ANNEX C -¨SERVICE LEVEL AGREEMENT ¨ OR ¨SLA¨
SLA – Service Level Agreement

Model 1 V3 – Standard 2021

1. Scope of this document

Conciliac offers a Help Desk to where our Customers can communicate and report problems, enquiries or bugs (hereinafter "incidents"). Conciliac Help Desk staff is highly trained to detect and identify issues related to the application and their solution. This process might, in exceptional cases, require accessing remotely to the Customer's systems to properly perform this task.

The purpose of this document is to define and establish the process to be followed to report any incident regarding the Conciliac ™ application, through any of the available communication channels, as well as the way in which these incidents will be managed.

The document also defines service levels to be delivered based on the severity of each incident.

Services not included under the scope of this document (non exhaustive list):

- Functional consultancy aimed at designing, planning or defining an individual Customer's specific solution.
- Technical assistance regarding reconfigurations and enhancements to applications already installed, not related to software failures or bugs.
- Individual customizations of the application

Services not included under the scope of this document will be quoted and billed separately.

2. Incident Reporting

The Customer will report the incident through any of the communication channels made available for this purpose:

- E-mail support@conciliac.com
- Telephone +541152784855

Once reported, Conciliac Help Desk Staff will register the incident and provide a ticket identification number that will be used for future reference

Business hours for personal attention channel (telephone) will be from 9:00 AM to 6:00 PM of all working days (GMT-3).

When reporting an incident, the Customer will have to provide the following information:

- Module and functionality where the incident occurs
- Detailed description of the incident
- Steps required to replicate the incident
- Any audit log or file that could help to understand the incident
- Screen shots of the incident
- Does the incident generate a financial and commercial exposure for the Company? 1=Critical, 2=High, 3=Medium or 4=Low/NA
- Does the incident affect the perform in a significative part of the Company's core business? 1=Critical, 2=High, 3=Medium or 4=Low/NA
- Number of users affected

- Is there an alternative solution to complete the job? 1=No, 2=Maybe, 3=Probably or 4=Yes/NA

Conciliac may modify the priority assigned by the customer based on the criteria described under "Determination of the severity of an incident.

Conciliac will analyze the incident and propose at least one course of action to solve it. Should Conciliac Help Desk needed to escalate the incident, the process will be transparent to the Customer, and response times will not be changed.

Once a course of action for a particular incident has been detected, Help Desk Staff will inform the Customer the steps to be taken to ensure the successful solution.

The Customer will implement the solution and confirm whether the incident is effectively solved, after which Conciliac Help Desk will close the ticket and the incident

3. Determination of the severity of an incident

3.1 Severity Classification criteria

In order to determine the severity of an incident, the following criteria will be applied:

- Commercial and Financial exposure
- Operational inactivity
- Number of user affected
- Existence of alternative solutions

All incidents reported will be classified according to these criteria, in order to determine the severity level that most appropriately describes the issue.

Severity Level			
Level 1 – Critical	Level 2 – High	Level 3 – Medium	Level 4 - Low
Commercial and Financial Exposure			
The incident generates a serious financial and commercial exposure for the Company	The incident generates some level of financial and commercial exposure	The incident generates a low financial and/or commercial exposure	The incident generates minimal to no financial and/or commercial exposure
Operational Inactivity			
The incident makes impossible to perform a significative part of the Company's core business	The incident makes impossible to perform a non significative part of the Company's core business	The incident makes impossible to perform some non significative part of the Company's core business, but can successfully execute most of the tasks. This can also include enquiries and requests of information	The incident makes impossible to perform a minimal part of the Company's core business, but can successfully execute most of the tasks.
Number of users affected			

Severity Level			
Level 1 – Critical	Level 2 – High	Level 3 – Medium	Level 4 - Low
The incident affects a substantial number of users (more than 50%)	The incident affects a medium number of users (between 25% and 50%)	The incident affects a small number of users (less than 25%)	The incident may affect no more than one to three users
Existence of alternative solutions			
No acceptable alternative solutions. The job cannot be completed in any other way.	Alternative solutions, acceptable or not, may exist for the incident.	An acceptable alternative solution probably exists for the incident.	An acceptable alternative solution exists and can be easily implemented, to allow the job to be completed.

