HIDORA SA – GENERAL TERMS AND CONDITIONS

Internal Ref.: 001-GC Hidora EN1 — Edition: October 2025
HIDORA SA (CHE-286.910.173) - Avenue des Morgines 12, 1213 Petit-Lancy, Suisse
Website : https://hidora.io/

These General Terms and Conditions ("GTC") govern all services provided by HIDORA SA ("HIDORA") to the Client (a legal entity or natural person acting within the scope of their professional activity), including infrastructure and cloud platform services (IaaS/PaaS), managed services, consulting, project services, maintenance, and related services (collectively, the "Services").

These GTC, the Special Conditions, and the Order(s), quotations, Purchase Orders, SOW/Project(s), and their appendices (collectively, the "Agreement") constitute the entire agreement between the Parties.

Table of Contents

1. KEY DEFINITIONS

Client Access :	Credentials (login, MFA, API keys) enabling administration of the Services.
Administrator:	User designated by the Client with management rights over the Account and Client Access.
AUP :	HIDORA's Acceptable Use Policy (Appendix A).
Affiliate:	Entity controlling, controlled by, or under common control with a Party (control ≥ 50% of voting rights or effective management).
Beta/Preview :	Pre-commercial test features, provided without warranties, which may evolve or be withdrawn.
Business Day :	Monday–Friday (excluding official public holidays at HIDORA's registered office).
Change of Control :	Transaction resulting in a change of control of more than 50% of a Party's share capital or voting rights.
Order :	Signed purchase order/quotation or online validation describing the offer, term, quantities, prices, and specific conditions of the relevant Service.
Account :	Customer space enabling management of the Services and Client Access, created upon formation of the Agreement.
Special Conditions :	Service-specific terms set out in the Order and/or Service description, which supplement and, in the event of conflict, prevail over these GTC.
Content :	Data, code, files, configurations, logs, and metadata provided or generated by the Client via the Services.
Service Credits :	Credits provided for under the SLA in the event of unavailability.
Deliverables :	Specific outputs of a project/managed services/consulting engagement as described in a SOW.
Personal Data :	Any data within the meaning of Swiss law (FADP) and/or the GDPR, processed by HIDORA in its capacity as processor.
Sensitive Data :	Special categories of data within the meaning of Swiss law (in particular Art. 5(c) FADP) and, where applicable, the GDPR, including in particular data relating to health, biometric and genetic data enabling identification of a person, religious, philosophical, political or trade union opinions or activities, social assistance measures, criminal or administrative proceedings and sanctions, as well as any other data that the law qualifies as particularly sensitive.
Environment :	Infrastructure, data centers, software, networks, and technical components operated by HIDORA and its subcontractors.
Incident :	Events affecting the availability, performance, security, or integrity of the Services.

Maintenance Window :	Scheduled time period during which HIDORA may perform maintenance operations that may temporarily affect the Availability of the Services. Applicable Maintenance Windows are published on the Portal/Service description and may be adjusted with reasonable prior notice.
Notice & Action :	Procedure for handling notifications of unlawful content or rights infringements described in **Appendix C**.
Project :	Structured engagement described in a SOW/Project Plan (milestones, Deliverables, acceptance criteria).
Site / Portal :	HIDORA's websites and customer portals (including the ticketing system) used for subscription and support of the Services.
SLA :	HIDORA's service commitments/SLA publications (link indicated in Appendix B).
Sub-processor :	Service provider appointed by HIDORA to process Personal Data on behalf of the Client.
User :	Any person authorized by the Client to use the Services.

2. TECHNICAL DEFINITIONS

SOW (Statement of Work)	Document describing the scope, Deliverables, milestones, acceptance criteria, and specific conditions of a Project or managed services engagement.
IaaS (Infrastructure as a Service)	Provision of virtualized IT infrastructure (servers, storage, network) managed by HIDORA, which the Client administers remotely.
PaaS (Platform as a Service)	Managed application platform enabling the deployment and management of applications without directly managing the underlying resources.
DRaaS (Disaster Recovery as a Service)	Service for business continuity and restoration of critical systems after a disaster, according to the parameters defined in the Order or SOW.
SaaS (Software as a Service)	Application logicielle hébergée par HIDORA et accessible à distance par le Client, selon les modalités contractuelles.
PAYG (Pay-As-You-Go)	Billing model based on actual consumption, without a fixed commitment.
API (Application Programming Interface)	Software interface allowing the Client to interact programmatically with the Services.
Backup as a Service (BaaS)	Managed backup service hosting copies of the Client's data, separate from DRaaS.

3. RULES FOR INTERPRETING DEFINITIONS

3.1 The terms "**including**" or "**in particular**" are to be understood without limitation..

3.2 Headings do not affect interpretation.

3.3 References to a legal text refer to any amended or replaced version.

3.4 Electronic communications are considered as written.

4. CONTRACTUAL HIERARCHY AND GOVERNING LANGUAGE

4.1 **Hierarchy :** In case of a conflict, the order of precedence is as follows: (i) Special Conditions of a Service or SOW/Project, (ii) Order(s), (iii) these GTC, (iv) commercial documents. Lower-ranking documents are interpreted complementarily to higher-ranking ones.

4.2 **Versions and Language :** Unless otherwise specified, the French version prevails. Translations are provided as a courtesy.

4.3 **Document Updates :** Operational appendices (SLA, AUP, Sub-processor register, procedures) may be updated for legal, technical, or security reasons; any substantial change likely to adversely affect the Client's essential rights will be notified with reasonable prior notice and applies only prospectively.

