via the acts or omissions of Client.

2.2. Restrictions. Client will only use the Services for its own internal business and may not use the Service as part of providing an application service offering, or any other renting or leasing of Service as part of an offering to unapproved third parties. Client will not, directly or indirectly, without the prior written consent of Oversight: (a) sublicense, transfer, or otherwise assign its rights in the Service or the Documentation to any third-party nor allow any third-party to access or use the Service or the Documentation; (b) modify the software elements of the Service or the Deliverables; (c) create derivative works of the Service or the Documentation or any components thereof; (d) translate, reverse engineer, de-compile, or disassemble the software elements of the Service for any other reason; or (e) copy the software elements of the Service or the Documentation, in whole or in part, except as permitted by this Agreement. The Service may only be used for lawful purposes; transmission of any material which is threatening, obscene, libelous, defamatory, discriminatory, or is otherwise offensive or illegal will constitute a material breach of this Agreement. Client must retain all legends relating to the copyright, trademarks, patents, or confidentiality on all copies of the Documentation or any print of a screen display from the Service.

3. TERM AND TERMINATION.

3.1. Term. This Agreement will commence on the Effective Date and continue in full force and effect until the last to expire of the Order(s). The term of each Order is as specified

in the particular Order. As used in this Agreement, **"Term"** means, collectively, the Initial Term (as defined in the applicable Order) and each Renewal Term (as defined in the applicable Order).

3.2. Termination for Cause. This Agreement or any Order may be terminated by a party if the other party commits any material breach of this Agreement or any Order which is not remedied within thirty (30) days of notice of such breach to the breaching party.

3.3. Termination**.** Either party may terminate the Service effective at the expiration of the then current Term upon ninety (90) days prior written notice.

3.4. Effect of Termination. Upon the earlier of termination of an Order or this Agreement: (a) except as expressly provided in this Section 3, all rights and obligations of the parties hereunder will immediately terminate; (b) each party will return or destroy all copies of the Confidential Information of the other party in its possession or under its control; (c) Oversight shall cease providing the Services; and (d) each party's obligation to pay all amounts due to the other party accrued prior to termination (or, where applicable, after termination) will not be affected. Except as otherwise set forth herein, the Service Fees are non-refundable. Oversight will retain Data for up to sixty (60) days after termination of this Agreement (the **"Data Retention Period"**). During the Data Retention Period, Client may download a copy of the Data at no additional charge. Following the earlier of (i) expiration of the Data Retention Period, (ii) the date upon which Client retrieves Data, or (iii) Client confirms it will not download its Data, Oversight will delete the Data from any systems on which Data is present without further notice to Client.

3.5. Survival. The provisions of this Agreement, which by their nature survive expiration or termination of this Agreement, shall survive.

4. PAYMENT TERMS; TAXES.

4.1. Fees. All Service fees for the scope of Services set forth in the applicable Order (the "**Service Fees**") are billed annually in advance in U.S. Dollars net of any foreign, federal, state, or local taxes, including without limitation, sales taxes, use taxes, VAT, excise taxes, duties, and import taxes (collectively, **"Taxes"**). Client will reimburse Oversight for the pre-approved actual and reasonable travel and living expenses incurred by Oversight in connection with the delivery of any training or other professional services by Oversight to Client as set for a particular Order.

4.2. Payment Terms. Client will pay the Service Fees and expenses (as applicable) within thirty (30) days of the invoice date, without deduction or setoff. If Client believes an invoice or charge is incorrect, Client must contact Oversight in writing within thirty (30) days of the invoice date or charge to be eligible to receive an adjustment or credit. Any undisputed payment not made when due will be subject to late charges of 1.5% per month (prorated on a daily basis beginning on the past due date). Client will be liable for any reasonable attorneys' fees or other costs associated with collecting late payments.

4.3. Taxes. Client is responsible for, and must pay, any and all Taxes (other than Taxes based on Oversight's income) imposed in connection with the Services and any other services provided in connection with this Agreement.

5. SERVICE AVAILABILITY.

5.1. Service Levels. The Service will be available at least 99% of the time during each month excluding Excusable Downtime (the "**Uptime Commitment**"). "**Excusable Downtime**" means time that the Service is not available to Client because of (a) maintenance which is scheduled (i) each week between 12:01 a.m. and 3:00 a.m. Saturday Eastern time, or (ii) during the third week of each month between

6:00 p.m. Saturday and 6:00 a.m. Sunday Eastern time (collectively, the "**Standard Windows**") or planned maintenance which cannot be reasonably scheduled during the Standard Windows for which at least 24 hours advance notice is given, (b) outages caused by misuse of the Service by Client, (c) failure of the Internet, and (d) events contemplated by Section 12.7. If the Uptime Commitment is not met in any month, Oversight will issue Client a credit based on the percentage of Service Fees calculated in accordance with the table below. Such credit will be applied to extend the then current Term or against subsequent invoice(s), as determined by Oversight in its reasonable discretion.

