DISTENCE
DISTRIBUTED INTELLIGENCE

Condence SaaS and support service level agreement

Updated	2023-12-12

Table of Contents

1 Background, Purpose of this document and definitions

The purpose of this document is to describe service content and provide an understanding of the service level and conditions applied to the Condence software as a service (further as: SaaS) product. Any 3rd party hardware with functional support is excluded from the provisions in this document.

Services are provided as a standard service of Distence Ltd. (further as: Service Provider) to customer-defined as service user (further as: Service User). The content of this document is subject to change as the Service Provider continuously improves its product, its operational models and relevant documentation.

General terms applied to the service are defined in a corresponding agreement between parties.

Confidential Information	means any information and material in whatever form disclosed to one Party by the other Party and either marked as confidential or should be understood to be confidential.
Customer	means the user of service, or it's affiliates or end-user customer(s).
Customer Data	means information or material transferred via service platform or Customer to Service or information or material otherwise provided or made available to Service Provider for Customer's benefit and purposes of the Service or other information or material specified as Customer Data by the Parties.
Customer Support	means the support functions provided by Service Provider to Customer.
Datapoint	means an analysis result sent from the edge device to the cloud. The data point consists of a timestamp and the latest analysed value.
Equipment	means the hardware and software which the Customer is required to have in use to use and enable the Service to be provided under this document.
Intellectual Property Rights	means any and all patents, utility models, designs, copyright, domain names, trademarks, trade names and any other intellectual property rights, whether registered or not and applications for any of the aforementioned respectively as well as any trade secrets.
Partner	is distributor of Condence technology having an agreement with Distence Ltd.
Party	refers to the Service Provider, Service User, Customer, User or is any individual, group or organisation participating in providing obligations under this Service.

Service	means services described in this document Condence SaaS service and support service together as within the content referred also separately.
Service Fee	means the agreed fee which covers the provision of the Service for the term of an agreed period.
Service Level	means the levels of performance to which the Services are to be provided to the Customer by Service Provider as specified.
User	means any active user account in the system. User can refer to an organisational entity or a person.
User Guide	means a written set of instructions detailing the usage of the features of the Service, technical requirements and other information relevant to the user of the Service.
User ID	means usernames, passwords or other identification methods to the Service.

2 Grant of access to the Service

The Service Provider agrees in full consideration of the payment of the Service Fee by the Service User to provide access to the Service under the terms and conditions of this document.

Service Users shall permit access to the Service only by those employees, contractors, customers or other third parties who fall within limiting the definition of a User.

Service Users must be preregistered to the service to meet the Service level. This registration process is done during the setup of service with your Service Manager or Key account manager.

Access to Condence online service is from specified web-link https://app.condence.io.

Access to support service is via email support@distence.fi.

Access to the knowledge base for documentation at https://support.condence.io.

Online support service's intent is to provide technical support and problem-solving. Online support is not intended to replace training services.

3 User IDs and Access rights

The Service Provider creates one administrator level user for a Customer account in the system. The administrator Customer account in the system shall be responsible for managing the users having access in the system. Including but not limited to the creation, distribution, and termination of User IDs and managing access rights under an account they control in the system.

Passwords are managed only by Users.

4 Service Provider's Customer Support

The Service Provider shall provide Customer with reasonable technical and use-related Customer

Support. The Service Provider shall provide support during the Service Provider's normal working hours on weekdays from 08:00 – 16:00 Finnish time (EET). The Service Provider shall provide support through email. In urgent cases, the Service Provider may support by phone or via online tools during normal working hours.

The Service Provider shall separately provide the Customer with appropriate contact details. The response time target for support is the next business day.

For the avoidance of doubt, the Service Provider shall not be obliged under this service to provide support, assistance or maintenance concerning third-party networks, equipment, or software.

In case a Customer requires substantial assistance in initialising the Service or integration with the Customers' systems, the Parties may separately agree upon technical support to be provided by the Service Provider.

