Valid from	08/15/2026	Jurisdiction	Italy / EU

Acceptable Use Policy

IndustryUX Platform — Annex incorporated by reference into the Master Subscription and Licence Terms

Codice documento	IUX-EN-35
Versione	1.2
Data	2026-08-11
Set	ANNEXES (EN)
Destinatari	All Customers, Authorised Users and account holders (B2B and B2C)
Lingua	English (authoritative)
Classificazione	Policy

Art. 1 — Purpose and subject matter

1.1 Purpose

This Acceptable Use Policy (the "Policy") defines the perimeter of permitted use of the IndustryUX platform, of the Applications and of every service, interface and deliverable made available by DEVIBRAIN S.R.L., a company incorporated under Italian law, with registered office at Via Coghetti 6, 24128 Bergamo (BG), Italy, VAT and tax code IT04507220160, certified electronic mail devibrain@pec.it (the "Provider (DevIBrain)", referred to in the remainder of this Policy as the "Provider"). Its purpose is to protect the integrity, security, availability and lawfulness of a shared, multi-tenant industrial platform, the rights of the Provider and of third parties, and the quality of the service delivered to all customers.

1.2 Nature of this Policy

This Policy is a standalone document, incorporated by reference into the contractual documentation and updated in accordance with Article 29 without the need to renegotiate the Agreement. It states operating rules of conduct; it does not create commercial entitlements, does not modify the fees and does not extend or reduce the licence rights granted under the Agreement.

1.3 Scope of application

This Policy applies to every commercial channel and to every deployment model of the platform, including self-service purchases in the online shop, Trial and Base plans, the Business plan, Enterprise Online, dedicated virtual private server deployments and On-Premise installations, in the latter case in respect of the licensing, activation, update, support and remote verification components that continue to interact with the Provider's infrastructure.

Art. 2 — Persons bound and definitions

2.1 Persons bound

This Policy binds the Customer and every person who accesses or uses the platform through the Customer's account or entitlements, including Authorised Users, administrators, employees, contractors, agents, group companies of the Customer, and any automated process, integration, script or third-party application operating with the Customer's credentials or keys. The Customer shall procure that all such persons comply with this Policy and shall remain liable towards the Provider for their conduct, within the limits of Article 13.

2.2 Definitions

Terms defined in the Master Subscription and Licence Terms (IUX-EN-01) have the same meaning in this Policy. In addition:

Term	Meaning in this Policy
Agreement	the Master Subscription and Licence Terms, the applicable channel schedule (the Shop Schedule, Schedule A, IUX-EN-10, or the Enterprise Schedule, Schedule B, IUX-EN-20), the Order and all annexes, including this Policy
Applications	the platform applications licensed to the Customer, as identified in the Master Subscription and Licence Terms and in the Order
Authorised User	the individual authorised by the Customer to access the platform through individual credentials
Customer Data	has the meaning given in the Master Subscription and Licence Terms and comprises all data, files, documents, drawings, three-dimensional models, images, texts, configurations, recipes, code and other materials uploaded to, stored on, processed by or generated through the platform by the Customer or by an Authorised User

Term	Meaning in this Policy
Entitlement	the contractual right of use granted to the Customer under the Agreement, as defined in the Master Subscription and Licence Terms, including the permitted number of Authorised Users, activations, Designated Assets and Generated Applications and the metered allowances
Generated Application	each output produced through the Applications and bound to a Designated Asset, including the web controls exported for supervisory and human-machine-interface runtimes
Grant	the technical representation of an Entitlement, as defined in the Master Subscription and Licence Terms: the cryptographically signed record (ECDSA P-256) issued by the Provider's Console and recorded in the License Manager, which evidences the rights of use, the metered allowances and the bound Designated Asset
Serious Abuse	any conduct listed in Article 23
Tokens	the prepaid unit of consumption measuring the use of metered features, allocated to a Designated Asset and permanently bound to it, usable for any consumption relating to that same Designated Asset and not transferable to another one; in the self-service plans governed by the Shop Schedule (Schedule A, IUX-EN-10) the corresponding units are credited to the wallet of the account as Prepaid Credits, are not allocated to any Designated Asset and follow the regime of that Schedule

Art. 3 — Relationship with the Agreement and order of precedence

3.1 Incorporation by reference

This Policy forms an integral and substantial part of the Agreement. Acceptance of the Agreement, in whatever form provided for the relevant channel, constitutes acceptance of this Policy. The version in force at the time of each act of use applies to that act.

3.2 Order of precedence

In the event of conflict between the documents making up the Agreement, the order of precedence is the one set out in Article 2.3 of the Master Subscription and Licence Terms (IUX-EN-01), which applies as such and is not restated here. For the purposes of that order this Policy ranks among the other annexes.

3.3 Breach of this Policy

Breach of this Policy is a breach of the Agreement. In accordance with Article 8.4 of the Master Subscription and Licence Terms, breaches of the rules of use are dealt with through the graduated procedure set out in Articles 22 to 24 of this Policy, and the remedies for serious breach provided for in those Terms, including termination pursuant to Article 1456 of the Italian Civil Code, are reserved to the cases of Serious Abuse. Depending on its gravity the breach accordingly entitles the Provider to apply those graduated measures and, in the cases of Serious Abuse, to suspend the service with immediate effect and to terminate the Agreement, without prejudice to compensation for damage and to any other remedy available at law.