Availability Percentage in any Month	**Percentage Credit**
Less than 99 % but at least 97.0%	5% of the annual Service Fee divided by 12
Less than 97.0% but at least 95.0%	10% of the annual Service Fee divided by 12
Less than 95.0%	15% of the annual Service Fee divided by 12

If in any period of 3 consecutive months the Availability Percentage during such period is less than 95%, Client will have the right, upon written notice to Oversight, to terminate the Order(s) for the affected Services and receive a refund of the Service Fees actually paid for the unexpired portion of the then-current Term for the affected Services.

5.2. Client's Equipment. Client is solely responsible to obtain and maintain its own computer hardware, software and telecommunications connections services as required to access Services.

6. WARRANTIES.

6.1. Service Warranties. Oversight warrants that the Services will be performed in (i) a good, professional and workmanlike manner; (ii) in substantial accordance with the Documentation; and (iii) in accordance with the terms of this Agreement. Client will promptly notify Oversight in writing of any failure of the Services to meet the foregoing warranties. Client will assist Oversight in identifying and reproducing the issue. Oversight will diligently and in good faith attempt to correct the reported defect by repairing or modifying the Service within a commercially reasonable period of time, not to exceed forty-five (45) days. If Oversight is unable to cure that defect by repairing or modifying the Service as provided herein, then Client may elect to terminate its right to use the Service, and Client will be entitled to a refund of the Service Fees actually paid to Oversight for the unexpired portion of the then current Term.

6.2. No Other Warranties. EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, OVERSIGHT, ITS AFFILIATES, THEIR THIRD - PARTY LICENSORS, DISCLAIM ALL OTHER WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR ACCURACY.

7. PROPRIETARY RIGHTS.

7.1. Generally. Oversight retains all right, title and interest in and to the Service, together with all patents, copyrights, trademarks, trade names, trade secrets, technology, ideas, know-how, and other intellectual property and proprietary rights pertaining thereto and all derivative works and improvements to the same.

7.2. Client Data.

7.2.1. Oversight does not own any data, information, or material that is submitted to the Service by Client (**"Data"**). Client will have sole

responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership of, or right to use, Data. Oversight will only use the Data for purposes of providing the Service, providing support for the Services (**"Support"**), and confirming Client's compliance with the terms of this Agreement. In addition, Client grants Oversight a non-exclusive, royalty-free license to Use anonymized Client Data in its business intelligence initiatives. "Anonymized" means data that is not attributable to Client, a data subject or otherwise identifiable as Client Data. "Use" means analysis for purposes of enhancing existing solutions, creating, displaying valuable indicators based on client resolutions to increase efficiencies, new solutions and tools, industry and regional key performance indicators (KPIs), benchmarks, and statistical results such as averages and means, for the distribution to and the benefit of Oversight's clients generally. As a cloud-based data-processor we will leverage anonymized client data to provide greater value to benefit all of our clients going forward.

7.2.2. Client will only submit Data to Oversight using methods set forth in the applicable Order or Exhibit 1 below. Sending Data by a non-approved method such as email is strictly prohibited. Oversight's receipt of Data under this Agreement denotes Oversight's right to process such Data. Reasonable requests to delete or purge Data that was incorrectly or inadvertently sent will be carried out by deleting such data from storage and processing systems.

7.2.3. Oversight will comply with the Data Management and Security principals set forth in Exhibit 2 to this Agreement and the Data Protection Agreement set forth in Exhibit 3 to this Agreement.

7.2.4. The parties acknowledge and agree that the Services are not intended for use in the storage, processing or handling of data that is (i) Payment Card Industry data, (ii) Protected Health Information subject to the Health Insurance Portability and Accountability Act, as amended ("**HIPAA**"), (iii) Sensitive Personal Data (iv) Educational Records, (v) about individuals under the age of 18 or (vi) the following unhashed data elements (a) Social Security number; (b) driver's license number or government issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account. **"PCI data"** means Cardholder Data as defined by the Payment Card Industry Data Security Standard ("PCI DSS") v3.2, Cardholder Name excluded, **"Protected Health Information"** has the meaning set forth in HIPAA, "**Educational Records**" has the mean set forth in the Family Educational Rights and Privacy Act ("**FERPA**") and "**Sensitive Personal Data**" as defined in Article 9 of the GDPR or other applicable data protection legislation.

7.2.5. During the Term, Oversight will perform daily and weekly back-ups of Data. Daily back-ups are stored on site and weekly backups are securely transferred from the primary data center to the disaster recovery **("DR")** site.

8. CONFIDENTIALITY.

8.1. Confidential Information Defined. "**Confidential Information**" means any technical data, pricing, know-how or business information specific to Client or Oversight which is marked as confidential or contains a similar legend or which from all the relevant circumstances would reasonably be assumed to be confidential and proprietary. Confidential Information does not include information which (a) was in the public domain at the time it was disclosed or becomes in the public domain through no fault of the receiver; (b) can be shown by written documentation to have been known to the receiver, without restriction, at the time of disclosure; (c) was independently developed by the receiver without any use of the discloser's Confidential Information; or (d) becomes known to the receiver, without restriction, from a source other than the discloser without breach of any confidentiality agreement and otherwise not in violation of the discloser's rights.

