Bio-ITech Service Level Agreement Cloud

1. General

This Service Level Agreement ("**SLA**") describes the maintenance and support levels available for the Software provided by Bio-ITech in the cloud as available at https://www.elabjournal.com. This SLA is subject to the General Terms and Conditions of the Bio-ITech division of Eppendorf, Inc. (Bio-ITech) of which a copy can be downloaded at https://www.bio-itech.nl/deliveryconditions/. In case the SLA is inconsistent with the General Terms and Conditions, the SLA will prevail.

The duration of the SLA is linked to that of the license for the Bio-ITech software. If support is required outside of the active license period, Bio-ITech will have the right to issue an additional quotation before the requested support is provided.

In all cases, Diagnosis Times, Resolution Times, and other services can only be met if the Client and the organization Key-User or Administrator are responsive to communication and cooperative.

If Bio-ITech needs additional information about a Support Request from the client, the time between Bio-ITech's follow up inquiries and the Client's answer (support ticket status "Pending") will not be considered in the calculation of the Diagnosis and Resolution Times. The administrative records of Bio-ITech will determine whether the agreed service levels have been met.

The provisions of this SLA are not applicable to the extent that they are beyond Bio-ITech's control, e.g. disruption or malfunction in connected external systems such as those from third party components. The software is supported to be used in the most recent versions of Safari, Internet Explorer, Google Chrome, Mozilla Firefox and Microsoft Edge web browsers. The Service Levels do not apply to other browsers.

Bio-ITech has the right to amend this document at any time, without further notice if at least an equivalent Service Level is delivered without an increase in the SLA charges. The active SLA can be requested at any time or can be downloaded at http://www.bio-itech.nl/terms/

2. Definitions

The terms used in this SLA are defined as follows:

Term	Definition
Bio-ITech	A division, operating from Cambridge (MA), belonging to Eppendorf, Inc., located at Enfield (CT).
Preventive Maintenance	The correction and supplementation of software or server components. The purpose of preventive maintenance is to prevent problems from occurring in the future.
Upgrades	Upgrades to the Software to add/expand on functionality and to fix encountered non-blocking Problems.
Corrective Measures	The rectification of Problems in the Software.
Diagnosis Time	The time needed to assess the content of a Problem or an Incident and to establish problem-solving approaches. The Diagnosis Time is measured from the confirmation of a Support Request concerning a Problem or Incident until Bio-ITech indicates that a start has been made to resolve the issue.
Problem	A reproducible defect in the Software or service provided by Bio-ITech that blocks the software from performing in accordance with the Agreement.
Incident	An event at the Client causing a disruption for using the Software as intended. This includes events related to: • The Client's configuration of the Software • A modified user interface resulting from maintenance.
Key-User	The contact person within the Client organization, appointed by the Client, who provides the 1st line support within the Client's organization in respect of the Software and services provided by Bio-ITech.
Information system	The information system of Bio-ITech on which the Software is installed and implemented.
Maintenance Window	Timeframe for execution of Preventive maintenance: which is from Monday to Friday between 10pm EST and 8am EST and from Saturday 8pm EST to Sunday evening 10pm EST, in accordance with Article 5 of this SLA.
Client	The organization that has entered into an Agreement with Bio-ITech.
Resolution Time	The time between the diagnosis of a Support Request and • In the event of a Problem/Incident: the communication made by Bio-ITech that an update is available • In the case of other support: the answering of the question and closing of the support ticket (status "Solved"/"Closed").
Agreement	This agreement as established between the parties.
Support Request	The Client's request for the resolution of a Problem or Incident or for other types of support.
Software	The software services provided by Bio-ITech to the Client under the Agreement.
Customer Care	Bio-ITech's Customer Support.
Hourly Rate	Bio-ITech's hourly rate of $ 120.00
Working Days	Working Days are from Monday to Friday, with the exception of United States federal holidays.
Office Hours	From 9am - 5.00pm EST on Working Days.

Service Interruption	The event in which the software is not accessible by the Client, due to software or network errors outside of the Client's network and within reach of Bio-ITech.
Service Credit	Credited amount in US dollars ($) that will be used as a deduction for any new and upcoming invoice towards Client.

3. Customer Care, Submission and Processing of Support Requests

Support per organization is most efficient when it is managed and funneled through a single Key-User. When service is delivered to multiple labs within an organisation, the Client is required to appoint a Key-User which acts as a single point of contact to the Bio-ITech Customer Care for sending Support Requests. When services are delivered to individual labs, The Client's Group Administrator is designated as the Key-User. The Client should inform Bio-ITech in a timely manner in case of the replacement of the Key-User. Operational communication concerning Support Requests is conducted primarily with the Key-User.

