



Partner Acceptable Use Policy (AUP)

Effective Date: 2/24/2026

Applies To: All partners, developers, retail affiliates, and third parties accessing or integrating with the Tronia Systems Ltd. API ("Tronia API Core").

1. Purpose

This Partner Acceptable Use Policy ("Policy") defines the permitted and prohibited uses of the Tronia Systems Ltd. API. It is designed to protect:

- The integrity, security, and availability of our systems
- Our customers' data and privacy
- Compliance with applicable laws and regulations
- The reputation of our company and our partners

All partners must comply with this Policy as a condition of accessing or using the API.

2. Scope

This Policy applies to:

- All API keys, tokens, credentials, and authentication mechanisms
 - All endpoints, parameters, other infrastructure used via the API
 - All applications, systems, and integrations built using the API
 - All data accessed, transmitted, processed, or stored through the API
 - All end users accessing services via partner integrations
-

3. Permitted Use

Partners may use the API only:

- In accordance with the executed agreement between any authorized agrē client/user and Tronia Systems Ltd.
 - For legitimate business purposes consistent with the API documentation and the requested retail integration scope
 - In compliance with all applicable laws, regulations, and industry standards
 - In a manner that does not harm the performance, security, or reliability of the API
-

4. Prohibited Activities

Partners must NOT:

4.1 Violate Laws or Rights

- Use the API in violation of any applicable law or regulation
- Infringe intellectual property rights
- Violate privacy or data protection laws
- Facilitate fraud, deception, or unlawful conduct

4.2 Security Violations

- Attempt to gain unauthorized access to systems or data
- Reverse engineer, decompile, or attempt to extract source code
- Interfere with or disrupt API functionality
- Circumvent authentication, rate limits, or security controls
- Introduce malware, spyware, ransomware, or malicious code

4.3 Abuse or Overuse

- Exceed rate limits or usage thresholds
- Conduct denial-of-service or stress-testing without written authorization
- Use automated scraping beyond documented API capabilities

4.4 Misuse of Data

- Store data longer than permitted by contract
- Share data with unauthorized third parties
- Use data for profiling, surveillance, or resale unless explicitly authorized
- Combine API data with other datasets in ways that violate privacy laws

4.5 Misrepresentation

- Impersonate Tronia Systems Ltd.
- Misrepresent the nature of your integration
- Remove or alter required branding, attribution, or disclaimers

5. Data Protection & Privacy

Partners must:

- Implement appropriate technical and organizational security measures
- Encrypt data in transit and at rest where required
- Limit access to authorized personnel only
- Promptly notify Tronia Systems Ltd. of any data breach or security incident
- Comply with applicable data protection laws (e.g., PIPEDA, PIPA, GDPR, GLBA or other regional laws as applicable)

6. Security Requirements

Partners must:

- Safeguard API credentials and not embed them in publicly accessible code
- Rotate credentials periodically
- Monitor systems for unauthorized access
- Immediately revoke compromised credentials

7. Monitoring and Enforcement

Tronia Systems Ltd. reserves the right to:

- Monitor API usage for compliance
- Investigate suspected violations

- Suspend or revoke API access without notice for violations
- Report unlawful activities to relevant authorities

Failure to comply may result in:

- Temporary suspension
- Permanent termination
- Legal action
- Financial penalties where permitted

8. Third-Party Integrations

Partners are responsible for ensuring that any subcontractors or downstream users comply with this Policy.

9. Changes to This Policy

We may update this Policy from time to time. Continued use of the API after updates constitutes acceptance of the revised Policy. A current version of this Policy will always be available on our website resource page: <https://my.tronia.com/resources/>

10. Reporting Violations

Partners must report suspected violations or security concerns to:

Operational Contact: support@tronia.com

Acknowledgment

By accessing or using the API, the Partner agrees to comply with this Acceptable Use Policy.