8.2. Nondisclosure of Confidential Information. Each party will treat the Confidential Information of the other party in a confidential manner with the same degree of care as such party treats its own proprietary information of like importance, which will be no less than a reasonable degree of care. This Section 8 will not prohibit disclosure of Confidential Information pursuant to the order or requirement of a court, administrative agency, or other governmental body; provided, the receiver will furnish prompt notice thereof to enable the discloser to seek a protective order or otherwise prevent such disclosure. The obligations of this Section will survive termination for any reason for a period of three (3) years.

8.3. Remedies. The parties agree that each party shall be entitled to seek equitable relief to protect its interests under this Section 8, including preliminary and permanent injunctive relief, as well as money damages. Nothing stated herein shall be construed to limit any other remedies available to the parties for breach of this Section 8.

9. INDEMNIFICATION

9.1. By Oversight. Oversight will defend or, at its option, settle, any third-party claim (a **"Claim"**) brought against Client, its Affiliate or their respective officers, directors, employees or agents relating to (i) any infringement of the intellectual property ("**IP**") rights of any third party by the Services when used as permitted under the terms of this Agreement; (ii) bodily injury or tangible property damage caused by the acts or omissions of Oversight or its employees or agents; (iii) Oversight's failure to comply with the Laws applicable to the Services; or (iv) Oversight's fraud, gross negligence or willful misconduct. In the event of an IP Claim, or if Oversight determines that the Services infringe as set forth above, Oversight will, at its sole option and expense, procure the right to use the Services or replace or modify the Services so as to avoid infringement. If neither of such alternatives is, in Oversight's opinion, commercially reasonable, Oversight's sole liability, in addition to its obligation to reimburse awarded damages and costs as set forth above, is to refund to Client any unearned prepaid amounts for such Services, in which event this Agreement will terminate immediately.

9.2. By Client. Client will defend or, at its option, settle, any Claim brought against Oversight, its Affiliate or their respective officers, directors, employees or agents relating to or arising out of (i) bodily injury or tangible

property damage caused by the acts or omissions of Client or its employees or agents; (iii) Client's failure to comply with the Laws applicable to the Services; or (iv) Client's fraud, gross negligence or willful misconduct.

9.3. Process. The foregoing indemnities are subject to the indemnified party taking all reasonable steps to mitigate any potential expenses and providing the indemnifying party with (i) prompt written notice of any such Claim or possibility thereof; (ii) sole control over the defense or settlement of such Claim; and (iii) all necessary information and assistance to settle or defend any such Claim. The failure of the indemnified party to comply with the foregoing requirements shall not relieve the indemnifying party of its obligations under this Section except to the extent the indemnifying party is prejudiced by such failure.

9.4. Exclusive Remedy. This Section 8 states the entire liability and obligation of Oversight, and the exclusive remedy of Client, with respect to any actual or alleged infringement of any intellectual property right by the Services provided hereunder.

10. LIMITATION OF LIABILITY.

10.1. Limit on Certain Damages. In no event shall Oversight have liability for any special, indirect, incidental, punitive, speculative, expectation, or consequential damages, including damages for lost profits, arising in any way out of this Agreement or any order under any cause of action, whether or not Oversight has been advised of the possibility of such damages. This limitation shall apply notwithstanding the failure of essential purpose of any limited remedy.

10.2. Limit on Total Liability. Except for the indemnifications in Section 9, in no event shall the maximum cumulative liability of Oversight, in connection with the Services and this Agreement or any Order, regardless of the form of action, exceed the fees paid by Client to Oversight during the then-current Term of the applicable Order.

10.3. Limit on Actions. No action, regardless of form, arising from or pertaining to the Services may be brought more than two years after such action has accrued.

11. INSURANCE.

11.1. Coverage Generally. Oversight Systems will, at a minimum, maintain the insurance coverage listed below:

11.1.1. Commercial General Liability Insurance with at least $1,000,000 per occurrence and $2,000,000 in the aggregate.

11.1.2. Full statutory coverage for Workers' Compensation and Employers Liability with limits as required by law.

11.1.3. Cyber Liability / Professional Liability coverage with a limit of at least $5,000,000;

11.1.4. Commercial Umbrella insurance with a limit of $5,000,000 per occurrence and in the aggregate.

11.1.5. Hired and non-owned Auto coverage with a limit of at least $1,000,00 per occurrence.

11.2. Certificates. Upon request, Oversight Systems will furnish Client with a certificate of insurance listing the types and limits of insurance as set forth above.

12. GENERAL.

12.1. Notices. All notices under this Agreement will be in writing and mailed or delivered (including by email) to each party as set forth on the cover page (as it may be modified by the recipient by notice to the other). All such notices will be effective upon delivery, but when emailed, such notices will be effective only upon confirmation of receipt.