To receive support, the Key-User can contact the Bio-ITech Customer Care Team via https://elabjournal.zendesk.com/ or by e-mail: support@elabjournal.com. Support Requests made by telephone and using other e-mail addresses are not covered by this SLA unless otherwise agreed.

Once the Support Request has been received, confirmation of receipt will be sent by e-mail to the Key-User. A diagnosis will be made by Bio-ITech in which the applicable category (Problem, Incident or Question) and priority (Urgent, High, Normal or Low) will be determined. The following definitions for the priorities apply:

Priority	Type of Support Request	Examples
Urgent	The Support Request concerns a Problem or Incident as a result of which the Software cannot be used at all by the Client. The Support Request is also clearly marked by the client in the subject header that this is an urgent matter.	There is a Problem with the Software that prevents it from running.
High	The Support Request concerns a Problem or Incident with the result that essential functionality of the Software is not available to the Client. The Support Request is also clearly marked by the client in the subject header that this is a matter with high priority.	The Software freezes when a certain critical feature is being used.
Normal	The Support Request concerns a Problem or Incident that prevents one or more functions of the Software from working properly, there is no work-around, but the Software can be used without any direct problems.	The Software freezes when a non-critical functionality is used, or when a functionality is used that only occurs in very specific cases, for which no work-around exists and that is considered to be non-blocking for working with the Software.
Low	Support Requests for minor bugs, request for upgrades, and user support for general questions.	A question concerning the use of the Software.

Following completion of the diagnosis, the Key-User will receive a notification via phone or e-mail on the subject, after which Bio-ITech initiates the resolution. The Diagnosis and Resolution Times as defined in Article 4 are maintained. The priority of a Support Request can change on an interim basis, e.g. because an alternative or temporary solution is available that affects the Priority.

Support Requests with either the High or Urgent priority status are always processed according to the tables in Article 4. Support Requests with the Low priority status are handled on a fair use policy and should in general not exceed the available Support hours per month based on the SLA Type per organization (see table below). If the number of Support Hours regularly exceeds the applicable maximum per month, the Client can purchase additional Support hours on a recurring (with 50% discount) or incidental basis (at 100% price) subject to the Hourly Rate when needed.

SLA Type	Low Priority Support hours per month
Bronze	2
Silver	3
Gold	5

4. Workhours

The Diagnosis Time and Resolution Time are applicable to Problems and Incidents if they are identified as such based on a Support Request. Diagnosis and Resolution Time Hours are applicable exclusively during the Hours and Days as stated in the table below.

Priority	Bronze	Silver	Gold
Urgent	9:00 am - 5:00 pm W	8:00 am - 5:00 pm WW	8:00 am - 10:00 pm A
High	9:00 am - 5:00 pm W	8:00 am - 5:00 pm WW	8:00 am - 10:00 pm AE
Normal	9:00 am - 5:00 pm W	8:00 am - 5:00 pm W	8:00 am - 5:00 pm W
Low	9:00 am - 5:00 pm W	8:00 am - 5:00 pm W	8:00 am - 5:00 pm W

Times are in EST time-zone. Abbreviations used are W: Workdays. WW: Workdays and Weekends except for national holidays. AE: Any day except for national holidays. A: Any day including national holidays.

4.1 Problems and Corrective Measures

Priority	Bronze		Silver		Gold	
	Diagnosis	Resolution	Diagnosis	Resolution	Diagnosis	Resolution
Urgent	< 8 hours	< 16 hours	< 6 hours	< 8 hours	< 2 hours	< 4 hours
High	< 8 hours	< 16 hours	< 8 hours	< 8 hours	< 2 hours	< 6 hours
Normal	Best effort	Best effort	< 24 hours	< 36 hours	< 8 hours	< 16 hours
Low	Best effort	Best effort	< 72 hours	Best effort	< 8 hours	< 36 hours

4.2 Incidents

Priority	Bronze		Silver		Gold	
	Diagnosis	Resolution	Diagnosis	Resolution	Diagnosis	Resolution
Urgent	Best effort	Best effort	< 16 hours	< 16 hours	< 8 hours	< 8 hours
High	Best effort	Best effort	< 16 hours	< 16 hours	< 8 hours	< 8 hours
Normal	Best effort	Best effort	< 16 hours	< 16 hours	< 8 hours	< 16 hours
Low	Best effort	Best effort	Best effort	Best effort	< 8 hours	< 32 hours

Solutions to Problems or Incidents are provided during Software updates, unless explicitly communicated otherwise with the Client. A Problem or Incident is considered resolved when the availability of the applicable Software update is communicated to the Client.

5. Maintenance, Updates

Corrective Measures and Preventive Maintenance are taken at the sole discretion of Bio-ITech.