Art. 4 — General principle of lawful and professional use

The Customer shall use the platform in compliance with the law, with this Policy, with the Agreement and with the technical documentation, for its own internal professional purposes, in a manner that does not harm the Provider, other customers, Authorised Users or third parties. The platform is a professional industrial engineering tool: it is not intended for consumers' personal or domestic use beyond the evaluation and learning use expressly permitted for the Trial and Base plans, and it is not intended for use by minors.

Art. 5 — Prohibited uses: unlawful activities

The Customer and its Authorised Users shall not use the platform, directly or indirectly, in order to:

• commit, prepare, facilitate or conceal any criminal offence or any other unlawful act, including fraud, money laundering, corruption, market abuse, tax offences and computer crimes;

• infringe applicable industrial, environmental, product-safety, labour or workplace-surveillance legislation, including any covert monitoring of employees prohibited by Italian Law 300/1970 and by data protection law;

• carry out activities subject to authorisation without holding the required authorisation;

• breach export control, embargo or sanctions rules, as further specified in Article 20;

• infringe the rights of third parties, including personality rights, confidentiality, trade secrets and intellectual property rights.

Art. 6 — Prohibited uses: intellectual property and third-party rights

The Customer and its Authorised Users shall not:

• copy, reproduce, distribute, sell, lease, lend, sublicense, publish or otherwise make the platform, the Applications or their components available to third parties outside the limits of the Agreement;

• remove, alter, obscure or falsify trademarks, logos, copyright notices, licence identifiers, version markings or provenance information affixed by the Provider to the platform or to the Generated Applications;

• upload, process or distribute through the platform any material infringing the copyright, patent, trademark, design, trade secret or database rights of a third party;

• use the platform, the documentation or the Generated Applications to develop, train, market or support a product or service competing with the platform, or to carry out benchmarking activities the results of which are disclosed to third parties without the Provider's prior written consent;

• extract, replicate or reuse, by automated means or otherwise, the structure, the interfaces, the component libraries, the templates or the documentation of the platform beyond the use permitted by the Agreement.

Art. 7 — Prohibited uses: licence integrity, entitlements and metering

7.1 Circumvention of technical protection measures

The Customer and its Authorised Users shall not circumvent, tamper with, disable, emulate, replicate, forge or in any way interfere with the mechanisms of activation, authentication, signature verification, Grant validation, metering and usage control of the platform, including the Grants, the activation codes, the licence files, the offline grace period, the counting of Tokens and the association of a Generated Application with its Designated Asset.

7.2 Use in excess of entitlements

The Customer and its Authorised Users shall not use the platform beyond the limits of the Entitlements, in particular by exceeding the number of Authorised Users, activations, Designated Assets, sites or Generated Applications, by sharing individual credentials, by using a single account for more than one individual, or by using a Grant issued for one Designated Asset on a different machine or plant. The replacement of the control hardware of the same machine, with the identifier updated in the Console in accordance with the Enterprise Schedule (Schedule B, IUX-EN-20), is not a use on a different machine and is not a breach of this Article.

7.3 Service bureau and provision to third parties

The Customer and its Authorised Users shall not use the platform to provide services to third parties in the form of a service bureau, outsourcing, time-sharing, hosting on behalf of third parties or any equivalent arrangement, nor allow access to persons other than Authorised Users, unless a partner or reseller agreement expressly signed by the Provider so permits.

7.4 Reverse engineering and mandatory statutory exceptions

The Customer and its Authorised Users shall not decompile, disassemble, reverse engineer or otherwise attempt to derive the source code, the structure, the algorithms or the protection mechanisms of the platform, of the Applications or of the Generated Applications. This prohibition does not apply, and shall not be construed as applying, to acts that cannot lawfully be prohibited under mandatory law, and in particular to decompilation for interoperability purposes permitted by Article 6 of Directive 2009/24/EC and by Article 64-quater of Italian Law 633/1941, which remains permitted subject to the conditions set out in those provisions. In order to make such acts unnecessary, the Provider undertakes to supply, upon reasoned written request and on reasonable terms, the interoperability information required for the Customer's independently created programs to interoperate with the platform.

7.5 Evidence

The records of issue, validation and revocation of the Grants maintained by the Console and by the License Manager, together with the metering records, constitute evidence of the Entitlements granted and of the use made of the platform, subject to proof to the contrary provided by the Customer.