12.2. Assignment. This Agreement, including any Order shall not be assigned or transferred by Client, without the prior written consent of

Oversight (which shall not be unreasonably withheld) and any attempt to so assign or transfer this Agreement without such consent shall be null and void. This provision shall not apply in the case of the sale of substantially all of the stock or assets of Client where the obligations under this Agreement are assumed by the successor entity. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of each party's respective successors and permitted assigns.

12.3. Governing Law. This Agreement shall be governed, construed and enforced in accordance with the laws of New York, without reference to conflict of laws principles. Each party hereby waives any right to trial by jury.

12.4. Independent Contractors. The relationship of Oversight and Client established by this Agreement is that of independent contractors.

12.5. Severability. In the event that any provision of this Agreement is found invalid or unenforceable, it will be enforced to the extent permissible and the remainder of this Agreement will remain in full force and effect.

12.6. No Waiver. The failure of either party to enforce at any time any of the provisions of this Agreement shall not be deemed to be a waiver of the right of either party thereafter to enforce any such provisions.

12.7. Force Majeure. Except for the obligation to make payments, neither party shall be liable to the other for its failure to perform any of its obligations hereunder during any period in which such performance is delayed by circumstances beyond its reasonable control including acts of God or of the public enemy, U.S. or foreign governmental acts in either a sovereign or contractual capacity, fire, flood, epidemic, pandemic, restrictions, strikes, and/or freight embargoes.

12.8. Export Restrictions. Client represents and warrants that Client is not (a) located in an embargoed country as designated by the Office of Foreign Asset Control of the Treasury Department (an **"Embargoed Country"**), or (b) listed on the prohibited persons list maintained by the Bureau of Industry and Security of the Department of Commerce (the **"Prohibited Persons List"**).

12.9. Attorneys Fees**.** Should it become necessary to take any action to enforce the terms of this Agreement or any Order, the prevailing party shall be entitled to recover its actual and reasonable attorney's fees and costs.

12.10. Counterparts. This Agreement may be executed in counterparts, each of which will be deemed an original, but all of which together will constitute one and the same agreement.

12.11. Publicity. Client agrees that Oversight may include identification of Client as a client on Oversight's marketing materials, provided that the identification of Client is no more prominent than the identification of Oversight's other clients and is otherwise consistent with Oversight's practice of identifying its clients on Oversight's marketing materials at the time.

EXHIBIT 1

Oversight Hosting Guide

Oversight provides the Service, complete with the required hosting and support services as simply and as consistently as possible. Oversight reserves the right to modify this Hosting Guide from time to time; provided, however, such modifications will not adversely affect the Services. Modifications will be posted to http://www.oversightsystems.com/exhibit-1 and a notice will be given to Client by its Account Manager.

Oversight provides:

- 12 x 5 access to product experts in our Client Support Center via telephone and email
- 24 x 7 Client Support Center access for production-down incidents
- Proactive support incident management
- Product updates, including functionality enhancements
- Defect resolution and problem correction
- On-line support and training resources

Client Support Center

Availability

Clients have two methods of creating, modifying and monitoring a support incident with the Client Support Center (**"CSC"**):

- Phone: Toll-free +1 866 876 5578
  Direct dial +1 770-984-4656
- Email to: support@oversightsystems.com*

**Note: Production Down and critical severity issues must be called into the CSC for Service Level credit purposes.*

CSC standard hours of operation are Monday through Friday (US national holidays excluded), from 8:00 A.M. to 8:00 P.M. Eastern Time (US).

Incident Management

When you have a question or encounter a problem or error, contact the CSC. All contact with the CSC is logged in Oversight's call tracking system. Each issue is assigned a unique Incident Number that enables the CSC to track and communicate the status and progress of the incident. The CSC works to proactively manage the incident.

Incident Severity and Response Targets

Upon communication of the request, the CSC engineer will work with the Client to assign an appropriate severity level, based on how the incident impacts the Client's business operations.

Incident Workaround and Resolution Targets

When an incident is reported, Oversight's objective is to find a satisfactory solution as soon as possible.

The following table outlines the expected initial response targets and workaround/resolution targets for the different levels of severity:

Severity	Description	Initial Response Target	Workaround / Resolution Target
0 - Production Down	Service* is not available. *Does not apply to Development or Test systems	15 Minutes	4 hours
1 - Critical	Severe impact on Client operations that cannot be circumvented, or where the fault prohibits Client from performing a critical business function.	1 hour	1 business day
2 - High	Serious problem where service is partially interrupted or impaired, but can be circumvented.	4 hours	1 week
3 - Medium	Problem has medium impact on business function, and can be circumvented.	8 hours	1 month
4 - Low	Problem has low impact on business function, and can be circumvented.	16 hours	N/A

Note: Production Down and Critical severity issues must be called into the CSC to meet response targets.

Incident Initial Response Target – Oversight will meet the Incident Initial Response Target 95% of the time.

After Hours Support

Outside the 12x5 support period, Clients may contact the CSC at any time. Severity 0 (Production Down) incidents called in during non-business hours will receive an initial response within an hour; other contacts made during non-business hours will be responded to the next business day, based on severity.

