Acceptable Use Policy

Effective May 22, 2026. This Acceptable Use Policy supersedes and replaces all prior versions.

This Acceptable Use Policy ("**AUP**") describes the rules for Client's use of services provided by Methodology IT ("Provider"). The AUP is incorporated by reference into the Master Services Agreement and the applicable Service Attachments. Client is responsible for ensuring that Client's employees, contractors, agents, and other users of the Services comply with this AUP.

Provider may modify this AUP from time to time and will publish the current version. Material changes to the AUP that increase Client's obligations will be communicated with reasonable notice.

1. Compliance with law

Client and Client's users will use the Services in compliance with all applicable laws and regulations, including those governing data protection, privacy, intellectual property, export control, telecommunications, communications decency, and human trafficking.

2. Prohibited content and uses

Client and Client's users will not use the Services to:

- transmit, store, distribute, or display content that is unlawful, defamatory, fraudulent, obscene, harassing, or threatening;
- infringe the intellectual-property rights of any third party, including by hosting pirated content, circumventing technical protection measures, or distributing material in violation of copyright, trademark, or patent law;
- distribute child sexual abuse material (CSAM) or other content unlawful under federal or state law;
- transmit malicious code (viruses, worms, trojans, ransomware, spyware) or other harmful content;
- engage in unauthorized access, attempted access, or surveillance of computer systems, networks, or accounts not authorized for Client's use;
- engage in phishing, pretexting, or other forms of deception to obtain credentials, personal information, or financial information from third parties;

- engage in denial-of-service attacks or any deliberate action that disrupts the operation of computer systems, networks, or services;
- send unsolicited commercial communications (spam) in violation of applicable anti-spam laws (CAN-SPAM Act, CASL, applicable state laws);
- engage in market manipulation, securities fraud, or other financial crime;
- conduct activities related to violence, terrorism, or the production or distribution of weapons of mass destruction.

3. Prohibited use of resources

Client and Client's users will not:

- use the Services in a manner that materially impairs Provider's ability to deliver Services to other clients (excessive bandwidth, storage, or compute consumption beyond Order limits);
- attempt to probe, scan, penetrate, reverse-engineer, or test the vulnerability of Provider's systems, networks, or applications without prior written authorization (authorized penetration testing under a separate Statement of Work is permitted);
- circumvent Provider's authentication, access controls, monitoring, or rate-limiting mechanisms;
- use the Services to operate publicly accessible servers or services not contemplated by the Order without Provider's consent;
- use Provider's systems as a transport, anonymization, or proxy mechanism for traffic originating from or destined for systems not within Client's environment.

4. Voice services — additional rules

For Voice and Collaboration Services (cloud telephony, VoIP) provided through Provider:

- Client will not use the Service for telemarketing or automated calling in violation of the Telephone Consumer Protection Act (TCPA), the Federal Trade Commission's Telemarketing Sales Rule, or state telemarketing laws;
- Client will not use the Service for international call-back or unauthorized international routing;
- Client will not engage in toll fraud, premium-rate fraud, or service-resale arrangements;
- Client will ensure that calls placed through the Service originate from registered caller-ID numbers with current registered addresses;
- Client will not place 911 calls from the Service for non-emergency purposes;
- The full Voice Services restrictions are set forth in the Service Attachment for Cloud and Hosting Services.

5. AI services — additional rules

Where Provider has delivered AI Services to Client (per the Service Attachment for Artificial Intelligence Services):

- Client will not use AI Services to generate content that is unlawful, defamatory, harassing, or that infringes third-party rights;
- Client will not use AI Services to impersonate identifiable individuals without consent, including for the creation of synthetic media depicting real persons;
- Client will not use AI Services to make automated decisions affecting individuals (employment, credit, housing, healthcare, government benefits) without appropriate human review and disclosures required by applicable law;
- Client will maintain appropriate human review of AI-generated outputs before relying on them for material business decisions;
- Client will not attempt to extract or reconstruct training data, system prompts, or model weights from AI Services;
- Client will comply with any data-handling restrictions communicated by Provider regarding specific Third-Party AI Platforms.

6. High-risk uses

Client will not use the Services in applications where Service failure could result in death, serious bodily injury, or severe physical or environmental damage. The full restriction on high-risk use is set forth in the Master Services Agreement.

7. Reporting violations

Client will notify Provider promptly on becoming aware of any actual or suspected violation of this AUP affecting Provider's Services. Reports may be sent to security@methodologyit.tech.

Third parties affected by potential AUP violations involving Provider's Services may contact abuse@methodologyit.tech.

8. Provider responses

Provider may take any of the following actions in response to a violation or suspected violation of this AUP, in addition to remedies set forth in the Master Services Agreement:

- request that Client investigate or remediate the issue;

- suspend or limit the affected Service component on reasonable notice (or immediately for incidents that materially threaten Provider's systems or third parties);
- cooperate with law enforcement and regulators as required by applicable law;
- terminate the affected Service or the Agreement for material breach in accordance with the Master Services Agreement.

Provider will document the basis for any enforcement action and will work in good faith with Client to restore Services promptly once the issue is remediated.

9. Updates

Provider may update this AUP from time to time. Material changes will be communicated with reasonable advance notice. Client's continued use of the Services after publication of an updated AUP constitutes acceptance of the updated AUP.