5. FORMATION OF THE AGREEMENT - ACCOUNT AND ORGANIZATION

5.1 The Agreement comes into effect upon the first occurrence of any of the following: (i) creation of an Account and acceptance of the GTC, (ii) signature of an Order/SOW, or (iii) access to or use of the Services.

i. The Client creates an **Account** and designates at least one **Administrator**. The Client remains responsible for all actions carried out via the Client Access, including by its Users, contractors, and persons under its control. The Client must implement strong authentication (MFA) and minimum permissions.

5.2 HIDORA may carry out identity/contact verifications at any time when required for security, fraud/anti-money laundering prevention, sanctions regimes, export control, or compliance purposes.

5.3 The Client's **Affiliates** may use the Services under the same Agreement (if indicated in the Order); the Client remains jointly and severally liable for their actions.

6. DESCRIPTION OF THE SERVICES

6.1 **Cloud IaaS/PaaS:** HIDORA's cloud Environment is primarily operated in Switzerland, with redundancy and scheduled maintenance. The features of the offerings are detailed on the Client Site/Portal and/or in the Order. HIDORA may evolve the Environment (hardware/software upgrades, patching) without materially degrading functionality or security.

6.2 **Projects, Managed Services, and Consulting:** Project/managed services/consulting engagements are executed according to a SOW/Project Plan (milestones, Deliverables, acceptance criteria). Timelines are indicative.

6.3 **Support.** HIDORA provides support via the portal/ticketing system and a helpdesk during published hours, with potential additional support levels depending on the offering.

6.4 **Third-Party and Open-Source Software:** Some Services rely on third-party software or Open-Source components. The Client accepts their license terms; in case of conflict, these licenses prevail for the relevant component. HIDORA provides no third-party warranties beyond those granted by the software publisher.

6.5 **Beta / Preview:** Features in Beta/Preview are provided "as is" without any commitment regarding availability, performance, or reversibility.

6.6 **Planned and Emergency Maintenance:** HIDORA may perform interventions during the published Maintenance Windows. In the event of emergency maintenance (security, stability), HIDORA will act with the best reasonable notice and limit the impact. Maintenance periods within the published Maintenance Windows (or duly notified emergency maintenance) are excluded from the Availability calculation under the SLA.

7. USE OF SERVICES - AUP AND SECURITY

7.1 The Client must at all times comply with the **AUP** (Appendix A): prohibition of illegal or public order–violating activities (including, without limitation: malware, SPAM, infringement of third-party rights and personality rights, fraud, system attacks, bypassing filters, unauthorized resale hosting, etc.).

7.2 HIDORA may suspend or limit a Service in case of a Contract violation, security Incident, threat to the Environment, or request from authorities or credible third parties; HIDORA will inform the Client to a reasonable extent and indicate corrective measures.

7.3 The Client is responsible for **secure configuration** (firewall, IAM, secret rotation, client-side encryption, backups, OS hardening) and ensuring the legality of its Content. HIDORA provides organizational and technical measures in line with industry best practices to protect the Environment.

7.4 **Personality Rights and Unlawful Content.** The Client warrants that its Content does not infringe personality rights (image, voice, sensitive data), copyright/trademark, trade secrets, or criminal law. HIDORA implements a **Notice & Action** mechanism (Appendix C) for third-party claims; in case of obvious risk, HIDORA may temporarily remove or suspend the disputed content.

8. DATA PROTECTION AND CONFIDENTIALITY

8.1 **Roles :** The Client acts as the controller of its **Personal Data**; HIDORA acts as a **processor** within the meaning of the Swiss FADP and, where applicable, the GDPR.

8.2 **DPA :** The provisions of **Appendix D** (DPA/Sub-processing) are an integral part of the Agreement (subject, duration, data types, categories of individuals, instructions, security, confidentiality, assistance, sub-processor register, transfers, reasonable audits/assessments, Incident notification, deletion/return).

8.3 **Location :** Unless otherwise specified, primary hosting is performed in **Switzerland**. Related processing (e.g., anti-DDoS, monitoring, support, backups) may involve subcontractors listed and contractually governed. Transfers outside Switzerland/EAA, if applicable, rely on a recognized mechanism (EU standard contractual clauses + Swiss addendum, or adequacy decision), with supplementary measures.

8.4 **Confidentiality :** Each Party shall protect the other Party's confidential information during the term of the Agreement and for **3 years** after its termination (without limiting trade secrets, which remain protected as long as they are secret). These obligations do not apply to information that is public, lawfully obtained from a third party, or independently developed. Confidentiality unrelated to Personal Data is governed by Appendix E (Confidentiality), which prevails in case of any conflict with this article.

9. BACKUPS, BUSINESS CONTINUITY, AND REVERSIBILITY

9.1 **Backups :** Unless otherwise specified by option/subscription, application-level backups are the Client's responsibility. HIDORA may offer backup/DRaaS solutions under the Special Conditions.

9.2 **Reversibility :** Upon termination, the Client may request the return of its Content in a reasonable standard format; fees may apply. Unless otherwise specified, HIDORA retains the Content for thirty (30) days following expiration or termination to allow the Client to retrieve it, and then permanently deletes it within the following thirty (30) days. The technical procedures for return and deletion are detailed in Article 11 of Appendix D – "Return and Deletion of Data."

10. FEES, INVOICING AND TAXES

10.1 Prices (excluding taxes) are listed on the Order/portal, according to the chosen model (subscription, PAYG, credits, hours/day). Taxes, import/export duties, fees, and bank charges are the responsibility of the Client.