Proactive Incident Updates

Clients will receive ongoing progress updates on each outstanding incident. The Oversight CSC expert assigned to the incident will monitor and communicate to the Client the progress of resolution, based on the assigned severity level. Regular proactive communication will continue until a resolution is reached. The following table outlines the timeline for proactive contact:

Severity of Business Issue	Frequency of Update
0 - Production Down	Hourly
1 - Critical	Every 8 business hours*
2 - High	Every 2 business days*
3 - Medium	Every 5 business days*
4 - Low	As required

**If requested by the Client*

Oversight and Client Responsibilities

Oversight Responsibilities

- **Handling of Non-Defect Requests**

  Client suggestions for enhancements or improvements to functionality are appreciated and will be forwarded to the Oversight's Product Management team for consideration in future releases.

- **Notice of Emergency Maintenance**

  Oversight will use reasonable efforts to provide 24 hours prior notice for emergency maintenance to the Service. The notice will specify the expected duration and impact of the outage.

- **Software Support**

  Oversight will determine which version of Oversight software that is used. Oversight will proactively provide software defect resolution and periodic point release updates containing all generally available error corrections.

Client Responsibilities

- **Providing Designated Support Contacts**

  The Client will be asked to designate named contacts that have the ability to add, modify or disable authorized users from the Service.

- **Provide Acceptable Input Data by Approved Methods**

  When Data is provided in a means other than by an established Oversight partner connector, Client is responsible for providing correct, consistent and complete Client input data that can be successfully processed by the Service. Currently approved methods are:

  - Secure File Transfer Protocol **("SFTP"**) directly to Oversight
  - HTTPS directly to Oversight
  - Client authorizing a third-party to SFTP Data directly to Oversight
  - Utilizing an Oversight Partner Connector

- **Problem Description**

  If an issue is reported to the CSC, Oversight requires a clear and definitive description of the problem. This includes describing what was expected to happen, what is actually happening, and why it is considered to be a problem. Information describing the situation in which the problem occurs is also needed.

Oversight Hosting Services

Service Availability and Business Continuity

Oversight uses industry standard technology and solid operational processes and procedures dedicated to provide business continuity and maintain availability of the Service. Oversight will perform daily and weekly back-ups of Data. Daily back-ups are stored on site and weekly backups are securely transferred from the primary data center from which the Service is provided to the DR site.

Maintenance Windows

Oversight performs system and software maintenance during periods when users will not be substantially impacted, typically at night or on weekends. Oversight's planned standard maintenance windows are each week 12:01 a.m. through 3:00 a.m. Saturday Eastern time and during the third week of each month between 6:00 P.M. Saturday and 6:00 A.M. Sunday, Eastern time (US). Planned standard maintenance activity and planned outages are not included in calculation of availability. Oversight reserves the right to do emergency maintenance for events such as correcting significant security vulnerabilities or other catastrophic issues affecting multiple Clients.

Data Availability within the Service

As long as Client is current on a subscription for the applicable Service, (i) exceptions and the data that generated the exception(s) will be available within the Oversight Service for five (5) years from the original transaction date; and (ii) data that did not generate an exception will be available for eighteen (18) months from its original transaction date (collectively, the **"Data Availability Period"**). After expiration of the Data Availability Period, Data will be purged from the Oversight Service.

Oversight Service Level Targets

Oversight's Service will meet the following service level targets. Unless otherwise specified, availability service levels will be measured monthly.

- Services Availability – Will be available to users 99% or more of the time measured monthly excluding planned outages. The Service is considered to be Available when any authorized user can successfully log-in and perform a reasonable portion of the available user actions.
- Incident Initial Response Time – Oversight will meet the Incident Initial Response Time 95% of the time measured monthly.

EXHIBIT 2

OVERSIGHT SYSTEMS' DATA MANAGEMENT AND SECURITY

This Data Management and Security exhibit describes the controls Oversight has implemented and maintains to protect Client Data that Oversight has access to in connection with the provision of the Services. This exhibit may be updated by Oversight from time to time but only in a manner that retains or increases the stringency of Oversight's security obligations; such updates will be posted at http://www.oversightsystems.com/exhibit-2.

1. GENERALLY.

Oversight complies with:

- SSAE-18 / SOC2 Type 2
- Applicable Data Protection Laws

Oversight complies with applicable portions of the following standards:

- PCI/DSS v3 – Self-certified
- ISO 27001/2 and NIST – ISMS and controls based on these standards

Oversight's primary and DR colocation data facilities are:

- SSAE-18 / SOC2 Type 2
- Geographically separated

2. DISASTER RECOVERY.

Oversight has implemented and maintains a comprehensive Disaster Recovery Plan (**"DRP"**). The DRP addresses the policies and procedures in the event of a disaster event which affects the ability of Oversight to provide the Service in accordance with this Agreement. A **"Disaster"** is defined as the loss of the primary production facility for an extended period of time. Non-Disaster events that impact the Service are handled by industry standard practices including backups, snapshots, virtualization, and other appropriate technologies. In the event of a Disaster or other event affecting Client's access to the Service, Oversight will provide Client with an email notice verifying activation of the Oversight DRP procedures as necessary for addressing the impact of a non-Disaster on the Service and the plan for reestablishing Service. Following a Disaster, Oversight will use all reasonable efforts to reinstate access to the Service within five (5) business days.

