

Acceptable Use Policy

1. About this policy

This Acceptable Use Policy governs your access to and use of the Services.

In this policy:

- **you** and **your** mean the individual accessing or using the Services;
- **Customer** means the organisation that has authorised you to access or use the Services; and
- capitalised terms not defined in this policy have the meanings given to them in the Terms of Service.

By accessing or using the Services, you agree to comply with this policy. If you do not agree to this policy, you must not access or use the Services.

You may use the Services only:

1. on behalf of the Customer that has authorised your access;
2. within the permissions and usage rights granted to you;
3. for the Customer's internal business operations; and
4. in accordance with the Agreement, the Documentation, the Customer's applicable policies and instructions, and applicable law.

Your compliance with this policy does not reduce or replace the Customer's obligations under the Agreement.

2. Account and access security

You must:

1. keep your username, password, access tokens, API keys and other credentials secure and confidential;
2. not share your credentials or permit another person to use your account;
3. use any authentication and security measures required by Virtuoso or the Customer;
4. access the Services only through the account and permissions assigned to you;
5. not attempt to obtain permissions or access rights that have not been assigned to you;
6. promptly notify the Customer and Virtuoso of any actual or suspected unauthorised access, credential compromise or misuse of your account;

and

7. cooperate reasonably with the Customer and Virtuoso in investigating and mitigating any such incident.

You are responsible for activity carried out using your account, except to the extent that the activity results from a breach of the Agreement by Virtuoso or from unauthorised access that you could not reasonably have prevented.

3. Authority to test and automate

You may use the Services only against applications, websites, systems, APIs, environments and infrastructure that you and the Customer are authorised to access and test.

Before configuring or executing a test, you must:

1. comply with the Customer's applicable instructions, policies and approval procedures;
2. ensure, so far as reasonably possible within your role, that all necessary permissions and approvals have been obtained;
3. select an appropriate production or non-production environment;
4. configure appropriate permissions, safeguards, usage limits and test data;
5. consider the possible effects of automated and concurrent execution; and
6. ensure that the proposed testing will not breach applicable law, third-party rights or third-party terms and policies.

Automated test execution may carry out actions without further confirmation, including submitting forms, creating, modifying or deleting records, sending communications, initiating transactions or triggering connected systems.

You must review your test configuration and implement appropriate safeguards before execution. You must not configure or execute a test if you know or reasonably suspect that it could cause unauthorised access, unlawful activity, loss of data, unintended transactions, material service disruption or other material harm.

You must implement appropriate safeguards before using the Services in a production, business-critical, regulated, safety-critical or customer-facing environment.

4. Customer Data and sensitive information

You must not submit data or materials to the Services unless:

1. you are authorised by the Customer to submit them;

2. the Customer has the necessary rights, permissions, consents and lawful bases;
3. their submission and processing are permitted by the Agreement and applicable law; and
4. you comply with the Customer's applicable data-handling, privacy and security policies.

Unless expressly permitted under the Agreement, an Order Form or the Data Processing Agreement, you must not submit:

1. live production personal data;
2. special category data or similarly sensitive personal data;
3. regulated health, financial, payment-card or authentication data;
4. production passwords, credentials, access tokens, cryptographic keys or other secrets;
5. third-party Confidential Information;
6. proprietary source code that the Customer is not authorised to provide;
7. data subject to processing, storage or localisation restrictions that are inconsistent with the operation of the Services; or
8. any other information that you know the Services are not designed or authorised to process.

Where reasonably practicable, you must use anonymised, pseudonymised, masked or synthetic data instead of identifiable or live production data.

You are responsible for understanding and appropriately configuring the sharing and access settings available to you. Information entered into test cases, variables, screenshots, logs, reports, AI Inputs and other materials may be accessible to other Permitted Users who have access to the relevant project, workspace or environment.

Virtuoso's collection, processing and use of Customer Data, Customer Test Execution Data, AI Inputs, AI Outputs and Usage Data are governed by the Agreement, including the Data Processing Agreement where applicable. Nothing in this policy grants Virtuoso any additional right to use Customer Data or Customer Materials.

