TERMS AND CONDITIONS OF USE — CONNECTILOGS

Between **10dencehispahard SLU**, **cdmon** (hereinafter, the **Provider**) and the natural or legal person who contracts, accesses, or uses ConnectiLogs (hereinafter, the **Client** or the **User**, as applicable), the present Terms and Conditions of Use (hereinafter, the **Contract**) are agreed.

This document governs the access, use, provision, limitations, availability, responsibilities, data processing, and all other aspects related to the ConnectiLogs service.

APPLICABLE LAW AND JURISDICTION

This Contract is governed by Spanish law. The parties submit to the Courts and Tribunals of Barcelona, expressly waiving any other jurisdiction that may correspond to them.

PURPOSE OF THE CONTRACT

The purpose of this Contract is to regulate the conditions under which the Provider makes available to the Client the **ConnectiLogs** service, a platform oriented towards the collection, ingestion, storage, normalization, querying, correlation, analysis, and visualization of activity logs, technical events, and security signals associated with the services contracted by the Client.

ConnectiLogs enables, among other functions, the visualization of information through dashboards, the generation of historical data queries, and the retrieval of indicators related to activity, availability, performance, alerts, or detected threats.

The Service is instrumental and supportive in nature. Its purpose is to facilitate the Client's orderly access to technical and operational information, but it does not in itself constitute a system of absolute protection nor a guarantee of the absence of incidents, attacks, errors, information losses, or interruptions.

ACCEPTANCE OF THE CONTRACT

Access to the Service implies full acceptance of this Contract. If the Client does not agree with any of its clauses, they must refrain from accessing or using ConnectiLogs.

DEFINITIONS

For the purposes of this Contract, the following terms shall have the meanings set out below:

Service: the ConnectiLogs platform, including its functionalities, interfaces, APIs, dashboards, modules, developments, integrations, documentation, and updates.

Client: natural or legal person who contracts the Service or for whom the Service is provided.

User: person who accesses the Service with valid credentials, whether on their behalf or on behalf of the Client.

Data: all information processed, queried, stored, or visualized through ConnectiLogs.

Logs: technical, activity, event, or security records generated by systems, applications, accounts, services, infrastructure, or user actions.

Data source: the specific origin from which logs or events are obtained.

Dashboard: panel or view for graphical or tabular representation of data.

Beta phase: period during which the Service is undergoing testing, validation, evolution, or pre-production and in which certain functionalities may not be stable or may change without prior notice.

Incident: any interruption, error, degradation, inconsistency, visualization failure, temporary loss of availability, or unexpected behavior of the Service.

Personal data: any information relating to an identified or identifiable natural person.

Processing: any operation performed on personal data, such as collection, recording, organization, storage, querying, retrieval, communication, or deletion.

DETAILED DESCRIPTION OF THE SERVICE

ConnectiLogs is designed to provide the Client with a centralized view of activity and technical events originating from their services contracted with the Provider and, where applicable, from other compatible sources that are expressly enabled.

The Service may include, depending on configuration, contracted plan, and development status, the following capabilities:

- ingestion of logs and events
- normalization and structuring of information from different sources
- indexing and storage for subsequent querying
- querying by filters, time ranges, sources, services, collections, or equivalent criteria
- visualization of queries through different types of charts or tables

The Client acknowledges that the Service is an observability and analysis tool, not a guarantee of results. The fact that an event does not appear in ConnectiLogs does not necessarily mean that it did not occur. Likewise, the presence of an event, alert, or indicator does not automatically imply that a real threat exists, as false positives, ingestion delays, ingestion incidents, or data enrichment issues may occur.

NATURE OF THE SERVICE AND ABSENCE OF ABSOLUTE GUARANTEE

The Client expressly accepts that ConnectiLogs:

- does not guarantee the detection of all threats, errors, unauthorized access, fraud, configuration failures, or security incidents
- does not replace human supervision, secure system configuration, technical administration, or the adoption of preventive measures by the Client

- does not replace backup tools, monitoring, firewall, antivirus, EDR, SIEM, IDS/IPS, or other security or business continuity solutions
- does not ensure perfect accuracy, perfect integrity, or permanent availability of all information
- must not be considered a sole or exclusive source of truth for critical decisions, given that the service's own logs are always available

The Client accepts that the interpretation of data requires technical judgment. Any decision based on information from ConnectiLogs must be assessed together with other evidence, procedures, and controls belonging to the Client.