3. SECURITY MEASURES.

Oversight has implemented physical, technical, and organizational measures and safeguards with respect to Data and the Processing of the same against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosures or access, and against all other unlawful forms of Processing, consistent with this exhibit and with the Data Protection Laws. Oversight will provide Client with information regarding Oversight's security measures upon request. Oversight limits access to Data to those personnel who have a business need to access the Data in the provision of services under the applicable services agreement.

Oversight follows industry standards and this exhibit which include the following minimum controls:

- Personnel. Background checks that cover criminal, financial and work history are completed before a person is allowed to start work. Each employee and contractor is required to sign a Non-Disclosure Agreement and an Acceptable Use policy before starting work.
- Encryption. Transmissions of Data shall use a minimum of industry standard 128-bit encryption.
- Portable Media. Transfers or transmissions of Data on recordable or portable media is prohibited. Portable media includes thumb drives, portable disc drives, CDs or DVDs, or any other portable device used to store and transfer electronic information.
- E-mail Transmission of Data Prohibited. Except when using the functionality specifically provided in the Service, data transferred by or on behalf of any Client or by or on behalf of Oversight will not be sent by e-mail. All such Data must be transferred using a secured file transfer mechanism.
- Encrypted Storage. All Data at rest shall be encrypted using a minimum of industry standard 256-bit.
- Passwords. Privileged user passwords will meet the following complexity and age requirements:
    - Minimum 15 characters including 2 upper, 2 lower, 2 numbers, 2 special characters
    - Expire every 30 days
- Access Control. Oversight implements role-based access control such that the permissions each individual is granted are based on what is required for them to perform the role(s) they are assigned by management. Exceptions require management approval.
- Workstations. Workstations used by Oversight to access Data use the following or similar minimum security controls:
    - Encrypted hard drives; and
    - Regularly updated antivirus and other anti-malicious software and programs and firewalls; and
    - Weekly Operating System patching; and
    - Password and screensaver controls with automatic lock of workstation upon idleness.
- Hosting. Oversight operates a cloud-based Software as a Service platform:
    - The primary production is located at an Atlanta GA data center.
    - The disaster recovery location is located at a US-based data center located in a different geographic area.
    - Only SSAE-18-certified colocation data centers are used for primary and disaster recovery sites.
- Servers. Servers used by Oversight to process Data use the following or similar minimum security controls:

  - Regularly updated antivirus and other anti-malicious software and programs and firewalls; and
  - Monthly patching of Operating System, Database, and Application; and
  - Encrypted management access.
- Backups. Backups are taken regularly to facilitate business continuity and disaster recovery:
  - Daily snapshots are stored locally
  - Weekly backups are securely copied via network to the disaster recovery site
- Network Security. Oversight's network security has the following or equivalent minimum capabilities:
  - Access control lists;
  - All Network traffic passes through firewalls. Oversight has implemented intrusion prevention systems that allow traffic flowing through firewalls to be protected 24x7;
  - Access to network devices for administration require a minimum of 256-bit, industry standard encryption;
  - Network, application, and server authentication passwords meet minimum complexity guidelines;
  - Firewalls are deployed to protect the perimeter Oversight network;
  - Web Application Firewalls (**"WAF"**) are deployed to protect the Oversight Service;
  - Virtual Private Networks (**"VPN"**) are required for the remote access to the Oversight client data environment, which include (i) connections with a minimum of 256-bit encryption; and (ii) split tunneling is disabled; and
  - Regular patches and updates.
- Physical Security. For all Oversight locations where Data is processed, Oversight has the following minimum physical security requirements in place:
  - A clean desk policy requiring that personnel do not leave Data exposed at the end of their workday;
  - Access to the facility or areas where Data is stored or accessible are controlled through key card and/or appropriate sign-in procedures;
  - All Personnel with access to the facility or areas where Data is stored or accessed will be required to have appropriate identification;
  - All Personnel are required to lock PCs with access to Data when not in use;
  - All monitors for such PCs are equipped with a privacy screen as necessary;
  - Oversight employees or contractors appropriately secure all third-party assets in their possession. This includes use of laptop locks (whether in the office, at home, or traveling) and storing secure access tokens in locked location; and
  - Cameras.
- Roles and Responsibilities. Oversight maintains separation of duties in security, compliance, and audit operations:
  - Operational Security – operational security is the responsibility of the IT team.
  - Information Security, Risk and Compliance – information security policy, audit, and compliance are the responsibility of the Information Security team.
  - Privacy – personal data privacy is the responsibility of the privacy team.

