Excavaite Inc.

Acceptable Use Policy

Effective Date: May 1, 2026

Purpose of This Policy

This Acceptable Use Policy (AUP) sets out the rules governing how Customers and Authorised Users may use the Excavaite Sentry-Creator platform. It is incorporated into and forms part of the Excavaite Terms of Service (available at excavaite.com/legal). Violation of this policy may result in suspension or termination of access.

1. Who This Policy Applies To

This policy applies to all Customers who have entered into an agreement with Excavaite Inc. for access to the Excavaite Sentry-Creator platform (Excavaite Cloud or Excavaite Private), and to all Authorised Users accessing the platform under a Customer's account. Customer organisations are responsible for ensuring that all Authorised Users are aware of and comply with this policy.

2. Permitted Uses

The Excavaite platform is licensed solely for the following permitted uses:

- Monitoring, analysing, and managing your organisation's own intellectual property assets
- Ingesting and analysing documents that your organisation owns or has the legal right to process
- Generating IP-related content analysis, prior art research, and strategic insights for internal business purposes
- Reviewing, approving, and acting on IP findings through the platform's workflow tools
- Exporting analysis outputs and reports for use in your organisation's internal processes
- Integrating the platform with authorised document sources through properly scoped connectors

3. Prohibited Uses

3.1 Document Submission Restrictions

You must not submit documents to the platform that:

- You do not own or do not have the legal right to process using third-party AI services
- Are subject to attorney-client privilege or legal professional privilege, unless your organisation's legal counsel has independently assessed and authorised such submission
- Are subject to export control regulations (including ITAR or EAR) that prohibit transmission to third-party AI services, unless you have confirmed compliance

- Contain classified or government-restricted information prohibited from processing by commercial AI services
- Belong to third parties and have been obtained without authorisation

Know Your Documents

Excavaite transmits document content to external AI service providers during ingestion and analysis. It is your responsibility to ensure you have legal authority to submit each document for external AI processing. Excavaite is not responsible for privilege waiver, regulatory exposure, or confidentiality breaches resulting from your submission of documents you did not have the right to process externally.

3.2 Platform Security and Integrity

You must not:

- Attempt to gain unauthorised access to any part of the Excavaite platform, infrastructure, or other customers' data
- Attempt to circumvent, disable, or interfere with authentication, access controls, or security features
- Probe, scan, or test the vulnerability of the platform without Excavaite's prior written authorisation
- Introduce or transmit malicious code, viruses, worms, trojans, or any disruptive or harmful elements
- Interfere with or disrupt the integrity or performance of the platform or its underlying services
- Use automated tools, bots, scrapers, or scripts to access the platform in ways not authorised by Excavaite

3.3 Intellectual Property and Reverse Engineering

You must not:

- Reverse engineer, decompile, disassemble, or attempt to derive source code from the platform or any containerised software
- Copy, reproduce, or create derivative works from the platform software
- Attempt to extract, export, or access API credentials embedded in the Excavaite Private container
- Use any outputs of the platform to train, fine-tune, or evaluate any AI or machine learning model
- Remove or alter any proprietary notices, labels, or marks on the platform

3.4 Misuse of AI and Analysis Features

You must not use the platform's AI analysis or content generation features to:

- Generate content intended to deceive, defraud, or mislead third parties
- Produce fraudulent patent applications, forged prior art, or fabricated IP records
- Investigate or analyse the IP of third parties without appropriate legal authority
- Circumvent or work around IP rights held by others
- Create content that violates applicable law, including copyright, defamation, or privacy law

3.5 Connector and Access Scope

You must not:

- Configure connectors to access document sources beyond what has been explicitly authorised by your organisation's appropriate authority
- Use service accounts or credentials that grant broader access than required for approved sources
- Attempt to use the platform's connector infrastructure to access any system or data outside the approved scope

3.6 General Legal Compliance

You must not use the platform to:

- Violate any applicable law or regulation, including data protection, privacy, export control, or intellectual property law
- Facilitate or participate in any illegal activity
- Transmit, store, or process personal data of individuals in ways that violate applicable data protection law
- Engage in any conduct that could expose Excavaite or other customers to legal liability

4. Responsibilities of Customer Administrators

System Administrators and Security Administrators have additional responsibilities under this policy:

- Configuring and maintaining connector scopes limited to explicitly authorised document sources
- Ensuring role assignments reflect the minimum access necessary for each Authorised User's function
- Promptly deprovisioning access for users who leave the organisation or change roles
- Reviewing audit logs regularly and investigating anomalous activity
- For Excavaite Private: applying security updates to the container within the timelines set out in the Terms of Service
- Maintaining the security of the infrastructure environment in which Excavaite Private is deployed

5. Reporting Violations

If you become aware of a violation of this policy, or of any security vulnerability in the platform, please report it promptly to: support@excavaite.com

Excavaite will treat all reports in confidence and will investigate promptly. We maintain a safe harbour for good-faith security disclosures made in accordance with our Responsible Disclosure Policy.

6. Consequences of Violation

Violation of this policy may result in one or more of the following actions at Excavaite's discretion:

- Written warning to the Customer organisation
- Temporary suspension of access for specific Authorised Users or the Customer account
- Permanent termination of the Customer's subscription in accordance with the Terms of Service
- Legal action where Excavaite has suffered harm or where criminal activity is involved
- Disclosure to relevant authorities where required by law

7. Updates to This Policy

Excavaite may update this Acceptable Use Policy from time to time. Material updates will be communicated to Customers at least 30 days before they take effect. The current version is always available at excavaite.com/legal.

8. Contact

Questions about this policy: support@excavaite.com

Excavaite Inc., [Street Address], [City], [State] [Zip Code]