Alauda Acceptable Use Policy

Effective Date: November 2026 **Version:** 1.4

---

1. Scope

This Acceptable Use Policy ("AUP") applies to all products, services, and online properties made available by Alauda Singapore Pte. Ltd. (UEN 202524557C), a company incorporated in the Republic of Singapore with its registered office at 6 Raffles Quay, #14-02, Singapore 048580 ("Alauda," "we," "us," or "our"), including but not limited to:

- **Alauda Products:** Alauda Container Platform (ACP), Alauda AI Platform, Alauda Enterprise Services, Alauda Virtualization, Alauda Storage Capacity Pack, and any other software, platforms, or services offered by Alauda from time to time
- **Alauda Cloud portal:** The cloud-hosted customer portal and associated online services operated by Alauda at https://cloud.alauda.io
- **Online Services:** Support portals, documentation sites, community forums, training platforms, APIs, and any other internet-accessible services provided by Alauda

This AUP is incorporated by reference into the Alauda Enterprise Agreement ("EA") pursuant to Section 7.2 of the EA, applies to your use of AI functionality of Alauda Products as described in the Alauda AI Supplemental Terms, and is incorporated into any other agreement between you and Alauda that expressly references this AUP (collectively, "Your Agreement"). Capitalized terms used but not defined in this AUP have the meanings given in Your Agreement.

All customers, authorized users, business partners, and any other individuals or entities that access or use Alauda Products, the Alauda Cloud portal, or Online Services ("you" or "Customer") are required to comply with this AUP.

Alauda may modify this AUP by posting a revised version at https://www.alauda.io/legal/acceptable-use-policy, or by providing notice using other reasonable means. If you do not agree to the revised version: (a) the existing AUP will continue to apply to Subscriptions you have purchased as of the date of the update for the remainder of the then-current Subscription term; and (b) the revised version will apply to any new purchases or renewals made after its effective date. If you do not agree to a later revision and you use an applicable copy of the software or an Alauda Model other than under an active Subscription covering that copy or model, the version of this AUP in effect on the date you obtained that copy or model continues to apply to it, no later revision imposes new or additional restrictions on your use of it, and a revised version applies only to a copy, update, or model obtained after its effective date.

---

2. Prohibited Uses

Nothing in this Section 2 limits your rights under, or grants Alauda rights that supersede, the terms of any applicable open source license or Model License for components or models included in Alauda Products (see Section 6.1 of the EA, Sections 1 and 2 of the EULA, and Sections 2.1 and 2.4 of the Alauda AI

Supplemental Terms), including redistribution permitted by those licenses following removal of Alauda trademarks.

You may not use, and may not permit any third party to use, Alauda Products, the Alauda Cloud portal, or Online Services to engage in or facilitate any of the following activities:

2.1 Illegal Activity

Use of Alauda Products or services for any purpose that is unlawful or that violates any applicable local, national, or international law, regulation, order, or governmental requirement, including but not limited to laws relating to data protection, privacy, export control, anti-corruption, sanctions, anti-money laundering, consumer protection, and intellectual property.

2.2 Unauthorized Access

Attempting to gain unauthorized access to any Alauda system, network, server, account, or service, or to any system, network, or service connected to or accessible through Alauda infrastructure, including by probing, scanning, or testing the vulnerability of any system or network, or by breaching or circumventing any security or authentication measure. This includes unauthorized access to other customers' data, environments, or resources. This Section restricts access to and testing of systems operated by Alauda or third parties (including other customers' environments); it does not prohibit security testing of your own deployments of Alauda Products in your own environment.

2.3 Service Interference and Disruption

Any activity that interferes with, disrupts, degrades, or impairs the performance, availability, or functionality of Alauda Products, the Alauda Cloud portal, Online Services, or any connected systems or networks, including denial-of-service attacks, intentional resource exhaustion, or introduction of excessive load. This Section applies to systems and services operated by Alauda or third parties (including other customers' environments); it does not prohibit performance or security testing of your own deployments of Alauda Products in your own environment.