Art. 8 — Prohibited uses: messaging, network and system abuse

The Customer and its Authorised Users shall not:

• send, or use the platform or its notification, sharing, invitation and electronic mail features to send, unsolicited commercial communications, chain messages or any other form of spam, nor use address lists collected without a valid legal basis;

• introduce, host, transmit or distribute malware, viruses, ransomware, logic bombs, backdoors, exploit kits or any other harmful code, or credentials, keys or data obtained unlawfully;

• attempt to gain unauthorised access to the platform, to its infrastructure, to the environments of other tenants, to accounts, keys or data that do not belong to them, or to escalate privileges beyond those granted;

• interfere with the operation of the platform, including through denial-of-service attacks, traffic floods, deliberate saturation of queues, resources or storage, or attempts to bypass rate limiting, quotas or isolation mechanisms;

• carry out automated mass extraction of data, systematic scraping, crawling or mass enumeration of interfaces or identifiers, outside the documented application programming interfaces and the limits set out in Article 18;

• use the resources of the platform for purposes unrelated to the Applications, including cryptocurrency mining, distributed computing, generic file hosting, proxying, relaying, tunnelling or anonymisation of third-party traffic;

• falsify identifiers, headers, network addresses, timestamps or logs, or otherwise conceal the origin of any activity carried out on the platform.

Art. 9 — Security testing and coordinated vulnerability disclosure

9.1 Prior authorisation

Penetration testing, vulnerability scanning, stress testing, load testing, red-teaming and any other security testing of the platform, of its interfaces or of the infrastructure require the Provider's prior written authorisation, which sets the scope, the environment, the time window and the contact points. Testing carried out without such authorisation is Serious Abuse under Article 23.

9.2 Reporting of vulnerabilities

Any vulnerability, security defect or anomalous behaviour identified in good faith, including where identified accidentally, shall be reported without undue delay to support@devibrain.com, with the technical details needed for reproduction, and shall not be disclosed to third parties or made public before the earlier of the remediation of the vulnerability and the expiry of ninety days from the report, save where a shorter period is required by law or agreed in writing between the Parties.

9.3 Good-faith research

The Provider will not bring contractual claims against a person who reports a vulnerability where that person acted in good faith, did not access, copy, alter or exfiltrate data beyond the minimum necessary to demonstrate the vulnerability, did not access personal data of third parties, did not degrade the service, did not use the finding for any other purpose and complied with Article 9.2. This provision does not limit the rights of third parties or the effects of mandatory criminal law.

9.4 Regulatory cooperation

The Parties acknowledge that the Provider may be subject to reporting obligations in respect of actively exploited vulnerabilities and severe incidents under Regulation (EU) 2024/2847, and that the Customer may be subject to incident reporting obligations under Italian Legislative Decree 138/2024. Each Party shall cooperate in good faith, and shall supply the information reasonably required, so that the other Party can comply with such obligations within the applicable time limits.

Art. 10 — Account security and credential management

10.1 Customer obligations

The Customer shall: keep credentials confidential and prevent their sharing; enable multi-factor authentication for every account holding administrative privileges, where the platform makes it available; assign to each Authorised User only the privileges required by that user's role; promptly

revoke access when an Authorised User leaves the organisation or changes role; and keep the list of Authorised Users and the administrative contact details accurate and up to date.

10.2 Devices and workstations

The Customer shall use the platform from devices protected by reasonable, up-to-date security measures, and shall not store credentials or Grant files in clear text on shared devices, in unprotected repositories or in publicly accessible locations.

10.3 Provider measures

The Provider applies the technical and organisational measures described in Article 28 of the Enterprise Schedule (Schedule B, IUX-EN-20) and in Annex 2 to the Data Processing Agreement (IUX-EN-31), and may require the reset of credentials, the revocation of keys or the re-verification of an account where there are reasonable grounds to believe that its security has been compromised.

Art. 11 — Application programming interface keys, machine credentials and integrations

11.1 Protection of keys

Application programming interface keys, service accounts, machine credentials, activation codes and Grant files are issued to the Customer's tenant, are personal to it and are not transferable. The Customer shall store them in a secret manager or in an equivalent protected store, shall not embed them in Generated Applications, in web controls distributed to third parties, in client-side code, in public or shared code repositories, in support tickets, in electronic mail or in documentation.

11.2 Rotation and revocation

The Customer shall rotate keys at least every twelve months, and immediately upon suspected compromise, upon the departure of a person who had access to them, or upon the Provider's reasoned request. The Provider may revoke a key with immediate effect where there is evidence of compromise or abuse, informing the Customer under Article 12.3.

11.3 Integrations and automation

Integrations, scripts, agents and third-party applications operating with the Customer's credentials or keys shall comply with this Policy, with the documented rate limits and with the fair-use standards of Article 18. The Customer is responsible for their configuration and behaviour and shall promptly disable any integration that generates anomalous traffic, duplicated calls or uncontrolled retry loops.

Art. 12 — Notification of compromise and cooperation

12.1 Notification by the Customer

The Customer shall notify the Provider without undue delay and in any event within twenty-four hours from becoming aware of any actual or suspected compromise of credentials, keys, Grants, accounts or environments connected to the platform, and of any unauthorised use of the service. Notification shall be sent to support@devibrain.com and, where the Customer wishes to give it certified date, also to devibrain@pec.it.

