cOASIS SERVICE LEVEL AGREEMENT

PURPOSE

The purpose of this Service Level Agreement ("SLA") is to provide a statement of Licensor's commitment to Availability of the Application Services (as defined in the License Agreement) made available to Licensee as further described in the Statement of Work (Exhibit D); provide an economic remedy should the Availability of the Application Services fall below the commitment level; and outline policies and procedures the Licensor uses to manage and maintain the Application Services and any related staff support services.

DEFINITION OF TERMS

"**Application Remedy Fee**" is defined as ten percent (10%) of the cOASIS License Fee.

"**Availability**" is defined as the ability to access the Application Services without downtime or outages (other than downtime or outages specifically excepted below).

"**Disaster Recovery**" is defined as providing to Licensee fully functioning Application Services in the same or another physical location in the event of a major hardware or network outage.

"**Incident**" is any unexpected result based on the specifications and documentation of the Application Services set forth in the Statement of Work or hosted sites.

"**Scheduled Maintenance**" is defined as the scheduled (daily, weekly, monthly, quarterly, semiannual or annual) operation tasks to maintain the integrity of Licensor hardware, applications, and network including periodic backups, system logging, disk space management, and performance tuning.

"**Security**" is defined as the managed authorization to access the Application Services, application site, the application programs, operating system, internal network, the database, data contents and the physical site.

"**Security Incident**" is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed through the Application Services.

"**Software Defect**" means a material failure of the Application Services to conform to the current specifications, including but not limited to functions that generate programming error messages, system errors, or "hung" or halted pages.

AVAILABILITY OF APPLICATION SERVICE

Licensor and its providers will host the Application Services and related software for Licensee. The cost and expense of all hardware and hosting of the Application Services are the sole responsibility of Licensor. Licensor's standard for the Availability of the Application Services is ninety-nine and a half percent (99.50%) of every calendar month. ("**Application Service Threshold**"). Notwithstanding this standard, Licensor agrees to the remedies provided below for failure to maintain such Availability.

Process for Determining Application Availability:

Licensor shall monitor Application Availability by having monitoring software request an application validation page from the Application Services on each of Licensor's application servers every five (5) minutes. If the Application Services does not respond or responds incorrectly on any server to two (2) consecutive requests, an automated alert to a possible state of Application Unavailability will be generated. Due to the clustered architecture of the Application Services, Application Unavailability should only occur in cases of concurrent unavailability of all clustered servers or unavailability of the database server. At Licensee's request, Licensor shall use data from these automated alerts to calculate Licensee's Application Unavailability (as defined below) for a calendar month and send the results of the calculation to Licensee.

"**Application Unavailability**" consists of the number of minutes that the Application Services was not Available to Licensee, but expressly does not include time for the following: (a) Scheduled Maintenance; (b) unavailability resulting from Licensee's equipment or facilities; (c) unavailability resulting from acts or omissions of Licensee contrary to this SLA, the License Agreement, or the applicable documentation; (d) unavailability resulting from upgrades to the service or equipment by Licensor; (e) unavailability resulting from the proper implementation of Operating System recommended Critical Updates; (f) unavailability resulting from the proper implementation of recommended Security Updates and Patches; and (g) unavailability resulting from reasons of Force Majeure (as defined in the License Agreement).

Process for Calculating Application Service Threshold and Service Credits:

For each cumulative hour or fraction thereof of Application Unavailability in excess of 0.5% in a calendar month, Licensee may request a service credit in accordance with the percentages set forth in the following table. The Application Service Threshold percentage will be calculated by dividing the total number of minutes in which there was Application Unavailability during an applicable month (excluding unavailability due to items (a) – (g) in the "Process" paragraph above) by the total number of actual minutes in such month (also excluding unavailability due to items (a) – (g) in the "Process" paragraph above), and then subtracting the resulting number from 1 and multiplying that amount by 100; *i.e.*, a calculation using the following formula: 1- (total Application Unavailability minutes in a month "except unavailability due to items (a) –

(g)" in the "Process" paragraph above]/total minutes in said month "except unavailability due to items (a) – (g)" in the "Process" paragraph above]) x 100.

Service Credits calculated under this Section are available to Licensee, provided that no credits are available to Licensee for those months in which Licensee was either not using the Application Services or had failed to make payments to Licensor as required by the License Agreement. In no case shall the sum of the credits issued for any given year for the Application Remedy Fee exceed ten percent (10%) of the cOASIS License Fee for Client.