10.2 Unless otherwise specified in the Order or Special Conditions :

a) **Recurring Services:** Recurring Services (hosting, maintenance, support, etc.) are invoiced **in advance** on a monthly, quarterly, or annual basis according to the agreed periodicity.

b) **Project or Consulting Services:** One-time services such as project work, deployment, integration, or consulting may be billed according to one of the following models :

- **Milestone-based :** 50% upon order or project start, and 50% upon delivery or commissioning, unless otherwise indicated in the Order ;
- **Time and Materials :** Based on actual time spent, according to applicable hourly or daily rates, invoiced periodically (typically at the end of the month) ;
- **Prepaid Package ("day bundle") :** Advance payment for the agreed number of days or units, consumed as services are delivered.

c) **Payment Terms :** Invoices are payable net within **30 days of issuance**, unless another deadline is expressly agreed. HIDORA reserves the right to suspend the provision of Services in case of non-payment by the due date.

10.3 **Late Payment :** In case of non-payment for more than 30 days, HIDORA may: (i) suspend the Services after at least ten (10) calendar days' written notice, except in emergencies or if the Environment is at risk, while reserving the right to require payment guarantees, (ii) demand early payment of amounts due, and (iii) apply customary late payment interest and collection fees. No refunds will be made for amounts already paid.

10.4 HIDORA may adjust prices for renewal periods; notice of changes will be communicated via the portal and/or email.

10.5 **Third-Party Products :** The prices and terms of third-party publishers/manufacturers apply and prevail for the relevant component.

11. WARRANTIES

11.1 **Cloud:** The cloud Services are provided "**as is**," subject to the service commitments set out in the applicable **SLA**.

11.2 **Projects / Consulting:** HIDORA provides these services with the care and diligence of an experienced professional and delivers Deliverables in accordance with the SOW at the time of delivery. Warranty period: **60 days** from formal acceptance; reasonable corrections of non-conformities attributable to HIDORA.

11.3 HIDORA **does not guarantee** uninterrupted or error-free operation, nor the complete absence of unauthorized access or third-party attacks; dates and times are indicative.

12. TERM, SUSPENSION, AND TERMINATION

12.1 **Term :** The term is specified in the Order/portal. Expired subscriptions result in automatic suspension, unless renewed.

12.2 **Suspension :** HIDORA may suspend all or part of the Services in case of a serious breach, security risk, fraud, non-payment, request from authorities, or threat to the Environment; suspension does not affect amounts due.

12.3 **Termination for Cause :** If the breach is remediable, HIDORA will notify the corrective actions to be taken within a reasonable period; failing this, HIDORA may terminate the Agreement by operation of law. The Client may terminate in the event of a material breach by HIDORA not remedied within a reasonable period.

12.4 **Change of Contro l:** HIDORA will inform the Client at least thirty (30) days before the effective date of any Change of Control concerning it, to the extent permitted by law. If the Client demonstrates a materially adverse impact on the security, confidentiality, or regulatory compliance of its processing, and HIDORA does not propose a reasonable commercial solution within an appropriate period, the Client may terminate the Agreement, without penalty, within thirty (30) days of notification, with a pro-rata refund of unused prepaid fees.

12.5 **End of Agreement and Data:** Upon expiration or termination, access is suspended; except as required by law, remaining data is permanently deleted after the technical periods indicated (see Appendix D). The Client is solely responsible for retrieving its Content beforehand.

13. INTELLECTUAL PROPERTY AND LICENCES

13.1 **Ownership :** The Client retains all rights to its Content. HIDORA retains all rights to the Environment, its documentation, models, scripts, tools, and know-how, including those developed during the performance of the Agreement.

13.2 **Reciprocal Licenses :** Each Party grants the other, for the duration of the Agreement and worldwide, a non-exclusive, non-transferable license strictly limited to the performance of the Agreement.

13.3 **Third-Party / Open-Source Software :** Third-party and Open-Source components integrated into the Services remain subject to their own licenses, which prevail for the relevant component; HIDORA provides no warranties beyond those granted by the publisher.

13.4 **Restrictions :** Unless otherwise required by mandatory law, the Client shall refrain from reverse engineering, circumventing technical measures, and shall preserve copyright notices.

13.5 **Feedback :** The Client's suggestions and feedback may be freely used by HIDORA to improve the Services, without royalty or obligation, and without disclosure of the Client's Confidential Information.

14. LIABILITY AND CAPS

14.1 Within the limits of mandatory Swiss law, HIDORA's total cumulative liability, for all causes combined, is capped at the greater of: (i) the amount actually paid by the Client for the Service giving rise to the damage during the six (6) months preceding the triggering event, or (ii) CHF 50,000.

14.2 HIDORA is never liable for indirect or consequential damages (loss of profit, business, reputation, unsaved data, expected savings, replacement costs), nor for harm caused by: (i) items not provided by HIDORA, (ii) use contrary to instructions or the AUP, (iii) fault of the Client or its contractors, (iv) force majeure.

14.3 Nothing excludes HIDORA's liability in cases of proven fraud or gross negligence.

14.4 Service Credits provided under the SLA constitute, where applicable, the Client's sole and exclusive remedy for service unavailability.

15. COMPLIANCE, SANCTIONS AND ETHICS

15.1 **General Compliance :** Each Party shall comply with applicable laws (Switzerland and, where applicable, the EU), including data protection (FADP/GDPR), telecommunications, sanctions/export control, anti-corruption, anti-money laundering, competition, intellectual property, and personality rights.

15.2 **Sanctions / Export :** HIDORA may refuse, delay, or suspend a Service if its provision would violate a sanctions or export control regime, or any legal obligation. The Client agrees not to redirect the Services to sanctioned users or jurisdictions.