12.2 Content of the notification and cooperation

The notification shall state, to the extent known, the nature of the event, the accounts, keys and environments involved, the time when it began and was detected, the categories of data potentially affected and the containment measures taken. The Customer shall cooperate in good faith in the investigation and in the containment activities and shall implement without delay the remediation measures reasonably indicated by the Provider.

12.3 Notification by the Provider

Where the Provider detects the compromise of an account, of a key or of a Grant of the Customer, it shall inform the Customer without undue delay through the administrative contacts registered in the account, indicating the measures taken. Where the event involves personal data, the notification obligations, time limits and roles set out in the Data Processing Agreement and in Articles 33 and 34 of Regulation (EU) 2016/679 apply.

Art. 13 — Responsibility for activity under the account

13.1 Principle

The Customer is responsible for all activity carried out through its account, its Entitlements, its keys and its integrations, and for compliance with this Policy by its Authorised Users and by the persons listed in Article 2.1, as if such activity were its own.

13.2 Limits of the principle

Responsibility under Article 13.1 does not extend to activity that the Customer proves to be attributable to a security failure of the platform for which the Provider is responsible, to conduct of the Provider or of its subcontractors, or to unauthorised access notified in accordance with Article 12.1, in respect of the period following the notification. The Provider shall in all cases cooperate to identify the origin of the event.

13.3 Consumers

Where the Customer is a consumer, responsibility for activity carried out under the account is limited to the cases in which the consumer is at fault, and no burden of proof is placed on the consumer beyond what is permitted by mandatory law. The provisions of Article 28 apply.

Art. 14 — Customer Data: prohibited content

The Customer and its Authorised Users shall not upload to, store on, process on, generate through or distribute by means of the platform any content which:

• is unlawful, or the possession or dissemination of which constitutes a criminal offence, including material depicting the sexual abuse of minors, which the Provider removes and reports to the competent authorities without prior notice;

• is defamatory, denigratory, threatening, harassing, discriminatory, or incites violence or hatred;

• infringes the intellectual property rights, the trade secrets or the confidential information of a third party, including technical drawings, models, libraries, fonts, images and documentation for which the Customer holds no sufficient right of use;

• contains personal data of third parties which the Customer is not entitled to process, or which the Customer processes without a valid legal basis, without the information required by law having been provided, or beyond the purposes agreed with the data subject;

• contains, without the Provider's prior written agreement, special categories of personal data within the meaning of Article 9 of Regulation (EU) 2016/679, data relating to criminal convictions and offences within the meaning of Article 10 of that Regulation, or personal data of minors;

• contains harmful code, live exploits, credentials or data obtained unlawfully;

• contains information classified for reasons of national security, or technical data subject to export control, in the absence of the required authorisations.

Art. 15 — Personal data uploaded to the platform

15.1 Roles and warranties

Where the Customer uploads personal data to the platform, the Customer acts as controller and the Provider as processor, in accordance with the Data Processing Agreement. The Customer warrants that it holds a valid legal basis, that it has provided the required information to data subjects and that the processing entrusted to the Provider is lawful.

15.2 Data minimisation

The Customer shall not upload personal data that are unnecessary for the operation of the Applications. In particular, three-dimensional models, charts, recipes, alarm configurations, media files and documents used for training the artificial intelligence features shall be, so far as possible, free of personal data, pseudonymised or aggregated.

15.3 Consequences

The upload of personal data in breach of this Article is a breach of this Policy and of the Data Processing Agreement. The Provider may require the Customer to remove the data concerned and, where the breach is serious or persists after the notice provided for in Article 24, may apply the

measures set out in Article 23.

Art. 16 — Artificial intelligence features: acceptable use and transparency

16.1 Roles under Regulation (EU) 2024/1689

The Provider acts as provider of the artificial intelligence systems included in the platform, in particular the training features and the local conversational assistant; the Customer that uses them in its own professional context acts as deployer. Each Party shall comply with the obligations attaching to its role.

16.2 Transparency

The Customer and its Authorised Users shall not disable, remove, obscure or alter the notice informing the user that the interaction takes place with an artificial intelligence system, nor the machine-readable markings identifying artificially generated or manipulated content, nor present such content as being of human origin where the law requires it to be identifiable.

16.3 Substantial modification

Where the Customer substantially modifies an artificial intelligence system of the platform, in particular through further training, structural changes to the retrieval pipeline or changes to its intended purpose, such as to alter its behaviour or its risk profile, the Customer may itself become provider of the modified version under Article 25 of Regulation (EU) 2024/1689. The Customer shall inform the Provider in writing in advance and shall assume the resulting obligations.

16.4 Prohibited uses

The Customer and its Authorised Users shall not use the artificial intelligence features of the platform for any practice prohibited by Article 5 of Regulation (EU) 2024/1689, including the inference of emotions of workers in the workplace outside the cases permitted for medical or safety reasons, social scoring, manipulative or exploitative techniques, and the generation of unlawful material. They shall not attempt to circumvent the safety measures or the filters of the systems, nor use them to generate content that infringes Articles 5, 6 or 14 of this Policy.

