Trackmedium Acceptable Use Policy

This Trackmedium Acceptable Use Policy (this **"AUP"**) describes prohibited uses of Trackmedium's public websites, customer portals, Products, applications, APIs, and related services, systems, and documentation (collectively, the **"Services"**).

Agreement by use. By accessing or using the Services, you agree to comply with this AUP.

Enforcement. If you violate this AUP, or authorize or assist others to do so, Trackmedium may suspend or terminate your access to the Services, consistent with this AUP, the Agreement (if applicable), and applicable law.

If you are a Subscriber under the Trackmedium Master Subscription Agreement (the **"MSA"**), this AUP is incorporated into the Agreement (as defined in the MSA) by reference. Capitalized terms not defined in this AUP have the meanings set out in the Agreement. If there is a conflict between this AUP and the Agreement with respect to acceptable use of the Services, prohibited conduct, Prohibited Data, or enforcement of this AUP, this AUP will control. The Agreement controls for all other terms.

This AUP applies to all users of the Services, including administrators, end users, authorized third-party users, and any other person who accesses the Trackmedium websites.

Subscriber responsibility. The Subscriber is responsible for ensuring that its Authorized Users and any permitted third parties comply with this AUP when accessing or using the Services under the Agreement.

Effective Date of this version: February 25, 2026.

1. General rule

Use the Services lawfully and responsibly. Do not use the Services in a way that harms Trackmedium, other users, or the confidentiality, integrity, availability, performance, or security of the Services or any system, network, application, or device.

Examples below are not exhaustive.

2. Prohibited use

2.1 Illegal, harmful, or abusive use or content

You may not use, encourage, promote, facilitate, or instruct others to use the Services to:

- violate any applicable law or regulation
- engage in fraud, deception, impersonation, or social engineering, including phishing
- store, transmit, publish, or make available content that is unlawful, infringing, defamatory, or otherwise harmful
- exploit, harm, or attempt to exploit or harm minors, including any sexual exploitation content involving minors
- violate privacy rights, including collecting, processing, disclosing, or sharing personal data without a lawful basis and required permissions
- upload or transmit malicious code such as viruses, worms, trojan horses, ransomware, time bombs, or other harmful components

2.2 Security violations

You may not attempt to compromise the security or integrity of the Services or any related system. This includes:

Proprietary to Trackmedium, LLC

- unauthorized access to any system, account, data, or network
- probing, scanning, or testing the vulnerability of any system, or breaching security or authentication measures, without Trackmedium's prior written authorization
- intercepting or monitoring data or traffic without permission
- forging, falsifying, or obscuring the origin of requests, messages, or headers to evade controls or misrepresent identity
- circumventing access controls, rate limits, technical restrictions, or other protective measures

Vulnerability reporting. If you believe you have discovered a security vulnerability, report it to security@trackmedium.com. Do not perform testing that could degrade the Services, access data you are not authorized to access, or violate law.

2.3 Network abuse and service disruption
You may not use the Services in a way that degrades, disrupts, or interferes with the Services or other users, including:

- denial of service attacks (DoS), distributed DoS, flooding, or similar activity
- excessive, abnormal, or abusive usage patterns that materially impact performance, availability, or stability
- using manual or automated means to avoid limits placed on the Services (including access, storage, bandwidth, API, or notification limits)
- scrape, crawl, harvest, bulk export, or bulk extract content or data from the Services without authorization, including any activity that (i) bypasses authentication or access controls, (ii) defeats rate limits or technical safeguards, (iii) ignores robots directives where applicable, (iv) accesses data you are not authorized to access, or (v) imposes unreasonable load
- operate or enable network services that can be used to disrupt, evade controls, or abuse third parties, including open proxies, open mail relays, or open recursive domain name servers (DNS resolvers), whether through the Services or in connection with use of the Services.