BETA PHASE

Beta condition

When the Service, a specific functionality, an integration, an API, a dashboard, or a module is in the beta phase, the Client expressly accepts it as a version in evolution, not fully stabilized, intended for real-world validation, feedback collection, and progressive correction.

Consequences of the beta phase

During the beta phase, the Client accepts that:

- errors, unexpected behavior, partial failures or degradations may exist
- some functions may change, disappear, be renamed or relocated without prior notice
- documentation may be incomplete or out of date in certain areas
- the user experience may differ from future stable versions
- availability may be lower than that of a production service
- data may require technical modifications or reconstructions
- certain functionalities may be activated only for specific clients, plans, or test groups

No strict SLA in beta

Unless expressly agreed otherwise, the beta phase will not be subject to a guaranteed SLA or service level commitments equivalent to those of a production version. The Provider may prioritize stability, correction, and functional validation over continuous availability or speed.

No guarantee of functional continuity

During beta, the Client accepts that a functionality may:

- be modified for technical reasons
- be temporarily disabled
- become a paid functionality
- be replaced by another solution

- not reach production if the Provider decides to discontinue it

Participation and Feedback

By participating in the beta, the Client agrees to actively collaborate by:

- reporting errors, incidents, or unexpected behavior
- providing feedback on functionalities and user experience
- participating in surveys or interviews if requested

The Provider may use the feedback provided to improve the Service without any obligation of compensation. The Client's contributions will not be considered confidential unless expressly agreed otherwise.

Transition from beta to production

The transition from beta to production, if it occurs, may involve:

- interface changes
- changes in limits or quotas, including the removal of features
- changes in retention
- changes in the commercial model
- changes in module availability
- data migration or modification

The Provider will endeavor to minimize the impact but does not guarantee that the transition will be entirely seamless.

Duration of the beta

The duration of the beta phase will be determined unilaterally by the Provider, based on technical maturity, operational stability, volume of incidents, and quality of use observed.

PERMITTED USES AND PROHIBITED USES

Permitted use

The Client may use ConnectiLogs solely for legitimate purposes related to the management, observation, analysis, or auditing of their services or those for which they hold valid authorization.

Prohibited uses

The following are prohibited, by way of example and without limitation:

- using the Service for unlawful, fraudulent, or bad-faith purposes
- accessing third-party data without authorization
- attempting to circumvent authentication, permissions, or technical controls

- exploiting vulnerabilities or conducting penetration testing without permission
- introducing malicious code, harmful scripts, or payloads that compromise the platform
- performing bulk or automated queries that degrade the Service
- reselling, sublicensing, or exploiting the Service without authorization
- copying, decompiling, modifying, or reverse engineering the software, except where expressly permitted by law

The Provider may adopt technical and contractual measures to prevent such uses.

CLIENT OBLIGATIONS

The Client undertakes to:

- keep and protect their credentials to prevent unauthorized access
- restrict access to authorized personnel only
- report security incidents or unauthorized access
- use the Service in accordance with the law, applicable regulations, and this Contract
- not rely exclusively on ConnectiLogs for critical decisions without additional validation
- maintain their own backup copies where appropriate
- fulfil their information, consent, transparency, or legitimization obligations when the data processed includes personal data or third-party data

The Client shall be solely responsible for the consequences arising from misconfiguration, lack of supervision, or incorrect use of the information obtained.

PROVIDER OBLIGATIONS

The Provider undertakes to:

- Provide the Service with professional diligence.
- Maintain the platform operational within the technical possibilities of a beta-phase environment.
- Communicate planned interruptions where reasonably possible.

The Provider does not guarantee:

- continuous or error-free availability
- that the Service will meet the Client's specific requirements
- accuracy, integrity, or timeliness of the data displayed

The Provider may:

- introduce improvements or updates

- correct errors
- modify performance or architecture
- restrict access for security reasons
- temporarily suspend the Service for maintenance, migration, or incident resolution

The Provider does not assume an obligation of result unless expressly established in writing.