5. Prohibited activities

You must not, directly or indirectly:

1. use the Services unlawfully, fraudulently or in breach of the Agreement, the Documentation, applicable industry requirements or third-party rights;
2. access or test any system, application, account, data, network or infrastructure without appropriate authorisation;
3. damage, disable, disrupt, overburden or impair the Services or any

- third-party system;
4. conduct or facilitate a denial-of-service attack, destructive load test or other disruptive activity;
 5. introduce, upload, transmit or execute malware, viruses, ransomware, malicious scripts, harmful code or other destructive material;
 6. circumvent or attempt to circumvent authentication, security controls, access controls, rate limits, usage limits or technical restrictions;
 7. gain or attempt to gain unauthorised access to the Services, another customer's environment, or any account, system, data or network;
 8. probe, scan or test the vulnerability of the Services without Virtuoso's prior written authorisation;
 9. reverse engineer, decompile, disassemble or attempt to discover any source code, model, algorithm, system prompt, architecture, underlying method or non-public interface of the Services;
 10. scrape, crawl, harvest, index or systematically collect content or data from the Services, except through an API or integration expressly authorised by Virtuoso;
 11. use the Services or Virtuoso Materials to develop, train, fine-tune, benchmark, evaluate, support or improve a competing product or service;
 12. copy, modify, distribute, resell, lease, sublicense or commercially exploit the Services or Virtuoso Materials except as expressly permitted by the Agreement;
 13. use the Services to provide services to a third party or operate a service bureau without Virtuoso's prior written consent;
 14. remove, obscure or alter any proprietary notice;
 15. impersonate another person or entity, misrepresent the origin of content, or engage in deceptive or misleading activity;
 16. use the Services to harass, discriminate against, defame, threaten or cause harm to any person or entity;
 17. upload, generate or transmit unlawful, infringing, defamatory, discriminatory, sexually exploitative, abusive or otherwise harmful content;
 18. infringe or misappropriate any Intellectual Property Right, privacy right, confidentiality obligation or other third-party right;
 19. automatically harvest or collect personal data or information about third parties without appropriate authorisation and a lawful basis;
 20. use the Services in a manner that creates a material security, legal, regulatory, operational or reputational risk to Virtuoso, the Customer, another customer or any third party; or
 21. encourage, enable, assist or instruct another person to carry out any activity prohibited by this policy.

6. AI Services

You may use AI Services and AI Outputs only as part of your authorised use of the

Services and in accordance with the Agreement, including Schedule B.

You are responsible for all AI Inputs that you submit. You must not submit an AI Input unless you and the Customer have all necessary rights, permissions, consents and lawful bases to submit and process it.

You must not use AI Services or AI Outputs to:

1. develop, train, fine-tune, benchmark, evaluate, support or improve a product, service or AI model that competes with the Services;
2. reverse engineer, extract or attempt to discover any underlying model, system prompt, instruction, algorithm, source code, architecture, safeguard or method used by Virtuoso or an AI Provider;
3. circumvent or attempt to circumvent any content filter, safety measure, usage limit, security control, access control or technical restriction;
4. generate or facilitate unlawful, infringing, malicious, deceptive, discriminatory, defamatory or harmful content or activity;
5. generate malware, exploit code or instructions intended to compromise or obtain unauthorised access to any system, except where expressly authorised for legitimate security-testing purposes;
6. misrepresent an AI Output as having been reviewed, verified or approved by Virtuoso;
7. represent that an AI Output is necessarily accurate, complete, unique, secure, non-infringing or compliant;
8. use an AI Output to make a decision about an individual that has legal or similarly significant effects without appropriate human review and compliance with applicable law; or
9. use an AI Output without appropriate human review where its use could have legal, regulatory, security, financial, operational or material business consequences.

AI Outputs are generated automatically and may be inaccurate, incomplete, unsuitable, non-compliant, insecure, duplicative or inappropriate for your intended use.

Before relying on or using an AI Output, you must review, test, validate and approve it to a standard appropriate to its intended use. This applies particularly where an AI Output is to be used in a development, testing, operational, regulated, compliance, security, customer-facing or production context.

You must not rely on an AI Output as a substitute for professional judgement, legal advice, compliance review, security review, technical review or human decision-making.