3.2 Severity weighting and priority determination

Any given incident needs to have at least two of the aforementioned criteria under the same severity level in order to define its priority. Should an incident have one criterion in severity each level, or two in a level and the other two in a different level, the priority will be given by the highest severity level.

The Help Desk agent managing the incident will determine, in conjunction with the Customer, the severity weighting and initial priority in each case.

Examples:

Criteria	Severity 1	Severity 2	Severity 3	Severity 4
Commercial & Financial Exposure	X			
Operational Inactivity	X			
Number of users affected			X	
Alternative Solutions		X		
Priority: Critical				

Criteria	Severity 1	Severity 2	Severity 3	Severity 4
Commercial & Financial Exposure			X	
Operational Inactivity	X			
Number of users affected			X	
Alternative Solutions	X			
Priority: Critical				

Criteria	Severity 1	Severity 2	Severity 3	Severity 4
Commercial & Financial Exposure		X		
Operational Inactivity	X			
Number of users affected		X		
Alternative Solutions				X
Priority: High				

Criteria	Severity 1	Severity 2	Severity 3	Severity 4
Commercial & Financial Exposure				X
Operational Inactivity			X	
Number of users affected			X	
Alternative Solutions		X		
Priority: Medium				

Criteria	Severity 1	Severity 2	Severity 3	Severity 4
Commercial & Financial Exposure				X
Operational Inactivity				X
Number of users affected	X			
Alternative Solutions			X	
Priority: Low				

4. Standard and Maximum Response Time

4.1 Standard Response Time:

Considers the time from the initial report of the incident to the provision of a primary response, analysis of the notified incidence and definition of the standard resolution procedure

4.2 Maximum Response Time:

Considers the maximum timeframe in which Conciliac has to provide a complete and definite solution or adequate course of action to solve the incident. The maximum response time is to be considered once the Standard Response Time is due.

4.3 Response Time per Severity Level

The Standard and Maximum Response Times are shown below:

Incident Severity	Standard Response Time	Maximum Response Time
Critical	Less than 4 (four) hours	2 (two) working days
High	Less than 8 (eight) hours	7 (seven) working days
Medium	Less than 16 (sixteen) hours	30 (thirty) working days
Low	Less than 36 (thirty six) hours	60 (sixty) working days

5. Customer Duties and responsibilities

Conciliac can only assure the abovementioned Standard and Maximum Response times whenever the Customer complies with the following requirements:

Before reporting any potential incident, the Customer has reviewed the Help Tab in the application and searched for self-help in the Support section in the Conciliac ™ web page: www.conciliac.com, containing videos and FAQs

A. The Customer reports the incident through any of the communication channels made available for this purpose: e-mail address, on line chat or telephone.

B. The Customer provides all the information that Conciliac may request in order to seamlessly solve the incidents. Some examples of this information may include log files, configuration parameters, screen shots, etc.

C. The Customer is highly encouraged to create and maintain a testing environment, in which the Customer will have installed the same version deployed in the production environment. The former environment is to be used to perform tests of the application without affecting the latter.

D. All incidents reported in the Production environment need to be replicated in the testing environment, in order to avoid the execution of tests in the Customer's productive environment. Should this not be feasible, the responsibility for performing the testing in the productive environment, as well as the access to potentially confidential information will be Customer's responsibility.

E. If necessary to adequately solve the incident, the Customer will provide remote access to the testing environment to Conciliac Help Desk Staff.

F. Conciliac Help Desk Staff may request, during the incident management process, additional information, files or documents in order to duly identify and solve the incident. The time consumed by the Customer to collect and provide the information requested by Conciliac, up to the moment in which this information is received by our Staff, will not be considered when calculating the Response Times mentioned above.