5 Changes to the Service

The Service Provider shall be entitled to make any such change to the Service that is necessary. These changes could emerge, e.g. from a need to prevent or mitigate data security risks to the Service. If the Service Provider makes a change to the Service, the Service Provider shall inform Customer or Partner of the change in good time or, if this is not reasonably possible, without delay. The Service Provider is not responsible of informing the changes to the service to the end users of Partners.

It is also to be noted that the Service Provider is continuously developing the service and software platform forming the Service. The Services; SaaS Service and support service, are continuously developed, and a new version of the service description and SLA shall automatically apply after one month of publishing. When a new version of this document becomes available, the new version will automatically supersede the old version, making the old version obsolete. Refer to https://support.condence.io for the latest official version of SLA.

6 Monitoring of the service

In addition to the system's design to minimise possible attack vectors, the system uses several tools to monitor and protect the system's integrity.

The direct detection and protection method against malicious actions is the AWS Web Application Firewall (WFA), which protects against attacks such as cross-site request forgery, cross-site scripting (XSS), file inclusion, and SQL injection threats.

The system's health is monitored by monitoring tools provided by the Datadog monitoring service.

7 Service production and compatibility

The Service Provider shall be responsible for the production environment of the Service and for ensuring that the Service corresponds to what is stated in this document.

The Service Provider shall not be responsible for the usability and compatibility of the Equipment or software used with the Service by the end-user or Customer other than expressly stated in general documents, manuals, and instructions.

Customer shall be responsible for acquiring and maintaining the functional status of Equipment that they need to use the Service. Customer shall both be responsible for the protection of their data environment and as well as for the communications costs or similar costs related to the use of

Service.

The Service Provider shall endeavour to make the Service as efficient as possible in terms of the amount of data transfer required between the monitoring equipment and the online services per datapoint. Yet it is noted that a customer might have access rights to create a configuration from the user interface that generates an excessive amount of data points.

7.1 Suspension of the Service

The Service Provider shall have the right to suspend delivery of the Service for scheduled maintenance breaks. The Service Provider shall notify the Customer of the scheduled maintenance breaks and the duration of them in advance. The time used for the scheduled maintenance breaks shall not be taken into consideration to the detriment concerning agreed Service Levels.

The Service Provider shall have the right to suspend delivery of the Service due to installation, change or maintenance work of general data network outside the Service Provider's control or due to severe data security risk to the Service or if required by mandatory law or competent authorities. The Service Provider shall notify the Customer of the suspension and the duration of the suspension in advance or, if this is not reasonably possible, without delay after the Service Provider has become aware of such matter.

7.2 Maintenance of the Service

The Service Provider shall be responsible for maintaining the Service in agreed order and condition. If the Service shall fail or break down, the Service Provider shall use its reasonable endeavours promptly to restore the Services to its proper operating condition under this document.

In the event of any failure or breakdown of the Services with the consequent loss or corruption of the Customer Data or any part thereof, the Service Provider shall notify Customer, as soon as reasonably practicable after the Service is available for use again.

8 Prices and Payment

The Service is provided against monthly Service Fees.

In case additional services, e.g. restoring of data or customer-specific user support is given, additional hourly pricing is adopted. The Service Providers' general price list applies.

In the case of the payment is due for more than 14 days the Service Provider has the right to stop delivering Service.

9 Subcontractors

The Service Provider shall have the right to subcontract its obligations. The Service Provider shall be liable for the work of its subcontractor as for its own.

10 Service Content and Service Levels

10.1 Availability Performance

The Service Provider shall perform its operations to maintain the Service in operation 24/7. The Service Level standard for Service should not at any point drop below 99,9% availability per

calendar month.

10.2 Unplanned Outages

The Service Provider shall perform its operations to minimise unplanned outages on Service or infrastructure which results in an inability to provide the Services for more than a ten (10) consecutive minute period. Unplanned outages should not exceed more than a single ten-minute period in a seventy-two (72) hour period.