ACCOUNT AND CREDENTIALS

Access to the Service does not require new credentials or users beyond those of the Control Panel; it is an additional service as a **cdmon** client. The Client is responsible for:

- Maintaining the confidentiality of their Control Panel credentials.
- Immediately notifying any unauthorized access.
- Ensuring that only authorized users have access.
- Providing truthful and up-to-date information.

The Provider may suspend or cancel accounts that contain false information or that breach these terms.

AVAILABILITY, MAINTENANCE, AND CONSISTENCY

Availability: Unless a specific SLA is agreed, the Service will be provided on a best-efforts basis and may experience interruptions, slowdowns, maintenance windows, or temporary unavailability.

Scheduled maintenance: The Provider may carry out corrective, preventive, evolutionary, or security maintenance tasks even without prior notice when technical urgency requires.

Unscheduled maintenance: In the event of a serious incident, the Provider may intervene without prior notice to restore the Service, protect data integrity, or contain security risks.

Contingencies: The Client accepts that there may be ingestion delays, data reprocessing, event queues, temporary duplications, time zone differences, partial gaps, or latencies between the generation of an event and its visualization.

TECHNICAL LIMITATIONS OF THE SERVICE

The Client acknowledges and accepts that the Service may be subject to inherent limitations, including but not limited to:

- data volume limits
- retention limits
- size limits per event or file
- query frequency limits

- concurrency limits
- export limits
- limits by plan or license
- dependency on external sources or third-party integrations
- variability in response times depending on load and query complexity

The Provider may adjust such limitations to preserve the overall stability of the system, prevent abuse, or adapt the Service to new technical requirements.

ACCURACY, INTEGRITY AND INTERPRETATION OF DATA

The Client accepts that the data displayed by ConnectiLogs may be affected by:

- ingestion delays
- loss of connectivity at the source
- configuration errors
- incompatible formats
- incorrectly labeled events
- aggregations and filters that simplify information
- retention and purge policies
- incomplete synchronizations
- alterations beyond the Provider's control

Therefore, the Client may not hold the Provider liable for conclusions based exclusively on a partial, aggregated, or delayed visualization of information.

PLATFORM SECURITY

Notwithstanding the foregoing, the Client understands that no system connected to public networks can be considered infallible. Consequently:

- there is no guarantee of invulnerability
- security incidents may occur despite the adoption of reasonable measures
- the Client must maintain their security practices, hardening, and supervision

In the event of suspected abuse or a security event, the Provider may block access, restrict functions, revoke tokens, restart processes, or take other proportionate measures to contain the risk.

The Provider implements technical and organizational measures designed to protect the Service and the data processed, including but not limited to:

- Encryption in transit (TLS) and at rest where applicable

- Access controls based on the principle of least privilege
- Security monitoring and anomaly detection
- Periodic patching and updating of components
- Network and environment segmentation

PROCESSING OF PERSONAL DATA AND PRIVACY

The Client declares that they have a sufficient legal basis to communicate or have processed the data they incorporate into the Service. In particular, they must ensure that the processing of logs, events, or metadata relating to natural persons has adequate legal ground, that the duty of information is fulfilled where required, and that prohibited or unnecessary data are not processed.

The Provider may act, depending on the case, as data a processor or as a data controller regarding certain data, under the data processing agreement entered into for the provision of hosting services.

The Client acknowledges that logs may contain data such as IP addresses, session identifiers, timestamps, access paths, user activity, technical identifiers, security metadata, or equivalent elements that, directly or indirectly, may be linked to a natural person.

The Client shall be responsible for:

- deciding which data they introduce or enable for processing
- informing their users or third parties where required
- responding to rights, claims, or requests arising from their relationship with such data
- fulfilling their obligations regarding storage, minimization, and purpose limitation

DATA STORAGE AND RETENTION

The Service may retain data for the period associated with the contracted plan, the operational limits defined by the Provider or applicable legal obligations.

Upon expiry of said period or upon reaching the storage limit, the Provider may:

- automatically delete old data
- block new uploads
- replace detailed data with aggregated data
- require an upgrade of plan or capacity

The Client accepts that retention is not indefinite and that, once the corresponding period has elapsed, certain data may not be recoverable.