- Governance – Oversight maintains a Risk and Information Security Steering Committee to govern its Risk Management and Information Security initiatives. The Oversight Board of Directors is regularly briefed on security and risk issues.
- Operations – operation of production systems is the responsibility of the IT and operations teams.
- Development – development and quality assurance of the Oversight solution is performed by development team members.

- Client Segmentation. Oversight processes information from multiple Clients in its Software as a Service platform. Each Client's data is logically separated from other Client's data but is processed on shared infrastructure. Client users only have access to their company's information.

4. AUDIT AND VERIFICATION.

At least once each calendar year, Oversight will retain a third-party auditor of national reputation (a) to perform audits of the Oversight's Information Security Management System that include Oversight's Data management systems and (b) to produce audit reports. Oversight will provide a summary copy of such reports to its Clients upon request.

Oversight performs internal scans, audits, and compliance checks and will provide an Executive Summary upon request.

Oversight will make available a simulated, sample Client scan target upon request.

Clients who require audits of Oversight's colocation facilities must pay any costs or fees those vendors charge for participating in Client-requested security evaluations, scans, or security evaluations.

5. VULNERABILITY MANAGEMENT.

Oversight maintains a Vulnerability Management Program, as part of the greater Risk Management program. Vulnerability Management includes systems hardening, patching, internal scanning, external scanning, and penetration testing.

6. SUPPLIER AND SUBPROCESSOR SECURITY.

Oversight maintains a comprehensive Vendor Management Program that includes evaluating the security posture of suppliers and subprocessors before work is performed and then annually based on risk assessment by Oversight.

7. SYSTEMS DEVELOPMENT LIFECYCLE.

Oversight's Systems Development Lifecycle process utilizes control standards related to various aspects of the development process such as securing the development environment, source code control, as well as standards around requirements definition, release and deployment, testing and training according to SSAE-18 requirements. Oversight uses test systems that exactly duplicate production for the most efficient problem resolution and highest quality testing.

EXHIBIT 3

DATA PROTECTION AGREEMENT ("DPA")

1. Defined Terms.

"**data controller**", "**data processor**", "**data subject**", "**process/processing**", and "**supervisory authority**" shall have the meanings set out in the applicable Privacy Laws;

"**CCPA**" means the California Consumer Privacy Act of 2018.

"**Data Protection Laws**" means rules and regulations applicable with respect to the processing of Personal Data under the Agreement and this DPA, including the European Data Protection Laws, UK Data Protection Laws, LGPD and the CCPA, each as updated, amended or replaced from time to time.

"**European Data Protection Laws**" means all Privacy Laws in the European Territories and which are applicable to the Personal Data in question including, where applicable, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (**"GDPR"**), the Swiss Federal Data Protection Act and its ordinances, and any applicable associated or supplementary data protection laws or regulations.

"**European Territories**" means collectively (i) the European Economic Area (**"EEA"**), namely the European Union (**"EU"**) Member States and Iceland, Lichtenstein and Norway, and Switzerland.

"**LGPD**" means the Brazilian Lei Geral de Proteção de Dados Pessoais Law n. 13.709/20.

"**Personal Data**" means Data that, alone or in combination with other information, is about, related to, or can be used to identify an identifiable living natural person. For clarity purposes, hashed, truncated, or encrypted versions of the foregoing that are unusable to uniquely identify an individual are not Personal Data for purposes of this DPA.

"**Subprocessor**" means any third party, appointed by Oversight to process a Client's Personal Data.

"**UK Data Protection Laws**" means the United Kingdom (**"UK"**) Data Protection Act 2018 and the UK General Data Protection Regulation.

2. Generally.

a. For purposes of this Exhibit 3 DPA, the parties agree that Client is the data controller of Personal Data and Oversight is the data processor of such data.

b. This DPA applies to the processing of Personal Data by Oversight on behalf of Client.

c. Oversight will ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

d. Oversight will take all measures required pursuant to Article 32 of the GDPR.

e. Oversight is prohibited from: (i) selling the Personal Data (as **"selling"** is defined in §1798.140(t) of the CCPA; (ii) retaining, using, or disclosing the Personal Data for any purpose other than for the specific purpose of performing the services specified in Agreement; and (iii) retaining, using, or disclosing the Personal Data outside of the direct business relationship between Oversight and Client.

f. Oversight shall immediately inform Client if, in its opinion, an instruction infringes the Data Protection Laws.

3. **Processor and Controller Roles and Responsibilities.** Oversight will process Personal Data only on documented instructions from Client and as set forth in the Agreement. Any additional or alternate instructions must be agreed to in an amendment to the Agreement. If the GDPR applies and Client is a processor, Client warrants to Oversight that Client's instructions, including appointment of Oversight as a processor or subprocessor, have been authorized by the relevant controller.