10.3 Planned Outages

Service Provider shall notify Customer of all outages or unavailability longer than 10 minutes by sending an email describing the nature, duration and resolution path for each outage to Customer.

Service Provider shall notify Customer of all planned outages more than 10 minutes but less than two hours at least 3 days before and outages more than two hours at least two weeks before such occurrence by sending an email describing the nature and duration, which shall in no event exceed three (3) hours per calendar month, of a such planned outage to Customer.

The target is to arrange planned outages (more than two hours) outside of business hours.

10.4 Excused Outages

The Service Provider shall not be liable for and no consequences are due for outages resulting from factors outside Service Provider's control, such as 1) any accidental network or fibre cuts or general power outages; 2) Force Majeure acts.

For the avoidance of doubt, the Service Provider shall remain liable for any situations that relate specifically to the Service Provider's service provision and Service Provider's IT network when such situations could have reasonably been avoided or mitigated by means in the Service Provider's control.

10.5 Remedies

Service availability is guaranteed to 99,00%. In case the availability of service remains under 99,00% for two consecutive months, Customer is entitled to a service credit amounting to 10% of the Service Fees paid by the Customer in the previous calendar month for each month of non-attainment of the availability target for as long as the availability remains under 99%.

11 Force Majeure Event

Force Majeure Event means any failure by a Party to perform its obligations under this Service caused by an impediment beyond its control, which it could not have taken into account at the time of the conclusion of this document, and the consequences of which could not reasonably have been avoided or overcome by such Party. If not proven otherwise such impediments may include but are not limited to, acts of government in its sovereign or contractual capacity, fires, disturbance of data networks, floods, epidemics, quarantine restrictions, strikes, lock-outs, industrial disputes, riots, acts of terror or specific threats of terrorist activity, transportation or energy. Strike, lock-out, boycott, and other industrial action shall constitute a Force Majeure Event also when the Party concerned is the object or a party to such an action.

Save for the obligation to pay money properly due and owing, neither Party shall be liable for delays and damages caused by a Force Majeure Event.

A Force Majeure Event suffered by a subcontractor of a Party shall also discharge such a Party from liability if subcontracting from other sources cannot be made without unreasonable costs or a significant loss of time.

A Party shall notify the other Party in writing without delay of a Force Majeure Event. The Party shall correspondingly notify the other Party of the termination of a Force Majeure Event.

12 Intellectual Property Rights

The Intellectual Property Rights to the Service and any amendments, modifications, derivate works or new versions thereto shall belong to the Service Provider or third parties. This Service does not grant any rights of ownership in or related to the Service or the Intellectual Property Rights owned by the Service Provider.

13 Customer Data and data processing

Data stored in the system is Customer data. The Service Provider has the right to use the Customer Data only for Service, provisioning of the Service and future improvements of the Service.

Customer data is separated from other customers with different accounts in the Service. User IDs are used to control and grant access to data. Superior users can see, e.g. User IDs are siding user layer/ account. Users with given user privileges can access and extract data with no control of the Service Provider.

When processing the data, the Service Provider in any circumstance, has no right to connect any personal or identifying company data that could identify User, organisation or location of data origins, exposing individuals or organisations

Personal data details include, e.g. user profile: first name, last name, phone, email, and password.

Company data details include, e.g. names of accounts, departments and data structure layer names (e.g. device or site name), user rights, access times or audit logs, documents, IP addresses, and device/hardware information.

However, the service is built on collected data and analytics. Some support services of features in the service may require the processing of data to be performed, be functional or to be optimised.

This does not limit what is said above about the company or Personal privacy.

14 Data backup

Backups for data are handled in Amazon S3 service.