The following schedule specifies the service credit schedule for failure to meet the Application Service Threshold.

Application Service Threshold	
Availability	**Service Credit Per Month**
99.50% or greater	None
99.00% to but not including 99.50%	5% of Application Remedy Fee
98.50% to but not including 99.00%	10% of Application Remedy Fee
98.00% to but not including 98.50%	15% of Application Remedy Fee
97.00% to but not including 98.00%	18% of Application Remedy Fee
Less than 97.00%	20% of Application Remedy Fee

***Service Credits*:**

In order for Licensee to receive a credit hereunder, it must request a credit within forty-five (45) calendar days after an Application Unavailability. Licensor will monitor Application Availability and notify Licensee if the Application Service Threshold is not met. Licensee will send an electronic mail message to the Licensor's controller requesting the credit.

***Scheduled Maintenance*:**

Licensor will maintain and upgrade its servers and infrastructure in a manner consistent with standard industry practice and will use commercially reasonable efforts to prevent and mitigate security risks, performance outages or loss of vendor support. To this end, Licensor may schedule infrastructure maintenance during normal business hours. If access to the Application Services is to be impacted, Licensor will make commercially reasonable efforts to provide Licensee at least seventy-two (72) hour notice. Licensor will consider the deadlines and meeting schedules of all clients when scheduling down time.

***Emergency Maintenance*:**

Licensor will perform emergency maintenance in its sole discretion when an emergency condition exists. Licensor will include authorized Licensee staff in the standard Licensor

notification process of emergency downtime. Emergency maintenance shall not be categorized as Application Unavailability as defined in the process sections above.

For purposes of this SLA, "**Emergency Maintenance**" shall be defined as activities to remediate, implement, or address security upgrades, hardware failures, network failures, software failures or any condition that in Licensor's sole discretion Licensor believes has or will negatively impact the Availability of the Application Services or database. Licensor may take the necessary steps to assure the continuity of service for all Application Services users.

***Critical Incident Response Team*:**

Licensor maintains a Critical Incident Response Team (CIRT) staffed by Licensor infrastructure technicians, developers, and executive staff. CIRT responds when automated or human monitoring detects an interruption in Application Availability. CIRT is responsible for escalating any interruption in Application Availability and communicating internally and externally about the estimated time to resolve the incident. Licensor's standard for communication about critical incidents is fifteen (15) minutes after assembly of the CIRT and every thirty (30) minutes thereafter until the incident is resolved. Licensor will communicate with Licensee and cooperate in efforts to ensure that infrastructure related to the meetings in this Agreement are operating and interfacing as intended and, if necessary, CIRT will call Licensee's designated technical representative in on any incidents to resolve Licensee infrastructure issues.

LICENSOR STANDARDS, POLICIES AND PROCEDURES

Software Defects:

Software Defects will be remediated without cost to Licensee. Licensor will use commercially reasonable efforts to remediate any defects according to severity of the defect. Should the defect be caused by a browser vendor's release of a new version of a browser, Licensor may communicate to users such problem with that browser version until a remediation strategy is identified and implemented.

Supported Browsers:

The list of currently supported browsers can be found on the cOASIS Knowledge Base. Log into cOASIS administration site; select Help from the main menu; click on the Knowledge Base tab; and select Recommended Browsers under the Categories section.

Service Policies:

Licensor offers support services in conjunction with the Application Services that are described in the Statement of Work. These services may include, but are not limited to, configuration of the Application Service for Licensee, reporting support, specific module support such as

notification creation and transmission, end-user phone and email support, participation in program planning and committee meetings, and training and product support to Licensee staff. Service engagements are guided by the Statement of Work and the timelines created therefrom. The timelines include both Licensee and Licensor tasks and are stored in Licensor's SharePoint (or successor) system with web-access to Licensee staff to tasks and task status. Additionally, a task status email is sent weekly to Licensee staff and Licensor services staff containing the status of tasks.

Through the system of project task creation, visibility and accountability, Licensor provides a method to reduce last minute tasks that could compromise the workflow cycle. But even with these measures, Licensee requests may be surfaced at the last minute and a policy has been created to incorporate such requests.

Licensor operates Client Services teams for the purpose of supporting Licensee throughout the use of Application Services. The specific support provided is specified and detailed in Exhibit D and is considered "in-scope" of the agreement. Notwithstanding the response that Licensor has outlined in the section titled Critical Incident Response Team above, Licensor maintains normal business operating hours for the teams it has located in Europe and the United States. Members of these teams are reached via the branded client email address and escalation list email and phone numbers provided. Licensor may assign team members in accordance with the provisions of Exhibit D to provide support to Licensee.