16.5 Training data

The Customer warrants that it holds the rights necessary to use the documents and data submitted for training, and that such use does not infringe the rights of third parties. Outputs of the artificial intelligence features are decision-support material: they shall be verified by qualified personnel before any operational use.

Art. 17 — Industrial deployment, human oversight and excluded critical uses

17.1 Nature of the platform

The platform, the Applications and the Generated Applications are visualisation, supervision, documentation and decision-support tools. They are not designed, tested or certified as safety instrumented functions, as safety components of machinery or plant, or as protective devices.

17.2 Excluded uses

The Customer and its Authorised Users shall not use the platform, the Generated Applications or the outputs of the artificial intelligence features as the sole or autonomous means for emergency stop functions, protection of persons, functional-safety interlocks, fire or gas detection, medical or life-support applications, control of nuclear installations, aviation or rail traffic control, or any other application in which a malfunction may directly cause death, personal injury, serious environmental damage or catastrophic damage to property, unless the Provider has expressly agreed to such use in writing and the relevant certification requirements have been met.

17.3 Human oversight and validation

The Customer shall ensure human oversight proportionate to the risk of the process concerned, shall validate every Generated Application in a test environment before production use, shall maintain a documented rollback procedure and shall remain responsible for compliance with the machinery safety and functional-safety legislation and standards applicable to its plant.

Art. 18 — Fair use of shared resources

18.1 Principle

The platform is delivered on shared infrastructure. Consumption of resources shall be consistent with normal professional use of the Applications by the number of Authorised Users and the plan set out in the Order, and shall not degrade the service delivered to other customers.

18.2 Fair-use standards

The following standards apply, in addition to any express limits stated in the Order or in the technical documentation:

Shared resource	Fair-use standard	Measurement	Measure applicable in case of excess
Calls to the application programming interfaces and to the licensing services	the rate limits published in the technical documentation and, where higher, those stated in the Order; where no limit is published, consumption not exceeding three times the average consumption of customers on the same plan	rolling period of thirty days, per tenant and per key	notice and rate limiting after five business days; immediate protective rate limiting where the stability of the platform is at risk
Outbound bandwidth and data export	volumes consistent with professional use of the Applications by the Authorised Users stated in the Order	rolling period of thirty days	as above; exports carried out for data retrieval or switching purposes are never limited below the throughput needed to complete retrieval within thirty days
Storage of Customer Data and project assets	the capacity stated in the Order, with a tolerance of ten per cent	monthly, at the end of the period	notice and offer of additional capacity; no deletion of Customer Data before thirty days have elapsed from the notice
Concurrent sessions, build jobs and export jobs	one concurrent session per Authorised User; queued execution of build and export jobs	continuous	queuing and fair scheduling; no permanent restriction without prior notice
Metered features	the prepaid Token balance allocated to each Designated Asset and, in the self-service plans governed by the Shop Schedule (Schedule A, IUX-EN-10), the Prepaid Credit balance of the account wallet	per transaction	metered features stop when the balance concerned is exhausted, in accordance with the Master Subscription and Licence Terms; the balance of one Designated Asset is never drawn on for another

Shared resource	Fair-use standard	Measurement	Measure applicable in case of excess
Support requests	volumes consistent with the support plan stated in the Order	rolling period of thirty days	prioritisation and, in case of repeated abusive volumes, notice under Article 24

18.3 Effect on service levels

Rate limiting, queuing or restriction applied under this Article as a consequence of excess consumption attributable to the Customer does not constitute unavailability for the purposes of the Service Level Agreement (IUX-EN-30) and does not give rise to service credits.

18.4 Excess use of entitlements

Consumption exceeding the Entitlements is regularised in accordance with the Master Subscription and Licence Terms, by payment of the fees due for the excess use, without prejudice to the measures set out in Articles 22 to 24 where the excess results from circumvention of the metering mechanisms.

Art. 19 — Multi-tenant protection and traffic management

19.1 Protective measures

Where an activity, even a lawful one, jeopardises the stability, the security or the performance of the shared infrastructure or of another tenant, the Provider may apply, with immediate effect and to the minimum extent necessary, protective measures such as rate limiting, queuing, temporary isolation of the environment concerned or suspension of a single feature.

19.2 Notice and proportionality

Protective measures shall be proportionate, limited in time and lifted as soon as the cause has ceased. The Provider shall inform the Customer without undue delay and in any event within twenty-four hours from their application, stating the reason, the scope and the expected duration, and shall cooperate with the Customer to identify a stable configuration.

19.3 Prohibition of interference

The Customer and its Authorised Users shall not attempt to evade protective measures, to distribute traffic across multiple accounts, tenants, keys or network addresses in order to circumvent limits, or to create accounts or Trials in series in order to obtain resources or benefits beyond those provided for in the Order.

