Employee Code of Conduct

Synthetic Users

Version: 1.2

Effective Date: January 2024

Last Updated: March 25, 2026

Document Owner: CTO — Artur Ventura

Review Frequency: Annually

Classification: Internal – Confidential

CRA Reference: 37.2.1

Change History

Version	Date	Author	Changes
1.1	January 2024	CTO / Security Lead	Initial release
1.2	March 25, 2026	Artur Ventura, CTO	Added version metadata and last review date; added change history and related documents. Per JPMC SCA CRA 37.2.1.

---

1. Purpose

This Code of Conduct defines the minimum standards of professional, ethical, and lawful behavior expected of all employees, contractors, and officers of Synthetic Users.

Compliance is mandatory.

2. Scope

This policy applies to:

- All full-time and part-time employees
- Contractors, consultants, and temporary staff
- Anyone with access to Synthetic Users systems, data, or intellectual property

Violations may result in disciplinary action, up to and including termination.

3. Professional Conduct

Employees must:

- Act honestly, ethically, and responsibly at all times
- Treat colleagues, customers, partners, and users with respect
- Avoid harassment, discrimination, or abusive behavior of any kind
- Comply with all applicable laws and regulations in jurisdictions where we operate

Zero tolerance for harassment, discrimination, or retaliation.

4. Conflicts of Interest

Employees must avoid situations where personal interests conflict with company interests.

You must:

- Disclose any actual or potential conflict to management

- Not use your role for personal gain
- Not engage in outside work that interferes with your responsibilities

Undisclosed conflicts are a breach of trust.

---

5. Data Protection & Confidentiality

Synthetic Users operates in data-sensitive environments. Employees must:

- Access customer data **only** when strictly required for their role
- Never access customer projects, questions, or outputs without authorization
- Treat all customer data, internal documents, code, models, and strategies as confidential
- Follow all security, privacy, and access control policies

Unauthorized access, disclosure, or misuse of data is grounds for immediate termination.

---

6. Information Security

Employees must:

- Use company-approved devices, accounts, and tools
- Follow access control, password, MFA, and SSO requirements
- Never share credentials
- Report suspected security incidents immediately

Security negligence is treated as a serious violation.

---

7. Responsible Use of AI

Employees must:

- Use AI systems responsibly and in line with company AI and Responsible Use policies
- Not introduce bias intentionally or manipulate outputs deceptively
- Not represent AI-generated outputs as factual or human-verified when they are not
- Ensure human oversight where required
- Not input sensitive customer data, PII, or confidential company information into unauthorized AI tools or external LLM services outside approved company infrastructure

Synthetic Users does not tolerate deceptive, unsafe, or unethical AI use.

8. Intellectual Property

All work created in the course of employment belongs to Synthetic Users unless explicitly agreed otherwise.

Employees must:

- Protect company IP, including code, models, prompts, architectures, and research
- Not reuse or disclose company IP after employment ends

IP theft or leakage will be pursued legally.

9. Use of Company Resources

Company systems, tools, and data are for business use only.

Employees must not:

- Use company resources for illegal or unethical activities
- Introduce unapproved software or integrations
- Circumvent monitoring, logging, or security controls

We log access. Assume misuse will be detected.

---

10. Anti-Bribery & Anti-Corruption

Employees must not offer, give, request, or accept any bribe, kickback, or improper payment — directly or through a third party — to secure business advantage or influence any decision.

Employees must:

- Decline gifts or hospitality that could be perceived as influencing a business decision
- Report any solicitation of bribes or suspected corrupt conduct immediately
- Comply with all applicable anti-bribery laws, including the U.S. Foreign Corrupt Practices Act (FCPA) and UK Bribery Act where applicable

Refer to the Anti-Bribery & Anti-Corruption Policy for full obligations.

---

11. Compliance & Reporting

Employees are expected to:

- Comply with all internal policies and procedures
- Cooperate with audits, investigations, and compliance reviews
- Report violations, risks, or unethical behavior promptly

Reports can be made without fear of retaliation.

---

12. Enforcement

Violations of this Code may result in:

- Warnings
- Suspension
- Termination
- Legal action where applicable

"I didn't know" is not an excuse.

13. Acknowledgment

All employees must acknowledge they have read, understood, and agreed to comply with this Code of Conduct. Acknowledgment is collected annually via digital sign-off at the December policy refresh (see User Awareness Training Program).

14. Related Documents

- Anti-Bribery & Anti-Corruption Policy — Full obligations for gifts, hospitality, and corrupt conduct
- User Awareness Training Program — Annual security and ethics training; digital acknowledgment process
- Information Governance & Records Management Standard — Data handling obligations
- Incident Response Plan — Security incident reporting
- Password Management Policy — Credential and access security obligations
- Access Rights Review Policy — Least-privilege and access control obligations