PROCENSE

Acceptable Use Policy

Enterprise Agents, Inc. d/b/a Procense • Effective Date: [Insert] • Version 1.0

This Acceptable Use Policy (the “Policy” or “AUP”) governs access to and use of the Procense platform, cloud services, IoT devices, software, documentation, and support (collectively, the “Services”) provided by Enterprise Agents, Inc. d/b/a Procense (“Procense,” “we,” “us,” or “our”). This Policy is incorporated into and forms part of the agreement under which a customer (“Customer”) subscribes to the Services. By accessing or using the Services, each Customer and Authorized User agrees to this Policy.

1. Purpose and Scope

Procense provides an industrial automation platform for regulated process manufacturing, designed to support 21 CFR Part 11, GMP, and related standards. This Policy defines acceptable and prohibited uses in order to protect the integrity, security, availability, and lawful operation of the Services and the data within them.

This Policy applies to all Authorized Users and to all access to or use of the Services, including the platform, digital forms and electronic records, IoT gateways and sensor interfaces (“Devices”), APIs, integrations, and AI-enabled features (“AI Features”).

2. Definitions

- **Authorized User.** An individual whom the Customer permits to access the Services under the Customer’s account.
- **Customer Data.** Data, content, and records that the Customer or its Authorized Users submit to or generate within the Services, including production and quality records.
- **Devices.** Procense-provided or Procense-certified IoT gateways, current receivers, sensors, and related hardware.
- **AI Features.** AI- or machine-learning-based functionality, including process-engineering agents and tools that generate insights, summaries, or recommendations.

3. Acceptable Use

- Use the Services only for the Customer’s internal, lawful business purposes, and in accordance with the agreement, this Policy, and applicable documentation.
- Ensure that all Authorized Users are properly trained and authorized, and keep account credentials confidential and secure.
- Enter accurate and complete information into digital forms and electronic records, consistent with the Customer’s own validated procedures and regulatory obligations.
- Configure and operate the Services and Devices within their intended specifications and documented parameters.

4. Prohibited Activities

Customer and Authorized Users will not, and will not permit any third party to:

- **Unlawful or harmful use.** Use the Services in violation of any applicable law, regulation, or third-party right, or to store or transmit unlawful, infringing, defamatory, or harmful material.
- **Unauthorized access.** Access or attempt to access any account, data, system, or network without authorization; circumvent or attempt to circumvent authentication, access controls, or usage limits; or share, sell, or transfer credentials.
- **Security testing.** Probe, scan, or test the vulnerability of the Services, or breach or circumvent any security or authentication measure, except with Procense's prior written authorization.
- **System integrity and availability.** Introduce malware or malicious code; conduct any denial-of-service activity; or otherwise interfere with, disrupt, degrade, or place an unreasonable load on the Services, the Devices, or other customers' use of the Services.
- **Intellectual property.** Copy, modify, translate, reverse engineer, decompile, or disassemble the Services or Devices; create derivative works; build a competing product or service; or remove, obscure, or alter any proprietary notice.
- **Data misuse.** Submit data the Customer lacks the right to use; upload personal, health, or other sensitive data except as permitted by the agreement and applicable law; or use the Services to unlawfully collect, monitor, or process information about others.
- **Misuse of Devices.** Tamper with, modify, or reverse engineer Device firmware or hardware; connect unauthorized equipment; or use Devices to access networks, systems, or data outside the authorized scope.
- **Misuse of AI Features.** Attempt to manipulate, jailbreak, or extract the underlying models or training data; submit prohibited content; or rely on AI-generated output as the sole basis for safety-critical, release, or regulatory decisions without appropriate human review and validation.
- **Misrepresentation.** Falsify records, electronic signatures, timestamps, or audit information, or use the Services to misrepresent the Customer's identity or affiliation.

> **Important.** The Services support compliance and decision-making; they are not a safety instrumented system and do not replace required validation, qualified human review, or QA disposition. Customer remains responsible for its own regulatory compliance, product-quality decisions, and operational safety.

5. Customer Responsibilities

- Manage Authorized Users, promptly deactivating access when it is no longer needed, and enforce strong credential practices.
- Ensure the accuracy, quality, and legal basis of all Customer Data submitted to the Services.
- Validate and operate digital procedures within the Customer's own change-control and quality-management framework.
- Promptly notify Procense of any suspected security incident, unauthorized access, or violation of this Policy.

6. Third-Party Services and Integrations

The Services may integrate with the Customer's third-party systems (for example, ERP or MES systems). The Customer is responsible for its own systems, accounts, and credentials, for

authorizing each integration, and for ensuring that its use complies with the relevant third-party terms. Procense is not responsible for third-party systems or for data that the Customer directs the Services to exchange with them.

7. Monitoring and Enforcement

Procense may monitor use of the Services for security, performance, billing, and compliance purposes, and may investigate suspected violations of this Policy. Procense is not obligated to monitor Customer Data or content, and any access by Procense is subject to the confidentiality and data-protection terms of the agreement.

8. Suspension and Consequences

Procense may suspend, limit, or terminate access to the Services, in whole or in part, where it reasonably determines that a Customer or Authorized User has violated this Policy or that continued use poses a security, legal, or operational risk. Where practicable, Procense will provide notice; in urgent cases, such as an active security threat, Procense may act first and notify promptly. Procense may cooperate with law enforcement and regulators as required by law.

9. Reporting Violations and Security Concerns

To report a suspected violation, security vulnerability, or misuse of the Services, contact Procense at support@procense.ai. Procense supports responsible disclosure and asks that you provide enough detail to reproduce and assess the issue, and that you avoid accessing or modifying data that is not your own.

10. Changes to This Policy

Procense may update this Policy from time to time. Material changes will be communicated through the Services or by other reasonable means. Continued use of the Services after an update takes effect constitutes acceptance of the revised Policy.

11. Relationship to Other Agreements

This Policy supplements and is incorporated into the subscription or master agreement between Procense and the Customer (the “Agreement”). Capitalized terms not defined here have the meanings given in the Agreement. In the event of a direct conflict, the Agreement governs, except with respect to security and acceptable-use obligations, where the more protective requirement applies.

12. Contact

support@procense.ai