Art. 20 — Export control, sanctions and restricted destinations

The Customer shall not use, export, re-export, transfer or make available the platform, the Applications, the Generated Applications or the related technical documentation in breach of Regulation (EU) 2021/821 and of the export control, embargo and restrictive-measures rules of the European Union, of the Italian Republic and of any other applicable jurisdiction; in favour of persons or entities subject to restrictive measures; towards embargoed territories; or for military end-uses or uses connected with the proliferation of weapons of mass destruction. Customers established outside the European Union that are not established in a partner country listed in the relevant annex to Regulation (EU) 833/2014 shall comply with the prohibition on re-export to, or use in, the Russian Federation and the Republic of Belarus stated in the Master Subscription and Licence Terms. Where a screening of the applicable lists produces a positive result, the Provider shall suspend the service with immediate effect until the position has been clarified, and such suspension shall not constitute a breach by the Provider.

Art. 21 — Monitoring, telemetry and evidence

21.1 What the Provider monitors

The Provider does not routinely inspect the content of Customer Data. In order to operate the service, to protect its security and to verify compliance with the Entitlements, the Provider processes technical telemetry, access logs, metering records, records of issue and validation of the Grants, and automated abuse-detection signals, in accordance with the principles of necessity and proportionality.

21.2 Access to Customer Data

Access to the content of Customer Data by the Provider's personnel occurs only where strictly necessary in order to respond to a support request made by the Customer, to contain a security incident, to comply with a binding order of a competent authority, or to prevent an offence of which the Provider becomes aware. Every such access is logged, limited to authorised personnel bound by confidentiality obligations, and reported to the Customer save where a legal provision prohibits it.

21.3 Retention of records

Security and abuse-detection logs are retained for twelve months. Records of enforcement decisions taken under this Policy and records of acceptance of this Policy, including the version identifier and the hash of the accepted text, are retained for ten years in tamper-evident storage, for the purposes of evidence and defence of rights.

21.4 Audit

The right of audit and verification, its notice period, its frequency and the preference for remote conduct are governed by the Master Subscription and Licence Terms. This Policy does not extend that right.

Art. 22 — Enforcement: principles and graduated measures

22.1 Principles

The Provider applies the measures provided for in this Policy in good faith, in a proportionate manner, having regard to the gravity, the recurrence and the effects of the breach, and choosing the least intrusive measure capable of protecting the platform, third parties and the other customers. Failure to exercise a right in a given instance does not constitute a waiver of it.

22.2 Graduated measures

Level	Typical situations	Measure	Notice
Level 1 — minor breach	first exceedance of a fair-use standard; multi-factor authentication not enabled on an administrative account; key not rotated within the period set out in Article 11.2; isolated formal non-conformity	written warning with request to remedy	prior written notice, with fifteen days to remedy
Level 2 — significant breach	repetition of a Level 1 event after a warning; sharing of individual credentials; use for the benefit of third parties outside the Order; use in excess of the Entitlements detected through the licensing records	rate limiting, restriction of the feature or of the individual user concerned, charging of the fees due for the excess use	prior written notice of five business days, with fifteen days to remedy

Level	Typical situations	Measure	Notice
Level 3 — Serious Abuse	the conduct listed in Article 23	immediate suspension of the account, of the tenant or of the feature concerned; termination of the Agreement where the breach is not remedied or is not capable of being remedied	written notice without undue delay and in any event within twenty-four hours from the suspension

Art. 23 — Immediate suspension for Serious Abuse

23.1 Cases

The Provider may suspend access to the platform, in whole or in part, with immediate effect, where it has reasonable and documented grounds to believe that one of the following situations exists:

• circumvention, tampering with or forgery of the activation, authentication, Grant or metering mechanisms referred to in Article 7.1;

• reverse engineering outside the mandatory statutory exceptions referred to in Article 7.4;

• intrusion, attempted unauthorised access, distribution of harmful code or attack against the platform, its infrastructure or another tenant;

• security testing carried out without the authorisation required by Article 9.1;

• unlawful content within the meaning of Article 14, or content the retention of which exposes the Provider to liability;

• breach of the export control or sanctions rules referred to in Article 20, or a positive result of a screening of the applicable lists;

• conduct that materially degrades the service delivered to other customers or that places personal data at risk;

• use excluded by Article 17.2 which places the safety of persons at risk;

• non-payment of the fees, in the cases and after the time limits set out in the Master Subscription and Licence Terms and in the payment terms.

23.2 Scope and duration of the suspension

The suspension shall be limited, so far as technically possible, to the account, to the environment or to the feature concerned, and shall be maintained only for as long as the cause persists or for as long as is necessary in order to secure the platform. The Provider shall inform the Customer under

Article 22.2, stating the facts, the measure adopted and the remediation activity required.

23.3 Termination

Where the Serious Abuse is not remedied within fifteen days from the notice, or is not capable of being remedied, or is repeated after a suspension, the Provider may terminate the Agreement with immediate effect by written notice, without prejudice to compensation for damage and to the reimbursement of the fees due for any use in excess of the Entitlements.

Art. 24 — Notice and cure for other breaches

For breaches of this Policy other than Serious Abuse, the Provider shall notify the Customer in writing, stating the conduct complained of, the provision breached and the remediation activity required, and shall grant the Customer fifteen days to remedy the breach and to give evidence of remediation. During that period the Provider may apply the Level 1 and Level 2 measures set out in Article 22.2, but shall not suspend the service. Where remediation does not occur within that period, the Provider may suspend the service and, where the breach persists for a further fifteen days, terminate the Agreement in accordance with the Master Subscription and Licence Terms.

