

Acceptable Use Policy

Updated 2026-09-21

This Acceptable Use Policy applies to the Trickest Technology and Services. All capitalized terms not otherwise defined here will have the meaning specified in the Master Software Services Agreement and its schedules and other references incorporated therein (the “**Agreement**”).

1. Acceptable Use

Client represents and undertakes that it will use the Technology, the Services and the Client Content with the Technology in accordance with the Agreement, the applicable law and the Documentation. Without prejudice to the generality of the foregoing and to the greatest extent permitted by the applicable law, Client agrees to the following:

1. Client will not circumvent any technological protection measures set by Trickest to control access to the Technology;
2. Client will not use, and will not encourage others to use, the Technology or Services to design, modify, create a derivative work or create any program that performs functions similar to the functions performed by the Technology;
3. Client will not disassemble, alter, adapt, merge, modify, translate, decompile, develop versions or derivative works, reverse engineer, upgrade, improve or extend, features or functionalities of the Technology or Services, or any portion of the Technology, or otherwise derive data representations or underlying algorithms, processes, methods or source code, therefrom or otherwise reduce them to human readable form;
4. Client must not remove, alter, modify or appropriate or use as their own, any proprietary markings included therein;
5. Client must not resell, sublicense, assign, transfer, rent, lease, lend or otherwise distribute the rights acquired under this Agreement;
6. Client will not use or encourage others to use the Technology and the Client Content in the Technology or other users' Content : (i) for benchmarking or comparison purposes, (ii) to infringe any rights, (iii) to violate any laws or contracts, (iv) to access, tamper with or misuse any Trickest, its Affiliates or their users systems, (v) share any content that is unlawful, harmful, threatening, obscene, violent, abusive, tortious, defamatory, libelous, vulgar, lewd, profane, invasive of another's privacy, hateful, or otherwise objectionable; (vi) to perform any type of

security testing in violation of this Agreement, applicable laws or contracts or attempt to disable, impair, or destroy the Technology or any systems used or accessed in conjunction with the Technology;

7. Client must not use the Technology or any Content on the Technology for any purposes prohibited by US, EU or other applicable law, including any export control laws or in connection with the design, construction, operation or supervision of any system where the use or a failure of such system could result in a situation that threatens the safety of human life or severe physical harm or environmental or property damage (including without limitation, for example, use in connection with any nuclear, military, avionics, life support, industrial, scientific, other life critical application or similar). The Technology is not designed for such use and Tricest expressly disclaims any liability or warranty for such use;
8. Access to the Technology (or certain Technology features, or Content) may be blocked by Tricest or by foreign governments in certain countries; Client is responsible to make sure that Client's use of the foregoing is legal and available where Client is using them;
9. Client must maintain, monitor, and control all activity conducted through Client's account, and back-up and validate data from all Client systems;
10. Client must not use the Technology or the Content to engage in or promote any unethical, immoral, or illegal activity or enterprise, or to interfere in any political, electoral, democratic process or for military or other purposes.
11. Any modification, reproduction, release, performance, display or disclosure of the Technology by the Client shall be governed solely by this Agreement and shall be prohibited except to the extent expressly permitted by this Agreement.

2. Technology SEP Use

When Client is using the Technology or Client is building and using within or in conjunction with the Technology tools and mechanism for the purpose of a Security Enhancement Program ("**SEP**", meaning an activity to engage in information / assets discovery, exploiting vulnerabilities, web application scanning, penetration testing, social engineering, or any other process related to ethical hacking or offensive cybersecurity or the exploitation of an IT system, configuration, software, or infrastructure with the permission of its owner to determine its vulnerabilities and weak points) Client is responsible to ensure that Client is allowed to do such actions in accordance with the laws applicable in Client's country of residence or where Client is engaging in such an action, that Client has all legally required authorizations, licenses and consent, including from the person for whose purposes Client is using the Technology. In jurisdictions where the standard of security or requirements needed to lawfully engage in SEP are lower than as specified herein, this Agreement will supersede and will represent the minimum legal and security standard and requirements that Client must follow before Client uses the Platform or engage in any SEP.

3. Client's Undertakings

Client represents that it has the appropriate rights to allow Trickest to use and/or modify any software or products as part of any Services and that Client has all required rights, licenses and consents to use the Technology and the Content. Trickest's provision of the Services and of the Technology is contingent upon the warranty provided herein. Client grants Trickest, and subcontractors (if any) a non-exclusive, limited license to use Client Data necessary for performing the Services (if any).

4. AI Features

When Client uses the AI features of the Technology, including the Trickest agent, Client agrees that:

1. Client will direct AI features only at systems, assets, and data that Client owns or is authorized to test, and Section 2 applies to every action an AI feature takes on Client's behalf;
2. Client will not attempt to circumvent, disable, or manipulate the safeguards of the Technology or of the underlying AI models, including by instructing an AI feature to ignore its restrictions, and will not use AI features to create or deploy malicious code, or to cause damage, outside the scope of an authorized SEP;
3. Client will review AI outputs, and actions proposed by an AI feature, before relying on or carrying them out, and remains responsible for actions an AI feature takes on Client's behalf, whether with Client's approval, under permissions Client configures, or under the default permissions of the Technology, except to the extent an action results from Trickest's breach of the Agreement;
4. Client will not use AI features to make or support decisions that produce legal or similarly significant effects for individuals, such as decisions about employment, credit, or access to services, or to profile or monitor individuals other than to the extent necessary and incidental to an authorized SEP;
5. Client will not submit special categories of personal data, criminal-offence data, or records about Client's employees, payroll, or its own customers or end users to AI features, unless the parties' data processing agreement expressly covers that processing;
6. Client will not use AI outputs to develop or train AI models that compete with the Technology;
7. where Client makes AI outputs available to others, Client will not present them as human-generated where the law requires disclosure that they are AI-generated; and
8. Client will comply with the usage policies of the model providers that serve AI features, as identified by Trickest from time to time, to the extent they apply to Client's use, and will not use AI outputs to develop models that compete with those model providers.

Trickest may suspend AI features for Client's workspace where it reasonably believes this Section has been breached or that suspension is necessary to protect the Technology, the underlying AI models, or third parties.