INTELLECTUAL AND INDUSTRIAL PROPERTY

All rights over ConnectiLogs, its code, design, architecture, brand, documentation, screens, data models, components, workflows, algorithms, improvements, and evolutions belong to the Provider.

Unless expressly authorized in writing, the Client may not:

- copy, reproduce, or distribute the Service
- modify it or create derivative works
- decompile, disassemble, or reverse engineer it
- systematically extract data or documentation for the purpose of reproducing the product
- use the Provider's trademarks, logos, or distinctive signs beyond what is permitted

Nothing in this Contract grants the Client any ownership rights over the software or the platform, but only a limited, revocable, and non-exclusive right of use under the agreed conditions.

SUPPORT AND CUSTOMER SERVICE

The scope of support will depend on the contracted plan, the nature of the incident, and the phase of the Service.

Unless specifically agreed otherwise, support may be limited to:

- reasonable operational incidents
- general functional queries for paid plans only—the standard channel will be the published help documentation
- verification of reproducible errors
- assistance with standard use of the Service for paid plans only—the standard channel will be the published help documentation

The following fall outside ordinary support, unless expressly agreed:

- advanced personalized consultancy
- custom developments
- complex forensic analysis
- data recovery outside the retention period
- integration with non-approved third-party systems

The Provider may prioritize tickets based on severity, impact, contracted plan, and resource availability.

MODIFICATIONS TO THE SERVICE AND THE CONTRACT

The Provider reserves the right to modify, update, replace or remove, functionalities of the Service, as well as to adapt this Contract when necessary for legal, technical, security, commercial, or product evolution reasons.

Where changes are substantial, the Provider will endeavor to communicate them through available means. Continued use of the Service after the modifications come into effect will imply acceptance of the same.

If the Client does not accept the changes, they may request cancellation of the Service, without prejudice against the provisions regarding billing, data retention, or export.

TERMINATION, SUSPENSION, AND CANCELLATION

The Provider may suspend or terminate access to the Service, in whole or in part, in the following circumstances:

- breach of this Contract
- non-payment
- fraudulent or abusive use
- serious risk to security or availability
- legal requirement or order from a competent authority
- end of the beta period without service continuity
- discontinuation of the product or any of its functional lines

Termination may result in loss of access to dashboards, APIs, reports, historical data, or associated configurations.

The Client shall be responsible for extracting or exporting the data they wish to retain within the period that the Provider, reasonably and subject to technical capacity, makes available for that purpose.

LIMITATION OF LIABILITY

To the fullest extent permitted by law, the Provider shall not be liable for:

- indirect, incidental, special, or consequential damages
- loss of profits, revenue, contracts, or reputation
- loss of business, opportunity, or clientele
- decisions made by the Client based on data from the Service
- damages arising from the Client's configuration errors
- unavailability caused by third parties, networks, external providers, force majeure, or maintenance

- loss or alteration of data arising from actions or omissions of the Client or third parties not under the Provider's control
- failure to detect a threat, alert, or security event
- The Provider shall not be liable for failures or delays caused by circumstances beyond its reasonable control, including but not limited to: natural disasters, fires, floods, earthquakes, epidemics, acts of terrorism, war, civil unrest, telecommunications failures, power outages, actions by governmental authorities, sabotage, large-scale cyberattacks or any other cause beyond the Provider's reasonable control.

Where applicable law permits the limitation of liability, such liability shall, where applicable, be limited to the amount effectively paid by the Client for the Service during the period immediately prior to the event giving rise to the claim, unless a different limit is established in a particular condition or in applicable mandatory law.

Nothing in this clause shall exclude liability that cannot legally be limited.

INDEMNIFICATION

The Client shall hold the Provider harmless against claims, sanctions, losses, costs, damages, or expenses arising from:

- unlawful or unauthorized use of the Service by the Client or their users
- regulatory non-compliance in data processing by the Client
- introduction of unlawful content or infringement of third-party rights
- breach of this Contract
- misconfiguration, negligence, or lack of due diligence in supervising the Service

This obligation shall include, where applicable, reasonable defense costs, legal advice, and incident management expenses.