Licensor may make use of subprocessors to fulfill provisions of Exhibit D. Licensor's current list of subprocessors that may be used is available here.

The parties recognize that the nature of the content workflow for abstract and presentation management lend themselves to project planning rather than last minute "ticketing" requests, but it is also understood that last minute requests may arise. Licensor maintains a help desk ticketing system that allows Licensee to make requests of Licensor. This system also provides visibility into the status and timeliness of the requests.

Licensor's standard for requests made through the help desk ticketing system are:

	Acknowledgment	Resolution, if in-scope	Quote, if not in-scope
High Priority	4 business hours	1 business day	1 business day
Medium Priority	1 business day	2 business days	3 business days
Low Priority	2 business days	2 business days	Mutual Agreement

Acknowledgement means that Licensor responds to the Licensee representative making the request via email or phone.
High Priority requests are understood by the Parties to mean a request that will have a material impact on the collection of content in the Licensor's tool, a material impact on the Licensee's

meeting if during the dates of the meeting, and/or an action having material cost impact to the Licensee.
Low Priority requests are generally considered to be training issues or feature requests.

Reporting from the help desk system is available to Licensee from time to time at Licensee request and with commercially reasonable response time from Licensor.

Information Security Policies for Licensor's Product and Licensor's Services:

Licensor has established policies with the development of its products and the delivery of its services acknowledging that while Application Services are directed at the widest possible distribution of scientific and educational content, the lifecycle of that content, certain actions taken on that content, and the personal information of submitters, presenters, members and other roles within the content lifecycle are considered by policy and regulation to be sensitive information requiring Security.

Licensor's systems are designed to promote such Security and are updated as technology and security threats evolve. Access to all Licensor systems is password controlled. Where supported, Multi-Factor Authentication (MFA) is utilized as an additional layer of protection. Federated Single Sign-On (SSO) with a customer's membership management system is recommended as the strongest layer of security and privacy, and all modules of the Application Services can be integrated with SSO. Licensor uses cloud-based hosting, where all servers are configured in Virtual Private Clouds (VPC) which in turn allows creation of public and private subnets to control system access. Private subnets isolate the Licensor systems from all other systems. Multiple layers of security, including subnets, security groups and network access control lists are employed to control access to the Licensor systems. Licensor follows cloud provider's security recommendations, and access to the Licensor servers is controlled by Virtual Private Network software (VPN) and security groups. The security groups act as a firewall to control inbound and outbound traffic to the Licensor systems. By default, all public inbound traffic is prohibited. The security groups are configured to allow HTTP and HTTPS traffic and only the additional ports necessary for proper operation of the Application Services. Load balancers are used to distribute workload across multiple servers. Although credit card data is not stored within Application Services, payment connections can be established to connect to a third-party processor, and therefore Licensor tests, on a quarterly basis, for PCI compliance. Periodic vulnerability testing is also performed.

Licensor's staff, including those involved in delivering services outlined in the Statement of Work, are made aware of the need for Security during the content lifecycle. Licensor staff are expected to follow procedures to encrypt any personal data sent via attachments or email. The parties recognize that given the critical nature of deadlines, Licensee and its agents may from time-to-time direct Licensor staff to communicate personal data outside these recommendations.

Licensor will notify Licensee within twenty-four (24) hours of any Security Incident related to Licensee's Data.

EMBARGOED CONTENT

The parties understand that the Application Services may be used for the collection and review of content that Licensee will by policy have not yet made public ("Embargoed Content"). Embargoed Content is considered Confidential Information as specified in the License Agreement between Licensor and Licensee. Licensor has designed certain modules of the Application Service to restrict display of the Embargoed Content until a date specified by the Licensee. Licensee is responsible for maintaining and confirming the dates for Embargoed Content. Licensor has also included functionality in the Application Services to log view access by administrative users to abstract content. These view logs are available to Licensee within the Administrative Module.