You remain responsible for the decisions and actions you take based on an AI Output.

7. Composable Assets

You may access and use the Composable Asset Library and Composable Assets only as permitted by the Agreement.

You must not:

1. redistribute, publish, sublicense, sell, transfer or otherwise make Composable Assets available to a third party;
2. include Composable Assets in a commercial product, service, repository, marketplace, library, training course or other offering;
3. create, compile, publish or maintain a competing directory, repository, catalogue, database, marketplace or asset library using Composable Assets or Composable Asset Library metadata;
4. scrape, crawl, harvest, download, index or systematically collect content or information from the Composable Asset Library, whether by automated means or systematic manual collection;
5. use Composable Assets or associated metadata, classifications, descriptions, categories, tags or organisational structures to develop, train, fine-tune, benchmark, evaluate, support or improve a competing product, testing platform, AI model or automated testing service;
6. remove proprietary notices or attribution from Composable Assets unless expressly permitted; or
7. use Composable Assets in breach of applicable law, third-party rights, the Agreement or the Documentation.

You may use generally available productivity, coding-assistance, documentation-assistance or generative AI tools in connection with your permitted internal use of Composable Assets only where:

1. that use does not train, improve or support a competing product or service;
2. it does not disclose Composable Assets outside the Customer's permitted environment; and
3. it complies with the Customer's applicable policies and the terms applicable to the relevant third-party tool.

You must not submit a Customer Contribution unless:

1. the relevant feature has been enabled by Virtuoso;
2. you are authorised by the Customer to submit it;
3. the Customer has all necessary rights, permissions and consents; and
4. the Customer Contribution complies with the Agreement and this policy.

8. Usage limits and fair use

You must comply with all usage rights, quotas, rate limits, concurrency limits, Executions, Parallels, Credits, retention periods and other restrictions specified in the Order Form, the Agreement or the Documentation.

You must not divide, duplicate, rotate or otherwise manipulate accounts, projects or workloads for the purpose of avoiding usage limits, technical restrictions or charges.

You must take reasonable steps to prevent automated tests from placing excessive, unintended or disruptive load on the Services or any third-party system.

You must not use any robot, spider, automated process or other means to access or interact with the Services except through functionality, APIs or integrations expressly made available or authorised by Virtuoso.

9. Reporting security issues and violations

You must promptly notify the Customer's appropriate security or administrative contact and Virtuoso at **notices@virtuosoqa.com** if you become aware of:

1. an actual or suspected breach of this policy;
2. unauthorised access to or use of the Services;
3. the actual or suspected compromise of account credentials;
4. use of the Services that has caused or is reasonably likely to cause material harm to Virtuoso, the Customer or a third party; or
5. a vulnerability affecting the Services.

You must not exploit a suspected vulnerability beyond the extent necessary to identify and report it.

You must not publicly disclose a suspected vulnerability affecting the Services before giving Virtuoso a reasonable opportunity to investigate and address it.

10. Investigation and enforcement

Virtuoso may investigate suspected breaches of this policy. You must provide reasonable information and cooperation in connection with any such investigation.

Where Virtuoso reasonably determines that your access to or use of the Services:

1. breaches this policy or the Agreement;
2. creates a material security, legal, regulatory or operational risk;
3. threatens the integrity, security, performance or availability of the Services or a third-party system;
4. may expose Virtuoso, the Customer or a third party to material liability or

- harm; or
5. may involve unlawful or unauthorised activity,

Virtuoso may take proportionate protective action. This may include removing or restricting content, limiting functionality, suspending automated execution, or restricting, suspending or disabling your access to the Services.

Where reasonably practicable, Virtuoso will notify you or the Customer and provide a reasonable opportunity to address the issue. Virtuoso may act immediately where necessary to prevent or mitigate unlawful activity, unauthorised access, a security incident, service disruption or material harm.

Any suspension or termination of the Customer's Services is governed by the Agreement.

11. Changes to this policy

Virtuoso may update this policy from time to time in accordance with the Agreement.

The current version will be made available at www.virtuosoga.com/acceptable-use-policy. If you do not agree to an updated version of this policy, you must stop accessing and using the Services.

Last reviewed: 25 August 2026