Art. 25 — Contesting a measure and reinstatement

25.1 Contestation

The Customer may contest a measure adopted under this Policy by writing to support@devibrain.com within fifteen days from the notice, setting out its reasons and any supporting evidence. The Provider shall give a reasoned reply within ten business days from receipt and shall lift or reduce the measure where the contestation is well founded.

25.2 Reinstatement

Where the Customer remedies the breach and confirms remediation in writing, the Provider shall verify remediation and restore full access within two business days from the successful verification. Where remediation requires activity by the Provider, the Provider shall carry it out with the diligence provided for in the Service Level Agreement (IUX-EN-30).

25.3 Unjustified measure

Where it is established that a suspension or restriction was not justified, the Provider shall restore the service without delay, shall extend the term of the subscription by a period equal to that of the measure and shall credit the fees relating to the period of unavailability. Any further remedy available to the Customer at law remains unaffected, within the limits of liability set out in the Master Subscription and Licence Terms.

25.4 Escalation

Where the contestation is not resolved, the dispute resolution mechanisms set out in the applicable channel schedule apply, including, for consumers, the alternative dispute resolution information provided there.

Art. 26 — Effects of suspension and termination on data, Tokens and fees

26.1 Customer Data

Suspension does not entail the deletion of Customer Data. Save where the retention of specific content is unlawful, the Customer retains, during the suspension and for thirty days from termination, the right to retrieve Customer Data and the exportable data in the structured formats described in the technical documentation, without any switching charge. The rights of retrieval, portability and switching provided for by Regulation (EU) 2023/2854 and the related time limits are not affected by any measure adopted under this Policy.

26.2 Tokens and Prepaid Credits

Suspension does not consume, reduce or extinguish any prepaid balance. Upon termination two distinct regimes apply, and this Policy does not alter either of them. The Prepaid Credits credited to the wallet of the account under the Shop Schedule (Schedule A, IUX-EN-10) are not forfeited: the Customer obtains the credit or the reimbursement of the part which has not been consumed, in accordance with that Schedule. The Tokens allocated to a Designated Asset under the Enterprise Schedule (Schedule B, IUX-EN-20) remain bound to that Designated Asset, are usable only for consumption relating to it and are not transferred to another Designated Asset, converted into credit or reimbursed, save for the mandatory rights conferred by law. Where termination follows a Serious Abuse attributable to the Customer, the Provider may set off against any credit or reimbursement due under this Article the fees due for use in excess of the Entitlements and any documented damage, giving an itemised statement. Mandatory consumer protection provisions remain unaffected.

26.3 Fees

Where the suspension is attributable to a breach by the Customer, the fees continue to accrue for the duration of the suspension, since the service remains available to the Customer upon remediation. No fee is due for the period of an unjustified measure, in accordance with Article 25.3.

Art. 27 — Reporting abuse and contacts

27.1 Reports

Any person may report a breach of this Policy, unlawful content or a security event to support@devibrain.com. The Provider shall acknowledge receipt within two business days and shall complete its assessment within ten business days, save where the complexity of the matter requires

a longer period, of which the reporting person shall be informed. Reports concerning material depicting the sexual abuse of minors, or an imminent risk to the safety of persons, are dealt with immediately.

27.2 Contact details

Ordinary communications relating to this Policy are addressed to support@devibrain.com; general communications to info@devibrain.com; formal notices, including for the purposes of a certified date, to devibrain@pec.it or to the registered office at Via Coghetti 6, 24128 Bergamo (BG), Italy. Communications to the Customer are addressed to the administrative contacts registered in the account and, where a measure under Article 23 is adopted, also to the electronic mail address of the account holder.

Art. 28 — Consumers: proportionality and mandatory rights

28.1 Proportionality

Where the Customer is a consumer, the measures set out in this Policy are applied with particular regard to proportionality: suspension is adopted only in the cases of Serious Abuse listed in Article 23.1, prior notice is given wherever the protection of the platform or of third parties allows it, and any restriction is limited to the feature concerned.

28.2 Mandatory rights

Nothing in this Policy limits the mandatory rights of consumers, including the legal guarantee of conformity of digital content and digital services, the right of withdrawal, the right not to suffer the outright forfeiture of sums paid in advance without a corresponding entitlement, and the jurisdiction of the courts of the consumer's place of residence or elected domicile. Any clause of this Policy that produced such an effect is void as against the consumer and does not affect the remainder of this Policy.

28.3 Alternative dispute resolution

Information on alternative dispute resolution bodies is set out in the Shop Schedule (Schedule A, IUX-EN-10). No reference is made to the European online dispute resolution platform, which was discontinued following Regulation (EU) 2024/3228.

Art. 29 — Changes to this Policy

29.1 Notice

The Provider may amend this Policy, giving thirty days' prior notice by electronic mail to the administrative contacts registered in the account and by notice within the platform. The notice identifies the version, the date of entry into force and the substance of the changes, and gives

access to the previous version.