15.3 **Ethics :** The Parties prohibit any corruption, undue influence, or similar practices, implement preventive measures, and provide an appropriate reporting channel.

15.4 **Regulatory Cooperation :** To the extent permitted by law and security requirements, each Party shall reasonably cooperate with competent authorities and notify the other Party if a compliance requirement impacts the performance of the Agreement.

16. EVIDENCE, LOGGING AND LIMITED AUDITS

16.1 **Evidence Agreement :** HIDORA's system logs, metrics, tickets, timestamps, and technical records are binding between the Parties, subject to contrary evidence provided by the Client.

16.2 **DPA-Related Audits :** With reasonable notice and during business hours, HIDORA allows document reviews related to Appendix D (DPA). No physical data center visits are required, except where mandated by applicable law.

16.3 **Retention :** HIDORA may retain, for as long as necessary, items strictly required for purposes of evidence, security, and compliance.

17. FORCE MAJEURE

17.1 **Principle :** No Party is liable for non-monetary breaches caused by an event reasonably beyond its control (major power outage, data center disaster, large-scale cyberattack, epidemic/pandemic, governmental act, conflict, natural catastrophe).

17.2 **Duties of the Affected Party :** Notify within a reasonable period, implement mitigation measures, and resume performance once the impediment has ceased.

17.3 **Payments :** Monetary obligations that have become due remain payable.

18. ASSIGNMENT AND SUBCONTRACTING

18.1 **Assignment :** No Party may assign the Agreement without the other Party's prior written consent, except: (i) assignment of HIDORA's receivables, or (ii) assignment in the context of a corporate reorganization or business sale (universal transfer); in these cases, notice is sufficient.

18.2 **Subcontracting :** HIDORA may subcontract all or part of the Services, under its responsibility, in accordance with Appendix D (Sub-processor register and data protection requirements).

19. NOTICES

19.1 **Methods : Contractual** notices are validly delivered in **writing** to the postal address of the registered office and/or the email address indicated in the **Account**. **Operational** communications may be sent via the **portal/ticket system**.

19.2 **Receipt:** Unless proven otherwise: (a) an **email** is deemed received on the **Business Day it is sent**; (b) a **registered** letter is deemed received no later than the **third (3rd) Business Day** after dispatch.

19.3 **Commercial References:** Unless the Client objects in writing, HIDORA may mention the **Client's name** and logo as a **reference** (without disclosing Confidential Information). The Client may **unsubscribe** at any time via legal@hidora.io; HIDORA shall comply with the Client's logo usage guidelines.

20. MISCELLANEOUS

20.1 **Independence of the Parties:** No relationship of subordination or general agency exists.

20.2 **Non-Waiver:** A Party's failure to enforce a right does not constitute a waiver.

20.3 **Severability:** The invalidity of any clause does not affect the validity of the others; it shall be replaced by a valid clause that best reflects the Parties' intent.

20.4 **Entire Agreement:** The Agreement supersedes and replaces all prior agreements relating to its subject matter.

21. GOVERNING LAW AND JURISDICTION

21.1 The Agreement is governed by Swiss law, excluding the Vienna Convention (CISG).

21.2 The **exclusive** jurisdiction is in **Geneva**, subject to appeal to the Swiss Federal Supreme Court under applicable law.

October 2025

Appendix A – Acceptable Use Policy (AUP)

1. Purpose and Scope

This Acceptable Use Policy governs all use of the Services by the Client, its Users, subcontractors, and Affiliates.

It complements the General Terms and Conditions and the Special Conditions. Any breach of the AUP constitutes a violation of the Agreement.

2. General Principles

The Client uses the Services legally, securely, and responsibly. It refrains from any action that could harm the Environment operated by HIDORA, other clients, or third parties.

The Client continuously respects personality rights, intellectual property, and applicable data protection laws.

3. Illegal or Harmful Content

The Client must not host, transmit, publish, or make available content that infringes copyrights, trade secrets, or personality rights, including image, voice, or sensitive data of third parties.

Defamatory, hateful, discriminatory, violent, terrorist, harassing, or threatening content is also prohibited, as is any child sexual abuse material or content inciting criminal activity.

The Client must not engage in phishing, fraud, identity theft, or any other deceptive practices.

More broadly, it ensures that all of its activities remain compliant with applicable laws, including those relating to telecommunications, gambling, regulated goods and services, and advertising.

4. Prohibited Technical Activities

The Client must not propagate malware (including ransomware, backdoors, or botnets), conduct attacks or attempted attacks on systems (e.g., mass scanning, brute force, DDoS/DoS, amplification attacks, injections, XSS, SSRF, privilege escalation, traffic interception or hijacking), or bypass or neutralize security mechanisms such as WAF, IDS/IPS, access control lists, or quotas.

The Client must not operate open relays, open resolvers, or unsecured anonymous proxies.

The Client must not resell the Services without authorization or set up “bulletproof” hosting.

Any use intended to disrupt the availability or performance of the Environment, Services, or third parties is prohibited.

5. Security and Identity Management

Under a shared responsibility model, HIDORA implements technical and organizational measures to protect the Environment.

The Client must implement multi-factor authentication for administrative profiles, apply least-privilege principles, keep systems and applications up to date, harden exposed systems and services, protect secrets (keys, tokens, certificates) and rotate them regularly.

The Client configures firewalls, segments networks, and filters incoming and outgoing traffic.

Where backups are not included in the offering, the Client implements its own backups and regularly tests restoration. It monitors resource usage and responds promptly to any alerts or incidents.

6. Email and Commercial Communications

The Client must not conduct illegal marketing activities or engage in SPAM-like practices. It obtains valid and traceable consent (e.g., double opt-in when appropriate), clearly identifies itself as the sender, provides an immediate unsubscribe mechanism, and retains proof of consent.