The Client and Bio-ITech may choose to annually identify and evaluate the need or wish for customizations to the Software. Bio-ITech is not bound by any obligations based on this evaluation. Bio-ITech will make a separate offer if custom Upgrades are requested, and will perform said Upgrades after obtaining the explicit approval of the Client. Diagnosis and Resolution Times for custom Upgrades, Corrective Measures and Preventive Maintenance are not applicable, if they are not based on Support Requests made by the Client.

Upgrades, Corrective Measures, Preventive Maintenance and, where applicable, solutions to Support Requests may result in a Software update. Bio-ITech will deploy Software updates within the Maintenance Window unless otherwise agreed.

The frequency and actual time of installation of updates, will be decided based on the impact of the installation (e.g. expected downtime) and the impact on the Client/End-user in the event the update is delayed. The priority is classified as Urgent, High, Normal or Low, based on the definitions given in Article 3.

Update impact	Priority	Frequency
Major (>5 min. downtime)	Urgent	At the discretion of Bio-ITech
	High	Within the Maintenance Window
	Normal	Within the Maintenance Window
	Low	Within the Maintenance Window
Regular (<5 min. downtime)	Urgent	At the discretion of Bio-ITech
	High	Within the Maintenance Window
	Normal	Within the Maintenance Window
	Low	Within the Maintenance Window
Minor (no downtime)	Urgent	At the discretion of Bio-ITech
	High	At the discretion of Bio-ITech
	Normal	At the discretion of Bio-ITech
	Low	At the discretion of Bio-ITech

If the update is in response to a Support Request, the priority as designated in the Support Request transcends. The Client will be informed as soon as an update is available that resolves the Support Request. The updates will be installed in accordance with the table above, based on impact and priority.

6. Availability Guarantee.

During the term of the Agreement, Bio-ITech will make the Software available twenty-four (24) hours a day, seven (7) days a week, at least for 99.0% for the Bronze SLA, and 99.9% for Silver and Gold SLA of the time as measured on a monthly basis, excluding the Maintenance Window. Bio-ITech will have failed to meet the required Availability if the Software fails to achieve the percentage Availability, as measured over the period of a given calendar month, in accordance with the following formula:

$$a = \frac{[(b-c)-d]}{b-c} \times 100$$

"a" = the actual percentage of the Availability in such month;
"b" = the total number of hours in such month;
"c" = the total number of Maintenance Window time in such month; and
"d" = the total number of hours of Service Interruption in such month.

7. Backup, Restore and Security

System Reliability

Bio-ITech will ensure, and will cause Affiliates and Subcontractors to ensure, as applicable, that all networking components, load balancers, web servers, application servers, database servers, and storage devices used to provide the Services and to Process or store Client's Data are configured using accepted industry-standard redundant design methodology, including, at a minimum: (i) web and database server clustering and load balancing; (ii) file system and database mirroring, replication, or other equivalent technologies; and (iii) carrier-class disk storage using RAID disks and multiple data paths. Bio-ITech will ensure that all Client's Data up to the last committed transaction is automatically backed up, at least daily, and encrypted on a regular basis, and backup media, where relevant, is verified for integrity and stored at a secure offsite facility. Bio-ITech will be responsible for the restoration of any lost Data. In the event of information processing errors caused by Bio-ITech, upon reasonable request, and subject to reasonable security procedures, Client will be permitted to request a restoration of Data from the most recent backup files.

Backup Procedures

Bio-ITech will operate the Software Services in accordance with the following procedures to enhance security. Bio-ITech will: (i) ensure that Client's Data is backed up encrypted and stored in a location and format available for retrieval as needed; (ii) store copies of Client's Data and data recovery procedures in a different place from where the primary computer equipment processing the Data is located; (iii) have specific procedures in place governing access to copies of Data; (iv) review data recovery procedures at least every six months.

Disaster Recovery and Business Continuity

Bio-ITech currently has and will maintain at all times an appropriate disaster recovery, business continuity and contingency plan and related policies and procedures (collectively, the "DR Plan"). The DR Plan will provide for continued operation in the event of a catastrophic event affecting Bio-ITech's business operations and will be in accordance with internationally accepted business continuity, contingency and disaster recovery planning standards, procedures and practices, including, at a

minimum, a disaster recovery facility that is geographically remote from its primary data center, along with all required hardware, software, and Internet connectivity sufficient to provide the Services without substantial reduction or degradation of functionality or availability, in the event the primary data center were to be rendered unavailable. Consultant will test all features of its DR Plan at least once per calendar year.

Intrusion Detection/Prevention

Bio-ITech, or an authorized third party, will actively monitor the Services and the Systems for unauthorized access, interception, or interruption using accepted industry-standard network-based intrusion detection or prevention mechanisms or Web Application Firewalls. The monitoring systems will raise incident related tickets following security incident SLAs. Bio-ITech will ensure, by applying appropriate means, that any user with access to Client's Data at the Bio-ITech facilities or the facilities at Bio-ITech's Affiliates, Agents or Subcontractors will have access to Client's Data only based on a least privilege approach/need to know principle.