29.2 Valid reasons

Amendments may be made only for a valid reason stated in the notice, namely: changes in applicable law or in the requirements of a competent authority; security requirements or newly identified abuse patterns; changes to the architecture, to the infrastructure or to the features of the platform; correction of errors or clarification of the text.

29.3 Right of termination

Where an amendment is materially adverse to the Customer, the Customer may terminate the Agreement, without penalty and with effect from the date of entry into force of the amendment, by written notice given within thirty days from the notice of amendment, and is entitled to a refund of the fees paid for the unused period and to the treatment of unused Tokens and Prepaid Credits provided for in Article 26.2. Consumers may in any event withdraw at no cost within the same period. The notice periods and rights applicable to changes in fees remain governed by the Master Subscription and Licence Terms.

29.4 Immediate changes

Where a change is required by a legal provision with immediate effect or is necessary in order to counter an imminent security threat, it takes effect immediately; the Provider shall give notice as soon as practicable, and the right of termination provided for in Article 29.3 applies from the date of that notice.

29.5 Records

Each version of this Policy is identified by document code and version number. The Provider retains the text of each version, the hash of the accepted text and the evidence of acceptance in accordance with Article 21.3.

Art. 30 — Governing law, jurisdiction and specific approval of onerous clauses

30.1 Governing law and jurisdiction

This Policy is governed by Italian law. For business customers, the Court of Bergamo has exclusive jurisdiction, and the Provider retains the option, at its sole election, of the arbitration provided for in the Master Subscription and Licence Terms in respect of counterparties established outside the European Union, the European Economic Area and the States party to the Lugano Convention, together with the right to seek interim relief and summary payment orders before any competent court. The United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. For consumers, the jurisdiction of the courts of the place of residence or elected domicile of the consumer and the other mandatory protections referred to in Article 28 apply.

30.2 Specific approval

Pursuant to Articles 1341 and 1342 of the Italian Civil Code, the Customer that is not a consumer specifically approves the following clauses of this Policy: Article 7 (prohibitions relating to licence integrity, entitlements and metering, and evidential value of the licensing records); Article 13 (responsibility for activity carried out under the account); Article 18 (fair-use standards and their effect on service levels); Article 19 (protective measures with immediate effect); Article 21 (monitoring, telemetry, retention of records and evidence); Article 22 (graduated enforcement measures); Article 23 (suspension with immediate effect and termination for Serious Abuse); Article 24 (time limits for remediation and termination); Article 26 (effects of suspension and termination on Tokens and fees); Article 29 (unilateral amendment of this Policy); Article 30.1 (governing law, exclusive jurisdiction, optional arbitration and exclusion of the Convention).

30.3 How specific approval is given

In the channels operating with electronic-mail one-time-password acceptance, the specific approval referred to in Article 30.2 is given through a separate confirmation step, distinct from acceptance of the Policy as a whole, recorded in the audit trail with timestamp, network address, user agent, account, document version and hash. In the channel reserved to European Union business customers, the specific approval is given by the second signature affixed to this document by means of a qualified electronic signature, in accordance with the signature blocks below.

Luogo e data: _____

DEVIBRAIN S.R.L.	IL CLIENTE
_____	_____

The specific-approval block below applies exclusively to business customers; it produces no effect as against consumers.

Ai sensi e per gli effetti degli artt. 1341 e 1342 c.c., il Cliente dichiara di avere letto e di approvare specificamente le clausole richiamate nel presente blocco.

Luogo e data: _____

DEVIBRAIN S.R.L.	IL CLIENTE
_____	_____

Status of this version and validation note. This document is release candidate v1.2 of the IndustryUX Acceptable Use Policy, produced on 10 August 2026 and updated on 11 August 2026, on the basis of the legislation in force at those dates. It reflects operating decisions taken by DEVIBRAIN S.R.L. and legal research carried out internally; it does not constitute legal advice and does not replace professional assessment. Before being adopted with real customers, published or annexed to executed contracts, this text must be validated by a qualified lawyer and, as regards Articles 12, 14, 15, 16 and 21, by the data protection officer or by a data protection professional, with particular attention to the points expressly flagged as requiring specialist verification: the export control classification of the cryptographic licensing module, the classification of the deployment models under Regulation (EU) 2024/2847, and the applicability of the re-export restrictions to software supplied on a standalone basis. Once validated, the version number and the date of entry into force are to be confirmed and the text recorded in the acceptance system in accordance with Article 29.5.

Changelog

Version	Date	Changes
1.0	2026-08-10	First release candidate of the Acceptable Use Policy (IUX-EN-35)
1.1	2026-08-11	Gate decisions: machine-bound Tokens, 24-month Prepaid Credit validity, On-Premise service-fee model
1.2	2026-08-11	Plan matrix 2026-08-11: the Pro plan is renamed Business and Enterprise Cloud is renamed Enterprise Online in the scope of application

IUX-EN-35 · v1.2 · 2026-08-11 · IndustryUX® è un marchio registrato di DEVIBRAIN S.r.l.