The Client implements SPF, DKIM, and DMARC appropriately and does not purchase address lists.

The Services must not be used as a mass routing platform without HIDORA's prior written consent.

7. Resources, Performance, and Fair Use

The Client respects published quotas, API limits, quality of service parameters, and fair-use rules. It does not intentionally overconsume or flood traffic in a way that degrades the Services.

HIDORA may apply proportionate and reasonable measures, such as rate limiting, filtering, network isolation, address blocking, or security patches, to preserve the integrity and availability of the Environment.

8. Personal Data and Personality Rights

The Client ensures it has a legal basis for any Personal Data processing carried out via the Services, informs data subjects in accordance with applicable law, and complies with the FADP and, where applicable, the GDPR.

Content affecting reputation, image, voice, or sensitive data is processed lawfully, necessary, and proportionately.

In the event of a credible allegation of infringement of personality or intellectual property rights, the Notice & Action procedure in Appendix C applies.

9. AI/ML and Digital Assets

When the Client trains, evaluates, or uses AI models via the Services, it strictly complies with applicable law and refrains from processing Personal Data without a proper legal basis. It does not collect or scrape third-party data en masse without rights.

Activities involving digital assets, including mining, staking, or running masternodes, are permitted only with HIDORA's prior written consent and in compliance with technical, electrical, thermal, sanctions, and export control requirements.

10. Security Testing and Responsible Disclosure

Any intrusion testing or active scanning initiated by the Client requires HIDORA's prior written consent specifying scope, time slots, and source addresses.

HIDORA supports responsible vulnerability disclosure: reports must be confidential, exploited only to a proportionate proof-of-concept, and must not access, alter, or exfiltrate third-party data.

11. Abuse Reporting and Cooperation

Abuse, Incidents, or suspected misuse must be reported to abuse@hidora.io or via the support portal with evidence. The Client cooperates in good faith with HIDORA to contain Incidents, investigate, revoke compromised secrets, deploy patches, and, if applicable, perform required legal notifications.

HIDORA informs the Client of authority requests where permitted by law and compatible with Environment security.

12. Enforcement and Remedial Measures

In case of actual or suspected AUP violations, HIDORA may take proportionate measures without delay to protect the Environment and third parties, including isolating resources, blocking traffic, or limiting/suspending access to features.

HIDORA informs the Client and, where relevant, proposes a remediation plan. In case of serious or repeated violations, HIDORA may suspend or terminate the Services under the General Terms. When the violation is attributable to the Client, HIDORA may charge reasonable investigation and mitigation costs..

13. Retention and Deletion

HIDORA may retain logs and records necessary for security, billing, legal compliance, and Incident investigation, according to its retention policies.

Data deletion and, if applicable, return are carried out in accordance with the General Terms and Appendix D.

14. AUP Updates

HIDORA may update this AUP for legitimate legal, security, or technical reasons. Changes are published and, where applicable, notified to the Client.

Continued use of the Services constitutes acceptance of the updated version.

15. Contact

Questions regarding this AUP may be sent to legal@hidora.io or via the support portal.

October 2025

Appendix B – Service Level Agreement (SLA)

1. Purpose and Scope

This SLA defines the service commitments applicable to HIDORA's cloud offerings (IaaS/PaaS) used in production. It covers the definition and calculation of availability, maintenance windows, measurement methods and evidence conventions, exclusions, service credits, the claim procedure, as well as support and response time commitments. Beta/Preview, test, or evaluation environments are not covered by this SLA.

2. Definition of Availability and Measurement Method

"Availability" means the percentage of time, over a calendar month, during which the control interfaces and critical components of a Service are operational and accept requests in accordance with published specifications. Measurement is performed by HIDORA using internal probes and metrics, excluding the items in Article 6 and outside announced maintenance windows.

An Incident is considered closed when the Service's nominal capacity is restored and validated by monitoring systems. Logs, metrics, and technical records collected by HIDORA serve as the binding evidence, unless contrary evidence is provided by the Client through consistent technical data.

3. Availability Commitments

HIDORA aims to provide high availability appropriate to the nature of each Service. Target objectives are published on the Service sheet and may vary depending on the architecture deployed by the Client.

When a multi-zone or multi-node configuration is implemented according to documented best practices, actual availability also depends on the Client's application design, fault tolerance, and failover management.

4. Published Targets

Availability targets and the service credit schedule applicable to each offering are published on the Service sheet.

In case of conflict with a contractual appendix, the appendix prevails for the current period.

Any change is notified at least thirty (30) days in advance and applies only to future periods.

5. Maintenance Windows

Planned maintenance operations occur during the Maintenance Windows published on the Portal/Service sheet. HIDORA provides prior notice for significant interventions. Emergency maintenance may occur outside planned windows when necessary to address a vulnerability or operational risk; HIDORA then provides the best reasonable notice and a post-intervention report.

Where possible, operations are designed to be non-impactful or minimally impactful. Emergency interventions needed to fix critical vulnerabilities may be performed without prior notice if the security or integrity of the Environment requires it.

6. Exclusions

The following are not counted as downtime: (a) announced maintenance windows, (b) unavailability caused by elements not provided by HIDORA or configurations contrary to recommendations, (c) Incidents resulting from voluntary overconsumption, prohibited use under the AUP, or actions by the Client/third parties acting on its behalf, (d) force majeure, (e) limitations of Beta/Preview versions, and (f) interruptions due to legal obligations, authority orders, or security measures required to protect the Environment.