8. Compliance with privacy laws

Bio-ITech will comply, and will cause all Affiliates of Bio-ITech, Subcontractors and Consultant Personnel to comply with: (i) all applicable international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective relating in any way to the privacy, confidentiality or security of Personal Information including, without limitation, the Regulation (EU) 2016/679 of the European Parliament (General Data Protection Regulation), the European Union Directives governing security of network and information systems (Directive 2016/1148), privacy and electronic commerce and communications (Directive 2002/58/EC), and data retention (Directive 2006/24/EC); the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) and relevant provincial laws; the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § § 6801-6827, and all regulations implementing GLBA; the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 et seq., as amended by the Fair and Accurate Credit Transactions Act ("FACTA"), and all regulations implementing the FCRA and FACTA; information security breach notification laws (such as Cal. Civ. Code §§ 1798.29, 1798.82 - 1798.84); laws imposing minimum information security requirements (such as Cal. Civ. Code § 1798.81.5 and 201 Mass. Code Reg. 17.00); laws requiring the secure disposal of records containing certain Personal Information (such as N.Y. Gen. Bus. Law § 399-H), and all similar international, federal, provincial, state and local requirements; (ii) all applicable industry standards concerning privacy, data protection, confidentiality or information security.

Bio-ITech will maintain a comprehensive written information security program according to ISO27001 that complies with applicable Privacy Laws, including mandatory training to Bio-ITech's Personnel who have access to Personal Information regarding the privacy, confidentiality and information security requirements set forth in the Agreement. Bio-ITech's information security program and the information security programs of its Affiliates and all Subcontractors will include appropriate administrative, technical, physical, organizational and operational safeguards and other security measures designed to: (i) ensure the security and confidentiality of Personal Information; (ii) protect against any anticipated threats or hazards to the security and integrity of Personal Information; (iii) protect against any Information Security Incident; and (iv) protect against the use of the Services or Bio-ITech's System as a portal to give unauthorized access to any other systems of Client.

9. Penalties, Claims and Discounts

Diagnosis and Resolution Time

For each day the applicable Diagnosis and/or Resolution Time has not been met, Bio-ITech will credit 1 day of all the payable license fees invoice as a discount. The Client will in this case waive his rights to dissolution, suspension and/or compensation related to these events.

Availability

For each month that Bio-ITech did not meet the minimum availability requirement, the following service credits will be applied of all the payable license fees invoice as a discount:

Availability Percentage	Service Credit
Below 99.9% but over 99.0%	25% of either the monthly fee or 1/12 of the yearly fee (Silver and Gold SLA only)
Below or equal to 99.0% but over 97.5%	50% of either the monthly fee or 1/12 of the yearly fee
Below or equal to 97.5%	100% of either the monthly fee or 1/12 of the yearly fee

Security Incidents

Bio-ITech's liability for Security Incidents and/or any claims from Client towards Bio-ITech due to Security Incidents is limited to the coverage of the Cyber Insurance Liability Policy that Bio-ITech maintains. The Cyber Insurance Liability Policy includes coverage for network security/data protection, liabilities for financial loss resulting or arising from acts, errors, or omissions, in rendering technology/professional services or in connection with the specific services described in violation or infringement of any right of privacy, including breach of security and breach of security/privacy laws, rules or regulations globally, now or hereinafter constituted or amended, data theft, damage, unauthorized disclosure, destruction, or corruption, unauthorized access, unauthorized use, identity theft, theft of personally identifiable information or confidential corporate information. The policy includes breach response costs (including notification costs, forensics, credit protection services, call center services, identity theft protection services, and crisis management/public relations services). Any liability by security incident is only recognized as such when the security incident was caused by the gross negligence or wrongful acts or omissions of Bio-ITech and its employees, directors, officers, subcontractors, agents or other members of its workforce.

Claims

Client is responsible for submitting a claim for any service credits. A claim will only be processed, if the Client has made a Support Request about the Issue or Problem. The claim can be submitted up to 10 Working Days following the end of the calendar month, in which the Support Request to which the claim relates to has been created. Claims can be submitted by email to legal@elabjournal.com. The administrative records of Bio-ITech will be decisive for calculating the total discount.

In all other cases in which Bio-ITech culpably fails to meet its obligations as occurs when Client becomes entitled to any Service Credits for any four (4) months in a twelve (12) month period, the Client will be entitled to dissolution, suspension and/or compensation following written notice of default, granting a reasonable period in which to rectify the non-compliance. Compensation for damages is subject to the limitations of liability provided for in the General Terms and Conditions and/or as described in the Security Incidents chapter.