Third-Party Code of Conduct

Last Updated: March 11, 2025

1. Purpose

This Third-Party Code of Conduct sets out the minimum standards that Synthetic Users expects from its suppliers, partners, subprocessors, contractors, resellers, and any other third party engaged in a business relationship with us (collectively, "Third Parties").

Synthetic Users operates an AI-powered research platform that processes customer data through frontier large language models. The integrity of our service depends not only on our own practices but on the conduct of every party in our ecosystem. This Code exists to protect our customers, our platform, and the broader research community.

2. Scope

This Code applies to all Third Parties that:

- Provide services, software, or infrastructure to Synthetic Users
- Process, store, or access Synthetic Users or customer data
- Act on behalf of Synthetic Users in any commercial capacity
- Supply goods, components, or professional services to our operations

Compliance with this Code is a condition of doing business with Synthetic Users and may be incorporated by reference into contractual agreements.

3. Legal and Regulatory Compliance

Third Parties must:

- Comply with all applicable local, national, and international laws and regulations in the jurisdictions where they operate.
- Maintain all licenses, permits, and registrations required for their business activities.
- Cooperate promptly and transparently with any regulatory inquiry or audit that relates to services provided to Synthetic Users.

4. Data Protection and Privacy

Given the sensitivity of the data flowing through our platform, we hold Third Parties to strict data protection standards:

- **Lawful Processing** — Process personal data only as authorized by Synthetic Users and in accordance with applicable data protection laws, including GDPR and CCPA.
- **Data Minimization** — Access and process only the minimum data necessary to fulfill contractual obligations.
- **No Secondary Use** — Never use Synthetic Users or customer data for any purpose beyond the agreed scope, including model training, analytics, benchmarking, or resale.
- **Encryption** — Encrypt data in transit and at rest using industry-standard protocols (TLS 1.2+ and AES-256 or equivalent).
- **Data Residency** — Honor data residency requirements as specified by Synthetic Users. Do not transfer data outside agreed regions without prior written consent.
- **Breach Notification** — Notify Synthetic Users of any confirmed or suspected data breach within **24 hours** of discovery, with full details of the scope, affected data, and remediation steps.
- **Data Deletion** — Securely delete or return all Synthetic Users and customer data upon termination of the engagement, and provide written confirmation of destruction upon request.

For subprocessors handling personal data, a Data Processing Addendum must be executed prior to any data exchange.

---

5. Information Security

Third Parties must maintain security controls proportionate to the sensitivity of the data and systems they access:

- **Security Certifications** — High-risk Third Parties (those processing customer data or accessing production systems) are expected to hold SOC 2 Type II, ISO 27001, or equivalent certifications.
- **Access Controls** — Enforce least-privilege access, multi-factor authentication, and role-based access controls for any system or data shared with Synthetic Users.
- **Vulnerability Management** — Maintain a vulnerability management program that includes regular scanning, patching, and remediation within defined SLAs.
- **Incident Response** — Maintain a documented incident response plan and notify Synthetic Users promptly of any security event that may impact our data or services.
- **Logging and Monitoring** — Maintain audit logs of access to Synthetic Users data and systems, and make them available upon reasonable request.

---

6. Responsible AI

Third Parties that provide AI models, AI infrastructure, or AI-related services to Synthetic Users must:

- **Transparency** — Clearly document model capabilities, limitations, training data provenance, and known biases.
- **No Unauthorized Training** — Never use Synthetic Users inputs, outputs, prompts, or customer data to train, fine-tune, or improve AI models without explicit written consent.
- **Safety and Alignment** — Maintain appropriate safety measures, content filtering, and alignment practices to minimize harmful outputs.

- **Human Oversight** — Support mechanisms for human review and intervention in AI-generated outputs.
- **Bias Mitigation** — Take active steps to identify and reduce demographic, cultural, and cognitive biases in AI systems provided to Synthetic Users.

---

7. Ethical Business Conduct

7.1 Anti-Corruption and Anti-Bribery

Third Parties must not engage in bribery, corruption, extortion, or embezzlement in any form. This includes compliance with the U.S. Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, and equivalent laws. No payments, gifts, or hospitality may be offered to Synthetic Users employees to influence business decisions.