7. Service Credits and Procedure

If an availability target for a Service is not met during a calendar month, the Client may request a service credit corresponding to a percentage of that Service's monthly fees, according to the schedule published with the Service sheet.

Credits are not refunds and cannot be exchanged for cash; they apply to future invoices and, where applicable, constitute the Client's sole remedy for unavailability covered by this SLA, without prejudice to the liability limitations in the General Terms. Credit requests must be submitted via ticket through the client portal within thirty (30) days following the end of the relevant month, describing the Incident, dates and times, impact, and affected resources. HIDORA reviews the request against its logs and issues a reasoned decision. Requests submitted outside the deadline or procedure are deemed abandoned.

8. Customer Support and Response Commitment

Customer support is provided on business days, Monday to Friday, from 08:00 to 18:00 CET, via the support portal (support.hidora.io) or email (support@hidora.io).

The infrastructure is monitored and on-call 24/7 to ensure operational continuity.

Response times depend on Incident severity:

- **High severity** – maximum response time of one hour

  Covers system crashes or suspension, data corruption or loss, or unavailability of critical HIDORA functions without a workaround ;

- **Normal severity** – maximum response time of two hours

  Covers system restarts or recoveries after errors or failures, severe performance degradation, or restricted operation ;

- **Low severity** - maximum response time of eight hours

  Covers issues with a workaround, minimal performance degradation, or functional/configuration assistance requests.

These response times are operational objectives; unless otherwise stated in Special Conditions, they do not constitute a guarantee of repair within a specific timeframe.

9. SLA Modifications

HIDORA may adapt this SLA for legal, technical, or operational reasons.

Changes are published and, where applicable, notified to the Client with reasonable notice.

Any modification affecting Availability targets or the credit schedule is notified at least thirty (30) days before implementation and applies only to future service periods.

Continued use of the Services after the changes take effect constitutes acceptance. Changes do not retroactively affect credits already earned for previous periods.

10. Precedence

In case of conflict between this SLA and Special Conditions for a Service, the Special Conditions prevail for that Service.

In case of conflict with the General Terms, the SLA is interpreted complementarily; liability limitations and other general clauses of the General Terms remain applicable.

October 2025

Appendix C – “Notice & Action” Procedure (Infringements of Rights and Personality)

1. Purpose and Scope

This Appendix describes the notification and action procedure implemented by HIDORA to handle, diligently and proportionately, allegations of third-party rights infringements committed through the Services.

It applies particularly to violations of personality rights (including image, voice, and sensitive data), defamation, copyright and trademark infringements, trade secret breaches, and, more generally, content clearly unlawful under Swiss law.

2. Guiding Principles

HIDORA acts as a hosting provider and intervenes without prejudging the merits of a dispute when the situation requires, based on credible information.

Intervention aims to prevent serious harm or to comply with a legal obligation or injunction.

HIDORA seeks a balance between freedom of expression, protection of personality, and intellectual property rights, respecting the principle of proportionality.

3. Valid Notification

Une notification est réputée vaA notification is considered valid when it clearly and completely includes: (a) precise identification of the disputed content or resource (URL, instance ID, relevant timestamp); (b) description of the allegedly infringed rights and the legal basis invoked; (c) relevant facts and, if possible, supporting evidence (screenshots, hash, header excerpts, WHOIS, etc.); (d) the requester’s contact details (name, role, address, email, phone) and, if applicable, proof of authority to represent; (e) a good faith statement certifying the accuracy of the information and the existence of a legally protected right or interest.

Notifications must be sent to **legal@hidora.io** or via the designated form/portal.

4. Acknowledgment and Assessment

HIDORA promptly acknowledges receipt, logs the notification, and performs a preliminary plausibility assessment, supplemented, if necessary, by requests for additional information from the requester.

If the notification is incomplete, HIDORA asks the requester to complete it within a reasonable timeframe. If not completed, the request may be closed without action, without prejudice to submitting a properly completed notification later.

5. Provisional Measures

When the alleged infringement appears manifest, or when an injunction from a competent authority is communicated, HIDORA may implement, temporarily and proportionately, one or more of the following measures: (i) targeted removal or blocking of content; (ii) limited suspension of a service, Account, or feature; (iii) access filtering or restriction by IP range, region, or protocol; (iv) request corrective action from the Client within a set timeframe.

HIDORA notifies the affected Client when legally permissible and compatible with security, inviting them to provide observations.

6. Counter-Notification and Restoration

The Client may contest the measures by submitting a reasoned counter-notification within the specified period, accompanied by supporting evidence (e.g., authorizations, licenses, legal exceptions, factual truth, overriding public interest).

HIDORA reassesses the situation in light of the conflicting information and may, if appropriate, restore content or adjust measures.

In the case of a persistent dispute on legal or factual issues, HIDORA may invite the parties to approach the competent authority; HIDORA complies with any enforceable decision or injunction.

7. Evidence Retention and Cooperation

HIDORA may retain, for the necessary period, technical logs, metadata, and strictly required elements for evidence, security, and compliance purposes.

Upon a legally valid request, HIDORA cooperates with competent authorities in investigations or proceedings, as permitted by applicable law and the security of the Environment.

Requests for access or disclosure must be sufficiently precise and legally grounded.

8. Repeated Violations and Graduated Measures

IIn case of **repeated** or particularly serious violations, HIDORA may apply graduated measures ranging from warning to temporary suspension or even termination of the Service in accordance with the General Terms.

HIDORA may also impose remediation, training, or targeted audit obligations when relevant to prevent recurrence.

9. Abuse of Procedure

Notifications that are manifestly unfounded, abusive, or made in bad faith may be rejected.

