DATANYX ACCEPTABLE USE POLICY

Tekizma Inc., DBA Datanyx

Effective Date: 18 March 2026

Version: 1.0

This Acceptable Use Policy ("AUP") sets out the standards of acceptable use for the Datanyx platform and all associated services ("Services"). It applies to all customers, administrators, and authorised users of the Services, regardless of deployment model — whether SaaS or On-Premise.

This AUP forms part of, and is incorporated by reference into, the Datanyx SaaS License Agreement or Datanyx On-Premise License Agreement, as applicable ("License Agreement"). By accessing or using the Services, you agree to be bound by this AUP. All capitalised terms used but not defined in this AUP have the meaning given to them in the License Agreement.

Datanyx may update this AUP from time to time to reflect changes in how the Services are used or to address emerging risks. We will provide at least thirty (30) days' prior written notice of any material changes. Continued use of the Services after a change takes effect constitutes acceptance of the updated AUP.

1. PURPOSE

Datanyx builds tools that help organisations connect to their data, make sense of it, and share insights across their teams. This AUP exists to protect the integrity and availability of the Services for all customers, to set clear expectations about responsible use, and to ensure that the Services are not used in ways that are unlawful, harmful, or contrary to the interests of Datanyx, its customers, or third parties.

2. PERMITTED USE

You may use the Services solely for your own internal, lawful business purposes in accordance with the License Agreement, this AUP, and all applicable laws and regulations. Permitted uses include:

- Connecting to authorised data sources and performing analytics, reporting, and data visualisation

- Loading, transforming, and processing data within the Datanyx platform for internal business intelligence purposes
- Generating and scheduling reports and data outputs for internal business use
- Configuring data pipelines and integrations with authorised third-party systems
- Providing authorised users within your organisation with access to the platform in accordance with your subscription and the License Agreement
- Using the platform for product evaluation, testing, or demonstration purposes in non-production environments where permitted by your subscription

3. PROHIBITED USES

You must not use the Services, and must not permit any authorised user or third party to use the Services, for any of the following purposes:

3.1. Unlawful and Harmful Activities:

- Violating any applicable local, national, or international law or regulation
- Processing, storing, or transmitting data in violation of any individual's privacy rights or applicable data protection laws, including the GDPR, CCPA/CPRA, CDPA, or HIPAA
- Engaging in any fraudulent, deceptive, or misleading activity
- Facilitating or promoting illegal activity, including money laundering, terrorism financing, or sanctions evasion
- Using the Services in embargoed countries or territories, or for the benefit of individuals or entities subject to applicable sanctions lists

3.2. Security and Integrity:

- Attempting to gain unauthorised access to the Services, Datanyx's systems or networks, or any other customer's data or account
- Introducing, uploading, or transmitting any malware, viruses, ransomware, spyware, or other malicious or harmful code

- Conducting penetration testing, vulnerability scanning, or security assessments of the Services without Datanyx's prior written consent
- Interfering with, disrupting, or degrading the performance, availability, or integrity of the Services or the infrastructure on which they run
- Circumventing or attempting to circumvent any security, access control, authentication, or usage limit measures implemented by Datanyx
- Using the Services to monitor, probe, or scan other systems or networks without authorisation

3.3. Intellectual Property and Data:

- Reproducing, modifying, distributing, sublicensing, selling, or creating derivative works of the Services or any component thereof without Datanyx's prior written consent
- Reverse engineering, decompiling, disassembling, or otherwise attempting to derive the source code of the Services
- Removing, obscuring, or altering any proprietary notices, labels, or marks on the Services
- Uploading or processing data through the Services that infringes any third party's intellectual property rights, or to which you do not have the necessary rights, licences, or permissions
- Using the Services to scrape, harvest, or extract data from third-party systems without authorisation from the relevant data owner

3.4. Platform Misuse and Unauthorised Distribution:

- Sublicensing, reselling, renting, leasing, lending, or otherwise transferring access to or use of the Services to any third party outside your organisation, except where expressly permitted under a written reseller or white-label agreement with Datanyx
- Using the Services on a timesharing, service bureau, or managed service basis to provide data processing, analytics, or business intelligence services to third parties