2.4 Licensing Circumvention

Circumventing, evading, or undermining any licensing restrictions, subscription entitlements, or usage limitations associated with Alauda Products, including but not limited to:

- **Over-deployment (under-licensing):** Deploying Alauda Products across more Units (Core-Pairs, Bare Metal Nodes, AI Accelerators, Storage Capacity Packs, or other applicable Units as defined in the Subscription Terms; a cluster is not itself a Unit) than are covered by Customer's active subscriptions
- **Subscription splitting:** Dividing, sharing, or pooling subscription entitlements across separate legal entities, organizational units, or environments in a manner not authorized by Your Agreement
- **Unauthorized redistribution:** Distributing, making available, or providing access to Alauda Products (including subscription keys, activation codes, container images, or proprietary components) to any third party not authorized under Your Agreement

2.5 Unauthorized Publication of Benchmark Results

Publishing, disclosing, or distributing the results of any benchmark, performance test, or comparative analysis of Alauda Products without Alauda's prior written consent. You may conduct internal benchmarks and performance tests for your own evaluation purposes, but any external publication or disclosure of such results requires Alauda's prior written approval. This Section 2.5 does not apply to the evaluation of Alauda Models licensed under third-party Model Licenses (see Section 2.4 of the Alauda AI Supplemental Terms).

2.6 Reverse Engineering

Reverse engineering, decompiling, disassembling, or otherwise attempting to derive the source code, algorithms, data structures, or underlying ideas of any component of the Alauda Products not licensed to you under an open source license or other license permitting such activities, which may include:

- Third-party software components licensed under separate non-open-source terms (as described in Section 6 of the EULA and the Alauda Open Source Notices)

This restriction does not apply to open source software components included in Alauda Products, which are governed by the terms of their respective open source licenses. Nor does this Section 2.6 restrict modification of a work that incorporates or links to a library licensed under the GNU Lesser General Public License (any version), or reverse engineering, decompiling, or disassembling that work to the extent necessary to debug such modifications, in each case to the extent the applicable LGPL requires that those activities be permitted. Nothing in this Section 2.6 applies to the extent the restriction is prohibited by applicable law (including any non-excludable decompilation or interoperability exceptions under the Copyright Act 2021 of Singapore).

2.7 Competitive Use

Using Alauda Products, documentation, technical information, or services as a basis for developing, marketing, or offering a product or service that competes directly with Alauda Products, or for the purpose of conducting competitive analysis on behalf of a direct competitor of Alauda.

This Section 2.7 does not: (a) apply to open source software components included in Alauda Products, whose use is governed by the terms of their respective open source licenses; (b) restrict the exercise of rights expressly granted under an applicable Model License with respect to an Alauda Model or Model Derivative; (c) apply to the evaluation of Alauda Models licensed under third-party Model Licenses (see Section 2.4 of the Alauda AI Supplemental Terms); or (d) limit either party's rights under Section 9.4 of the EA to independently develop or market similar or competitive products.

2.8 Unauthorized Resale, Sublicensing, and Hosted Services

Reselling, sublicensing, renting, leasing, lending, time-sharing, or otherwise making Alauda Products or services available to any third party, or offering Alauda Products as part of a hosted, managed, or software-as-a-service (SaaS) offering, unless expressly authorized in writing by Alauda in Your Agreement or a separate written agreement.

2.9 Malicious Code and Harmful Activity

Transmitting, uploading, distributing, or introducing any virus, worm, Trojan horse, ransomware, spyware, adware, rootkit, keylogger, or other malicious, harmful, or destructive code or software through

or to Alauda Products, the Alauda Cloud portal, or Online Services.

2.10 Intellectual Property Violations

Using Alauda Products or services in a manner that infringes, misappropriates, or violates the intellectual property rights (including patents, copyrights, trademarks, trade secrets, and other proprietary rights) of Alauda or any third party.

2.11 AI Misuse

Where you use AI functionality of Alauda Products (including the Alauda AI Platform and Alauda Models) or run any model on the Alauda AI platform, you may not use such functionality or any model: (a) in violation of Section 6.1 or the last sentence of Section 6.3 of the Alauda AI Supplemental Terms at https://www.alauda.io/legal/ai-supplemental-terms; (b) to generate, disseminate, or facilitate any content or activity prohibited by Sections 2.1 through 2.10, including malicious code, phishing, or spam; (c) to intentionally circumvent, disable, or remove safety filters, guardrails, alignment measures, or content-moderation, logging, or audit mechanisms of a model or AI feature, or to intentionally induce a model to produce output that violates this AUP; or (d) to engage in practices prohibited under Article 5 of Regulation (EU) 2024/1689 or equivalent applicable law, such as social scoring, untargeted scraping of facial images to create or expand facial recognition databases, or purposefully manipulative or exploitative techniques likely to cause significant harm. This Section applies subject to Sections 2.1 and 2.4 of the Alauda AI Supplemental Terms: to the extent an applicable Model License does not permit Alauda to impose additional restrictions, this Section does not restrict the exercise of rights expressly granted under that Model License.