HIDORA reserves the right to request guarantees or charge reasonable costs for analysis and handling when the burden clearly exceeds what can be expected of a diligent host, without prejudice to possible liability actions against the author of an abusive notification.

10. Transparency and Updates

HIDORA may publish aggregated and anonymized information on the volume and type of notifications handled (transparency report), subject to confidentiality and security requirements.

This Appendix may be updated for legal, technical, or operational reasons. Updates are published and, where applicable, notified to the Client. Continued use of the Services constitutes acceptance.

11. Governing Law

The procedure described above is governed by Swiss law. This is without prejudice to remedies available before competent authorities or courts under the forum designated in the Contract.

October 2025

Appendix D – Data Processing Agreement (DPA – Subcontracting)

1. Purpose, Parties, and Duration

This Appendix governs, under the Swiss Federal Act on Data Protection (rev. LPD) and, where applicable, the GDPR, the processing of Personal Data carried out by HIDORA ("Processor") on behalf of the Client ("Controller") in connection with the provision of the Services.

It applies for the duration of the Contract and until the obligations of data return or deletion described below have been fulfilled.

2. Categories of Data, Data Subjects, and Purposes

Unless otherwise stated in specific terms and conditions, the Services may allow the Client, under its sole responsibility, to host, store, back up, or transmit identification and contact data, technical identifiers, logs and metadata, as well as application content that it uploads to the Services, including, according to its own use, data related to its end customers, employees, service providers, and prospects.

It is expressly agreed, however, that depending on the nature of the subscribed Service, HIDORA may be limited to providing infrastructure, a platform, computing, storage, or backup capabilities, without accessing the content of the data or reviewing it, and without performing any processing on such data other than what is strictly necessary, automatically or incidentally, for the technical provision of the Service, security, continuity, backup, maintenance, client-requested support, or compliance with a legal obligation. In particular, the mere fact that data is hosted on HIDORA's infrastructure does not, by itself, imply that HIDORA consults, uses, or materially processes such data beyond what is required to perform the Contract.

Where the Service in question involves active intervention by HIDORA on the data, such as in support, maintenance, migration, restoration, technical analysis, application monitoring, or any other service requiring access to content, HIDORA acts exclusively on documented instructions from the Client, within the contractually agreed limits, and only to the extent strictly necessary to perform the Contract.

Sensitive Data. The Client is informed that HIDORA's Services are not specifically intended for the processing of data that is particularly sensitive under the Swiss Data Protection Act (LPD) or, where applicable, special categories of data under the GDPR (e.g., health data, biometric or genetic data, political or religious opinions, data relating to legal proceedings or sanctions). If, according to its own practices, the Client nevertheless decides to host or process such data using the Services, it is responsible for ensuring the lawfulness of such processing, informing the data subjects, and implementing appropriate technical and organizational measures. Unless expressly agreed otherwise, HIDORA assumes no additional specific obligations related to the sensitive nature of the data beyond the security measures generally applicable to the subscribed Services.

The purposes of any operations that may be performed by HIDORA are limited, depending on the Service concerned, to the provision and technical operation of the Services, including hosting, storage, backup, technical transmission, monitoring, securing, maintenance, support, restoration, service continuity, billing, and, in aggregated or non-identifiable form, technical improvement of the Services, only to the extent strictly necessary for the performance of the Contract.

3. Roles, Instructions, and Compliance

The Client determines the essential purposes and means of processing and remains solely responsible for the lawfulness of processing conducted via the Services.

HIDORA acts only on documented instructions from the Client, including for transfers to third countries, except in case of mandatory legal obligations; in such cases, HIDORA informs the Client prior to processing, as permitted by applicable law.

The Client commits to issuing only instructions compliant with applicable law and to promptly inform HIDORA of any changes potentially affecting compliance.

4. Confidentiality and Authorized Personnel

HIDORA ensures that persons authorized to process Personal Data are bound by confidentiality obligations and receive appropriate training.

Access rights are granted based on a need-to-know principle and are periodically reviewed. All access is logged proportionally to the risks.

5. Technical and Organizational Measures (TOMs)

HIDORA implements appropriate technical and organizational measures according to the risk to ensure an adequate level of security.

Measures include information security governance, identity and access management (MFA when applicable, role separation, logging), network protection (segmentation, filtering, monitoring), data protection (encryption at rest and in transit where relevant, key lifecycle management), vulnerability and change management (inventory, patching, reviews), backup and periodic restoration tests, continuity and disaster recovery (documented plans, exercises), endpoint and server management (hardening, updates), and operational hygiene (procedures, reviews, awareness).

HIDORA makes an up-to-date description of its TOMs available upon reasonable request.

6. Subsequent Processors

HIDORA may engage Subprocessors to perform all or part of the processing.

HIDORA imposes equivalent data protection obligations on these Subprocessors and remains liable to the Client for their acts and omissions.

HIDORA maintains a list of relevant Subprocessors and notifies the Client of any material changes with reasonable notice. The Client may object for serious data protection reasons; the Parties will seek a reasonable commercial solution in good faith. If unsuccessful, the Client may terminate the relevant Service part without penalty from the effective date of the change.

7. Location and International Transfers

Primary hosting is conducted in Switzerland, unless otherwise agreed.

Where ancillary processing involves transfer to a country without an applicable adequacy decision, HIDORA implements a recognized mechanism (e.g., EU standard contractual clauses 2021 including Swiss addendum, or equivalent instruments) and, if applicable, supplementary measures per competent authority recommendations.

HIDORA will review in good faith any Client request for additional information regarding transfer risk assessment.