7.2 Conflicts of Interest

Third Parties must disclose any actual or potential conflict of interest that could affect their objectivity or the integrity of their relationship with Synthetic Users.

7.3 Fair Competition

Third Parties must compete fairly and comply with all applicable antitrust and competition laws. Price-fixing, bid-rigging, market allocation, and other anti-competitive practices are prohibited.

7.4 Accurate Records

Third Parties must maintain accurate and complete business records. Falsification of records, invoices, or reports provided to Synthetic Users is grounds for immediate termination of the relationship.

---

8. Labor and Human Rights

Third Parties must uphold fundamental human rights and fair labor practices:

- **No Forced or Child Labor** — Third Parties must not use forced labor, bonded labor, indentured servitude, or child labor in any part of their operations or supply chain.
- **Fair Wages and Working Hours** — Compensate workers fairly and comply with applicable wage, hour, and benefits laws.
- **Non-Discrimination** — Provide equal opportunity and do not discriminate based on race, color, religion, gender, sexual orientation, gender identity, national origin, disability, age, or any other protected characteristic.
- **Freedom of Association** — Respect workers' rights to freedom of association and collective bargaining in accordance with local law.
- **Safe Working Conditions** — Provide a safe and healthy work environment that meets or exceeds applicable occupational health and safety standards.
- **No Harassment** — Maintain a workplace free from harassment, abuse, intimidation, and retaliation.

These expectations align with the principles outlined in our Human Rights Policy.

9. Environmental Responsibility

Third Parties are expected to:

- Comply with all applicable environmental laws and regulations.
- Minimize the environmental impact of their operations, including energy consumption, waste generation, and emissions.
- Where providing infrastructure or compute services to Synthetic Users, transparently report on energy sources and sustainability practices.
- Pursue continuous improvement in environmental performance.

10. Confidentiality and Intellectual Property

- **Confidentiality** — Protect all confidential information received from Synthetic Users with at least the same degree of care used to protect their own confidential information, and no less than reasonable care.
- **No Unauthorized Disclosure** — Do not disclose Synthetic Users' confidential information, trade secrets, or proprietary technology to any third party without prior written consent.
- **IP Respect** — Do not infringe upon the intellectual property rights of Synthetic Users or any other party. Ensure that all deliverables provided to Synthetic Users are free of third-party IP encumbrances unless disclosed.

11. Subcontracting

Third Parties must not subcontract or delegate any obligation involving Synthetic Users data or systems without prior written approval. Any approved subcontractor must comply with the standards set forth in this Code.

12. Monitoring and Audit

Synthetic Users reserves the right to:

- Request evidence of compliance with this Code, including certifications, audit reports, and policy documentation.
- Conduct or commission audits of Third-Party practices related to this Code, with reasonable notice.
- Require completion of security and compliance questionnaires during onboarding and on an ongoing basis.

Third Parties must cooperate with these requests in good faith and within reasonable timeframes.

13. Reporting Violations

Third Parties are encouraged to report any known or suspected violations of this Code, including concerns about unethical conduct, data misuse, or security vulnerabilities.

Reports can be directed to compliance@syntheticusers.com and will be treated confidentially. Synthetic Users does not tolerate retaliation against anyone who reports a concern in good faith.

14. Non-Compliance and Remediation

Failure to comply with this Code may result in:

- A request for prompt corrective action with defined timelines.
- Suspension of data access or system privileges.
- Termination of the business relationship.
- Legal action where applicable, including claims for damages.

Synthetic Users will work constructively with Third Parties to address compliance gaps, but reserves the right to take immediate action where customer data or platform integrity is at risk.

15. Review and Updates

This Code is reviewed at least annually and updated to reflect changes in our business, regulatory requirements, and industry best practices. Third Parties are responsible for monitoring updates and maintaining compliance with the current version.

16. Contact

For questions about this Third-Party Code of Conduct, contact us at compliance@syntheticusers.com.

Synthetic Users, Inc. 4223 Glencoe Ave, Suite C215-523, Marina del Rey CA 90292