2.12 Online Services Abuse

With respect to the Alauda Cloud portal and Online Services, you may not:

- Transmit spam, phishing messages, or other unsolicited bulk or deceptive communications
- Upload, post, store, or share content that is unlawful, harassing, or exploitative, including child sexual abuse material
- Conduct cryptocurrency mining or other proof-of-work computation on Alauda-operated infrastructure

---

3. Security and Compliance

3.1 Customer Responsibility. Customer is responsible for maintaining the security of its own systems, networks, accounts, credentials, and data in connection with its use of Alauda Products and services. Customer will implement and maintain reasonable administrative, technical, and physical safeguards to protect against unauthorized access to or use of Alauda Products and services within Customer's environment.

3.2 Account Security. Customer is solely responsible for all activities that occur under Customer's accounts and credentials. Customer will maintain the confidentiality of all passwords, API keys, access tokens, and other credentials associated with its use of Alauda Products and services, and will not share credentials across unauthorized users or systems.

3.3 Vulnerability Notification. Customer will promptly notify Alauda at security@alauda.io upon becoming aware of any actual or suspected security vulnerability, breach, unauthorized access, or other security incident affecting Alauda Products, the Alauda Cloud portal, or Online Services. Customer will cooperate with Alauda in investigating and remediating any such incident.

3.4 Compliance with Laws. Customer is responsible for ensuring that its use of Alauda Products and services complies with all applicable laws, regulations, and industry standards, including data protection, privacy, export control, and sector-specific regulatory requirements applicable to Customer's industry and jurisdiction.

---

4. Reporting Violations

If you become aware of any violation of this AUP, or if you have concerns about activity that may constitute a violation, please report it promptly to:

Email: security@alauda.io

When reporting a violation, please provide as much detail as possible, including:

- A description of the suspected violation
- The date and time of the suspected activity
- Any relevant evidence, such as logs, screenshots, or other documentation
- Your contact information for follow-up

Alauda treats all reports seriously and will investigate in a timely manner. Alauda will not retaliate against any person who reports a suspected violation in good faith.

---

5. Enforcement and Remedies

5.1 Investigation and Action. Alauda reserves the right, but is not obligated, to investigate any suspected or reported violation of this AUP. If Alauda determines, in its reasonable discretion, that a violation has occurred or is occurring, Alauda may take any action it deems appropriate, including but not limited to:

- Issuing a warning to the Customer
- Requesting that Customer immediately cease the violating activity
- Suspending Customer's access to the affected Alauda Products, the Alauda Cloud portal, or Online Services, in whole or in part, until the violation is remedied
- Terminating Customer's access to Alauda Products, the Alauda Cloud portal, or Online Services, in whole or in part
- Removing or disabling access to any content or materials that violate this AUP
- Reporting the violation to applicable law enforcement authorities

5.2 No Waiver of Other Rights. Alauda's exercise of its rights under this Section 5 is without prejudice to any other rights or remedies available to Alauda under Your Agreement, at law, or in equity, including any rights of termination set forth in the Alauda Enterprise Agreement. The failure of Alauda to enforce

any provision of this AUP at any time does not constitute a waiver of that provision or of any other provision.

5.3 Cooperation. In the event of a suspected violation, Customer will cooperate promptly and fully with Alauda's investigation, including by providing requested information, access, and assistance.

5.4 Liability. Customer is responsible for any violations of this AUP by its employees, contractors, agents, affiliates, and any other parties who access or use Alauda Products or services through Customer's accounts or under Customer's subscriptions.

5.5 Governing Law. This AUP is governed by the law governing Your Agreement and is subject to the dispute resolution provisions set forth in Your Agreement; if no such agreement applies to you, this AUP is governed by the laws of the Republic of Singapore, and the courts of the Republic of Singapore have exclusive jurisdiction over any dispute arising out of it.