- Providing access to the Services to individuals or entities outside your organisation other than authorised users identified in your applicable Order Form
- Assigning, transferring, or delegating your rights or obligations under the License Agreement to any third party without Datanyx's prior written consent
- Using the Services to build or operate a competing product or service, or for benchmarking or competitive intelligence purposes against Datanyx without Datanyx's prior written consent
- Using the Services in any manner that exceeds the usage limits, licensed modules, or authorised user count set out in your applicable Order Form
- Sharing account credentials, API keys, or access tokens with unauthorised individuals or entities
- Using automated scripts, bots, or crawlers to interact with the Services in a manner that places an unreasonable or disproportionate load on Datanyx's infrastructure
- Accessing the Services for the purpose of monitoring their availability, performance, or functionality for competitive purposes, or for any other benchmarking purpose without Datanyx's prior written consent

3.5. Sensitive and High-Risk Data:

- Processing Protected Health Information ("PHI") as defined under HIPAA unless a valid Business Associate Agreement ("BAA") has been executed with Datanyx
- Processing payment card data in a manner that is not compliant with the Payment Card Industry Data Security Standard ("PCI DSS")
- Processing special categories of sensitive personal data (including biometric data, genetic data, data concerning health, racial or ethnic origin, political opinions, religious beliefs, or sexual orientation) without a lawful basis and appropriate safeguards in place

4. CUSTOMER RESPONSIBILITY FOR AUTHORISED USERS

You are responsible for ensuring that all authorised users within your organisation comply with this AUP. You must:

- Ensure that authorised users are made aware of this AUP and the applicable terms of the License Agreement
- Maintain appropriate access controls and promptly revoke access for any user who is no longer authorised or who has violated this AUP
- Promptly notify Datanyx if you become aware of any actual or suspected breach of this AUP or any unauthorised access to or use of the Services
- Take reasonable steps to prevent unauthorised access to your account credentials and report any suspected compromise to Datanyx immediately

5. DATA RESPONSIBILITY

You are the Controller of all data you connect to, load into, or process through the Datanyx platform. You are solely responsible for:

- Ensuring that you have the lawful right and authority to connect to, access, and process all data sources and datasets used with the Services
- Ensuring that your use of the Services to process personal data complies with all applicable data protection laws and the Datanyx Data Processing Addendum ("DPA")
- Ensuring that data subjects have been provided with appropriate notices regarding the use of their personal data in connection with the Services
- Classifying the sensitivity of your data and configuring the Services appropriately to protect it

6. ENFORCEMENT AND CONSEQUENCES

6.1. Suspension: If Datanyx reasonably believes that your use of the Services violates this AUP, or poses a threat to the security, integrity, or availability of the Services or other customers' data, Datanyx may suspend or restrict access to the Services. Where reasonably practicable, Datanyx will provide notice and an opportunity to remedy the violation before suspension. Datanyx may act immediately and without prior notice where the violation poses an immediate or serious risk.

6.2. Termination: Serious or repeated violations of this AUP may result in termination of the License Agreement in accordance with its terms. Termination for AUP violations constitutes termination for cause.

6.3. Cooperation: You agree to cooperate with Datanyx in investigating any suspected AUP violation, including by providing information, logs, or access reasonably requested by Datanyx, to the extent permitted by applicable law.

6.4. No Liability for Enforcement Action: Datanyx will not be liable for any damages, losses, or claims arising from actions taken in good faith to enforce this AUP, including suspension or termination of access.

7. REPORTING VIOLATIONS

If you become aware of any use of the Services that violates this AUP, or if you wish to report a security concern, please contact Datanyx at legal@datanyx.com.

8. RELATIONSHIP TO OTHER AGREEMENTS

This AUP supplements and does not replace the License Agreement, the Data Processing Addendum, the Privacy Policy, or any other agreement between you and Datanyx. In the event of any conflict between this AUP and the License Agreement, the License Agreement shall prevail. This AUP represents Datanyx's minimum standards for acceptable use and does not limit any rights or remedies available to Datanyx under the License Agreement or applicable law.