2.4 Credential, account, and access misuse
You may not:

- share credentials, tokens, API keys, or passwords except as permitted by the Agreement and your internal security policies
- allow multiple individuals to use one account in a manner not permitted by the Agreement
- access or attempt to access data, environments, tenants, or resources you are not authorized to access
- provide access to any third party except as expressly permitted under the Agreement

2.5 Licensing and commercial misuse
You may not:

- bypass or attempt to bypass licensing constraints, concurrent session limits, or user limits stated in your Order Form or Agreement
- resell, sublicense, rent, lease, or provide the Services as a service bureau or time-sharing arrangement except as expressly permitted in writing by Trackmedium.

2.6 Competitive misuse, benchmarking, and automated extraction
Except as expressly permitted by the Agreement or by Trackmedium in writing, you may not:

- access or use the Services for benchmarking or competitive analysis purposes
- use the Services to develop, train, improve, or validate a competing product or service
- systematically extract content, data, or outputs from the Services to build datasets for machine learning or AI training, or to build competing knowledge bases

A violation of this section is a material breach of the Agreement.

Proprietary to Trackmedium, LLC

2.7 Tampering with integrity and compliance features
You may not manipulate, disable, or attempt to circumvent controls designed to support integrity and compliance, including audit trails, logs, approvals, authentication controls, authorization checks, and workflow enforcement.

2.8 Messaging and notification abuse
You may not use the Services to send spam or unsolicited bulk messages, or to obscure or falsify message headers or sender identity.

2.9 Sanctions and export controls
You may not use the Services in violation of applicable export control or sanctions laws and regulations.

3. Prohibited Data
The Services are designed for quality management and compliance processes. Unless Trackmedium expressly agrees in writing (for example, in an Order Form, a Statement of Work (SOW), or an addendum), you will not submit, store, or process:

- **Payment card data** regulated by PCI DSS (full card numbers, magnetic stripe data, CVV, or equivalent)
- **Protected health information (PHI)** or other regulated medical data subject to HIPAA or similar healthcare laws, where a specific agreement is required
- **Classified information** or other government-regulated restricted data (including data subject to special handling requirements)
- **Export-controlled data** subject to ITAR or similar export control regimes that require special controls
- **Highly sensitive credentials** such as private keys, root passwords, or master encryption keys, except where Trackmedium specifically provides a feature intended for secure secret storage
- **Government-issued identification numbers** (for example, passport numbers, national ID numbers, or driver's license numbers)
- **Biometric identifiers** (for example, fingerprint templates or facial recognition templates)
- **Personal Data of children** under the age threshold specified by applicable law

You are responsible for determining whether your content is subject to special legal or regulatory requirements and for ensuring appropriate agreements are in place before submitting such content to the Services.

4. Monitoring and enforcement
Trackmedium may investigate suspected violations of this AUP or misuse of the Services. Trackmedium may take appropriate action consistent with applicable agreements and law, including:

- removing, disabling access to, restricting, or modifying content or resources
- rate limiting or throttling
- suspending or terminating access to the Services
- reporting suspected unlawful activity to appropriate authorities, and cooperating with lawful requests

Trackmedium may take any of the above actions in its reasonable discretion to protect the Services, Trackmedium, users, or third parties.

Child safety reporting. If Trackmedium becomes aware of content involving sexual exploitation of minors or other illegal child sexual abuse material, Trackmedium may report it to appropriate authorities and take immediate action to restrict or remove access as permitted by law.

Trackmedium is not obligated to monitor the Services for violations of this AUP. Failure to enforce this AUP in one instance does not waive Trackmedium's rights.

5. Reporting violations

Proprietary to Trackmedium, LLC

If you become aware of any violation of this AUP, you will promptly notify Trackmedium and provide reasonable assistance, as requested, to stop or remedy the violation.

How to report. To report a violation, email **legal@trackmedium.com**.

6. Changes to this AUP

Trackmedium may modify this AUP at any time by posting a revised version at https://www.trackmedium.com/legal. By accessing or using the Services, you agree to the most recent version of this AUP.

Proprietary to Trackmedium, LLC