The backups are located at multiple Amazon Web Services (AWS) availability zones (physically separate data centres) in the same AWS region. Data object versioning is used. Data is encrypted and has been protected against bucket deletion. Versioned objects are protected against deletion or alteration. Backups are not accessible with typical administrative roles. Backup data is only used with read-only access for recovery purposes.

All recovery situations are exceptions to the service and will be separately agreed with Customer.

14.1 Back-Up of Customer Data

The Service Provider shall be responsible for making backup copies of the cloud stored Customer Data included in the Service, excluding 3rd party Customer Data stored locally e.g. sensor configurations. The Service Provider shall make backup copies at least once during the Service Provider's normal working day and properly maintain the backup copies in conformity with reasonable industry standards.

If the Customer Data is deleted, lost, altered or damaged by using either the Customer's User ID or either of them has otherwise by its action deleted, lost, altered or damaged the Customer Data, the Service Provider shall have the right to charge for the recovery of such Customer Data on the agreed pricing principles.

The Service Provider shall ensure that the Customer Data back-ups are retained for a minimum period of five (5) months from the expiration or termination.

15 Logs

Logs exist on three distinct levels in the Condence system:

1. Cloud service logs
2. Relay container logs
3. Edge terminal internal logs

15.1 Cloud service logs

The Cloud portion of the Condence system runs in the Amazon AWS environment, and Amazon CloudWatch manages the generated logs. The content and retention policy are determined based on the type and frequency of the data.

Logs covered, but not limited to

- Logins, login attempts, and password resets
- Alarm delivery
- Data replication
- Database
- Processes (Lambdas)

Cloud service logs are not accessible to the end-users.

15.2 Relay container logs

Relay container is a stateless service and does not save or generate any logs internally. Relay container runs inside the customers' IT infrastructure, and tools can process the container output at the customers' disposal for container monitoring.

15.3 Edge terminal logs

In edge terminals, the logging level is, by default, the lowest level and only significant incidents are reported to the cloud. For troubleshooting purposes, the Service Provider can turn debug-level logging on.

Edge terminal logs are not accessible to end-users.

16 Removal of Customer Data

The Service Provider has the right to remove data after an edge device has been inactive for 3 months.

17 Responsibilities

Service Governance	Service Provider	Service User
SaaS service levels and Service Level Agreement (SLA)	X	
Provide access and provide basic instructions on using service	X	

Service management and delivery	Service Provider	Service User
Architect and design infrastructure, capacity, storage, backup, and recovery	X	
Set up device parameters and configure smart terminal parameters		X
Set up and configure data connections		X
Ensure terminal parameters are reasonable and data transmitted and stored is on a reasonable level		X
Manage platform services, such as the servers, databases, storage, and backup process	X	
Provide administrative support for lifecycle management	X	
Create a deployment plan with specific steps to complete upgrades and apply fixes	X	
Manage SaaS patching or upgrading	X	
Provide ID and access management for platform user interface	X	
Monitor system availability and performance	X	

Incident and problem management	Service Provider	Service User
Report incident, request service		X
Receive trouble report as the first point of contact	X	
Answer support requests questions from users	X	
Create or log a service request ticket based on observed system behaviour	X	
Create or log a service request ticket based on system alerts	X	
Validate incident information availability and capture all relevant information within the service request ticket	X	
Contact third-party service to troubleshoot cases that are triaged as being third-party service issues (e.g. connectivity service provider)		X
Respond to an incident within the service levels that are agreed	X	
Perform a severity analysis from 1-3 (one is the most critical)	X	
Notify the assignee by email severity 1 issues	X	
Provide first-level support or resolution, or both, using scripts	X	
Incident and problem resolution for infrastructure, platform, and core product issues	X	
Communicate & report ticket status on-line or email if separately agreed	X	
Customer approval for fix (auto-approval in 14 days)		X
Close tickets	X	

Change Management	Service Provider	Service User
Keep SaaS software stack at up to date version	X	
Notify users about new features and functionality	X	