8. Assistance to the Controller and Data Subject Rights

HIDORA reasonably assists the Client, within its technical and organizational capabilities, to respond to data subject rights requests, conduct impact assessments, and notify authorities or data subjects when required.

HIDORA forwards to the Client any request received directly from a data subject without responding, unless instructed otherwise or legally required.

9. Data Breaches and Incident Management

HIDORA notifies the Client without undue delay after becoming aware of an Incident affecting Personal Data processed on behalf of the Client.

The notification contains available information at that stage and is updated as necessary, including the nature of the Incident, approximate categories and volumes of data and data subjects affected, likely consequences, measures taken or proposed to mitigate the breach, and relevant contact points.

The Client remains responsible for legal evaluation of the breach and notifications to authorities or data subjects, in accordance with applicable law. HIDORA will not perform external notifications without the Client's prior written instructions, except as legally required.

HIDORA documents all data breaches, including facts, effects, and corrective actions, to demonstrate compliance with data protection obligations.

10. Processor Assistance

HIDORA assists the Client, to the extent reasonably possible given the nature of processing and information available, to comply with data security obligations, data protection impact assessments, and prior consultations with supervisory authorities.

HIDORA provides necessary information to the Client to demonstrate compliance under this Agreement and allows reasonable audits, in accordance with the General Terms.

Any assistance exceeding minimal legal obligations may be subject to additional remuneration at the applicable hourly rate.

11. Data Return and Deletion

Upon Contract expiration or termination, HIDORA shall, per the Client's written instructions, either return or securely delete all Personal Data processed on behalf of the Client, except where legal obligations require retention.

Deletion is carried out securely according to current technical standards, ensuring data cannot be reconstructed. HIDORA confirms completion in writing.

Absent specific Client instructions within thirty (30) days after Contract end, HIDORA is authorized to delete data; deletion occurs no later than thirty (30) days thereafter (except for legal retention obligations). Upon prior Client request, return in a reasonable standard format may be arranged; fees may apply.

12. International Data Transfers

Primary hosting is in Switzerland.

Ancillary processing (e.g., anti-DDoS, monitoring, support, backups) may involve Subprocessors. All transfers outside Switzerland/EU/EEA rely on a recognized mechanism (e.g., EU standard contractual clauses with Swiss addendum or adequacy decision) with appropriate supplementary measures.

HIDORA ensures all involved Subprocessors provide protection equivalent to Swiss and EU law..

13. Governing Law and Jurisdiction

This Agreement is governed by Swiss law, excluding its conflict-of-law rules and any international conventions on the sale of goods.

Any dispute regarding validity, interpretation, or performance of this Agreement falls under the exclusive jurisdiction of the courts at HIDORA SA's registered office, subject to mandatory legal remedies.

October 2025

Appendix E – Confidentiality (NDA Framework)

1. Purpose and Scope

This Appendix governs confidentiality for information other than Personal Data (which remains subject to Appendix D – Data Processing Agreement). It applies to all confidential information exchanged between the Parties in connection with the Contract, including pre-contractual and immediate post-contractual exchanges.

2. Definitions

Confidential Information means any non-public information, in any form (written, oral, visual, code, configurations, diagrams, metrics, logs, know-how, business plans, pricing), marked or reasonably identifiable as confidential, disclosed by one Party (the "Discloser") to the other (the "Recipient").

Information is not considered confidential if it: becomes public without fault of the Recipient; is received legitimately from a third party not bound to confidentiality; is independently developed; or was already known to the Recipient without a confidentiality obligation.

3. Permitted Use

The Recipient may use Confidential Information only to perform the Contract and must refrain from any other direct or indirect exploitation. Any copy or extraction must remain strictly necessary for this purpose.

4. Restricted Access

The Recipient limits access to only those who need to know (personnel, agents, subcontractors, advisors – collectively "Authorized Persons"), who are bound by equivalent confidentiality obligations. The Recipient remains responsible for the actions of these persons.

5. Protective Measures

The Recipient implements appropriate technical and organizational measures to protect the confidentiality, integrity, and availability of information, at least equivalent to those applied to its own sensitive information, in line with industry best practices. Logs, metrics, and technical records may be retained for proof and security purposes per the Contract.

6. Mandatory Disclosures

If disclosure is required by law, injunction, or competent authority, the Recipient may disclose only the strictly necessary portion, after prior notice to the Discloser (if legally permitted) to allow protective measures (e.g., seals, closed sessions, protective orders).

7. Confidentiality Incidents

The Recipient promptly informs the Discloser of any unauthorized access to Confidential Information known to it and cooperates in good faith to mitigate its effects. If the incident involves Personal Data, the obligations and timelines of AppendixD apply.

8. Return and Destruction

À Upon the Discloser's request or at the end of the Contract, the Recipient returns or destroys the Confidential Information (including copies, notes, derivatives), subject to: standard technical backups and retention; legal retention obligations; and items kept for proof, security, and compliance purposes.

The Recipient confirms destruction upon reasonable requests.

9. Residual Knowledge

General skills, ideas, or know-how retained in memory alone by the Recipient's personnel are not restricted, provided no Confidential Information is disclosed and intellectual property rights are not violated.

10. Duration

Unless a stricter NDA is in place, the obligations of this Appendix survive indefinitely as long as the information remains non-public; trade secrets remain protected without limitation.

11. Precedence and Interaction

(a) A project-specific NDA prevails over this Appendix for that project or subject matter.

(b) This Appendix E prevails over the General Terms regarding confidentiality of information other than Personal Data (which falls under Appendix D).

12. Governing Law

This Appendix is governed by Swiss law; the exclusive forum is Geneva, in accordance with the "Governing Law and Jurisdiction" article of the Contract.

October 2025