BACK-UP & RETENTION POLICIES FOR LICENSOR'S PRODUCT

Licensor has developed back-up and retention policies that support the requirements of the Application Services. A variety of back-up strategies are employed, including snapshots of virtualized servers in the cloud, redundant database instances that exist across multiple cloud zones, and transactional back-up of MS SQL Servers. Database server data are persistent for the term of the Agreement in that "delete" is limited to specialized functions such as score reports, and only then with verification. Specialized deletions (such as Right to Be Forgotten) are available only via Licensor's database administrator staff. Back-up and retention policies may vary at Licensor's sole discretion, but in no case will back-up of database servers and content servers be less than daily and in no case will uploaded content or database backups be retained for fewer than seven (7) days.

COMPLIANCE WITH ACCESSIBILITY GUIDELINES

Licensor makes commercially reasonable efforts to comply with existing accessibility standards including Web Content Accessibility Guidelines (WCAG 2.1), European Accessibility Act (EAA/EN 301549), Americans with Disabilities (ADA Title III) and Accessibility Canada Act (ACA). In addition to designing our Application Services with these requirements in mind, Licensor makes use of an optional accessibility plug-in known as AccessiBe to provide additional accessibility options.

COMPLIANCE WITH CAN SPAM

Licensor makes commercially reasonable efforts to comply with the Canadian Anti-Spam Legislation (CAN SPAM). Notwithstanding that, the parties recognize that the Application Services are capable of sending email to whomever the Licensee specifies. Licensor

recommends that Licensee follow the provisions of CAN SPAM, including incorporating notice and unsubscribe functions available in the Application Services.

COMPLIANCE WITH DATA PRIVACY LEGISLATION

Licensor makes commercially reasonable efforts to comply with the European Union's General Data Protection Regulation (GDPR) and the applicable privacy and data protection legislation enacted by states within the United States. With respect to GDPR, the Parties agree that Licensor is considered to be a Data Processor and has policies with respect to data privacy and retention, Subject Access Requests, Right to Be Forgotten, and notice of Security Incidents. Licensor's current privacy policy detailing our policies is available here. Licensor's current Data Processing Agreement that governs our processing of Personal Data is available here.

Licensor makes use of cookies in its Application Services in order to provide users with essential functionalities, remember user preferences and to gather critical security and operational usage information. Licensor has implemented a process to capture cookie preferences from end users across all Application Services. Licensees already managing cookie preferences may deactivate and/or request assistance in deactivation of the Licensor's cookie capture preference process.

Licensor recommends that:

- Licensee use Federated Single Sign On strategies to limit the amount of information transmitted to Licensor to only that required for the workflow task;
- Licensee document the Right to Be Forgotten consistent with the needs of Licensee's workflow; and
- Licensee adopt policies for notification in case of Security Incidents.

THIRD PARTY DATA ACCESS AGREEMENT

Licensee may have third-party vendors, contractors, and suppliers that may need to access Licensee data through Licensor Application Services. To ensure all parties understand their obligations to Licensee and Licensor, such parties must sign a Data Access Agreement (DAA). The DAA details their obligations as a user of Licensor Application Services, the permitted uses of Licensor Application Services, and their responsibilities regarding any changes to Licensor Application Services.

APPLICATION PERFORMANCE UNDER LOAD

Licensor has designed the Application Services to make use of auto-scaling capabilities within the cloud hosting environment and periodically performs load testing to ensure compliance with known and projected usage. Specific load requirements above Licensor's normal

projected load can be specified in the Statement of Work with any associated fees detailed in Exhibit E.

CHANGES TO SLA

Amendment to Service Level Agreement

Licensor may, at its sole discretion, make changes to this SLA based on changes to the features or functions of the Application Services or as required by any third-party providers to Licensor; provided that any change to the SLA does not affect the calculation or allocation of Service Credits, Backups and/or Disaster Recovery. Any other amendments or modifications to this SLA may be made only by mutual written agreement of the parties. The current SLA can be found on the cOASIS Knowledge Base. Log into cOASIS administration site; select Help from the main menu; click on the Knowledge Base tab; and select Service Level Agreements (SLA) under the Categories section.

New Applications

Licensor will apply the appropriate development process and service level for all applications or enhancements, even if the product enhancement is outside of the Application Services, or applied only to Licensee. Licensor will, at its sole discretion, determine the definition of "appropriate development process and/or service level."

GENERAL TERMS AND CONDITIONS

Dependence on Other Organizations

If Licensor is dependent on other internal Licensor resources (*i.e.*, help desk, database services, etc.) or external suppliers in order to provide application support services to Licensee, Licensor will manage the interface into those internal Licensor resources or suppliers (and will be responsible for the performance of such internal Licensor resources or suppliers) as it relates to the provision of services under this SLA.

Revised June 14, 2024