4. **Processing Details.** The parties acknowledge and agree that:

a. The subject-matter of the processing is limited to Personal Data within the scope Data Protection Laws;

b. The duration of the processing shall be for the duration of the term of the Agreement and until all Personal Data is deleted or returned in accordance with the terms of the Agreement;

c. Client is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Oversight by or on behalf of Client, and (ii) the means by which Client acquired any such Personal Data;

d. The nature and purpose of the processing shall be to provide the Services pursuant to the Agreement;

e. The categories of Personal Data processed by Oversight are set forth in Section 12 of this Exhibit 3; and

f. The types of data subjects are set forth in Section 12 of this Exhibit 3.

g. At the choice of Client, Oversight will delete or return and then delete all the Personal Data to Client after the end of the provision of the Services and securely delete existing copies unless Data Protection Laws requires the continued storage of the Personal Data.

h. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Client and Oversight

shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

i. the anonymization, pseudonymization and encryption of Personal Data;

ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

iii. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

iv. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

i. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

5. **Data Subject Rights; Assistance with Requests.** Oversight will make available to Client in a manner consistent with the functionality of the Services and Oversight's role as a processor of the Personal Data of data subjects, the ability to fulfill data subject requests to exercise their rights under Data Protection Laws. Oversight shall comply with reasonable requests by Client to assist with Client's response to such a data subject request. If Oversight receives a request from Client's data subject to exercise one or more of its rights under Data Protection Laws in connection with the Services, Oversight will redirect the data subject to make its request directly to Client. Client will be responsible for responding to any such request. Oversight shall comply with reasonable requests by Client to assist with Client's response to such a data subject request.

6. **Records of Processing Activities and Processor Responsibilities.** Oversight shall maintain all records required by Data Protection Laws (such as Article 30(2) of the GDPR) and, to the extent applicable to the processing of Personal Data on behalf of Client, make them available to Client upon request. Oversight will make available to Client all information necessary to demonstrate compliance with Processor responsibilities (such as the obligations set forth in Article 28 of the GDPR) and allow for and contribute to audits, including inspections, conducted by Client or another auditor mandated by Client.

7. Data Security.

a. Oversight has implemented and maintains appropriate technical and organizational measures to protect Data and Personal Data as set forth in Exhibit 2 to the Agreement. Oversight will make available such other information as is reasonably requested by Client regarding Oversight security practices and policies. Oversight will assist Client in demonstrating compliance with the obligations pursuant to Data Protection Laws (such as Articles 32 to 36 of the GDPR), taking into account the nature of processing and the information available to Oversight.

b. If Oversight becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Data or Personal Data while processed by Oversight (each a **"Security Incident"**), Oversight will promptly and without undue delay (1) notify Client of the Security Incident; (2) investigate the Security Incident and provide Client with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

c. Client is solely responsible for complying with its obligations under incident notification laws applicable to Client and fulfilling any third-party notification obligations related to any Security Incident; provided, however, Oversight shall make reasonable efforts to assist Client in fulfilling Client's obligation under Data Protection Laws or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

8. **Use of Subprocessors.** The Subprocessors used by Oversight to the provide Services as of the Effective Date are listed at https://www.oversight.com/sub-processors. Oversight has entered into an agreement with each Subprocessor containing data protection obligations no less protective than those in this Agreement with respect to the protection of Client Data to the extent applicable to the nature of the Services provided by such Subprocessor. Oversight will inform Client of any intended addition of Subprocessors at least thirty (30) days in advance, thereby giving Client the opportunity to object. If Client objects to the use of a new subprocessor by notifying Oversight in writing within ten (10) business days after receipt of Oversight's notice, Oversight will use reasonable efforts to recommend a commercially reasonable change to Client's use of the Services to avoid processing of Personal Data by the objected-to new subprocessor without unreasonably burdening Client. If Oversight is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Client's sole remedy is to terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Oversight without the use of the objected-to new subprocessor by providing written notice to Oversight. Oversight is liable for the acts and omissions of its Subprocessors to the same extent Oversight would be liable if performing the services of each subprocessor directly under the terms of the Agreement.

9. **Data Protection Indemnity.** Each party will, at its expense, defend, and will indemnify and hold harmless the other party, its Affiliates, and their respective officers, directors, employees, or agents from and against any amounts payable (including costs, expenses or liability, including reasonable attorney's fees and costs, related to an allegation) resulting from, any third party claim or suit, to the extent such third party claim or suit alleges loss of data or damages resulting from a failure to comply with the provisions set forth in this Exhibit 3.

10. **Transfer Mechanisms.** For purposes of personal data transfers from European Territories, Oversight complies with the Controller to Processor Standard Contractual Clauses incorporated herein from https://www.oversight.com/eu-standard-contractual-clauses by

reference. For Personal Data transfers from countries outside the European Territories, Oversight will enter into appropriate personal data transfer agreements on request.

11. Data Subjects.

Data Subjects may include:

- Personnel Client authorizes to access the Service.
- Personnel initiating, reviewing, modifying or approving Client's corporate-spend.
- Personnel listed as attendees in Client's expense reports.

12. Categories of Data.

The categories of Personal Data transferred may contain: company name, employee name, attendee name, title, corporate email address, email contents, telephone number, userid, employee id, IP address, personnel-initiated corporate-spend details including location, personnel home country.