

## ACCEPTABLE USE POLICY

This Acceptable Use Policy (the "Policy") describes the acceptable use of and access by a person authorized to use the Services by a Customer (a "User") to the Xeikon platforms (the "Services") offered by Xeikon to its customers (each a "Customer") who has granted access to the Services. By accessing or using the Services, you agree to the latest version of this Policy.

### 1. LAWS

- 1.1. The User shall not use the Services:
- a. with the intent to violate or intentionally violate any local, national, foreign, or international statute, regulation, rule, order, treaty, or other law (each a "Law" and jointly "Laws");
  - b. in a manner that violates the terms of this Policy.

### 2. FORBIDDEN CONTENT

- 2.1. User may not use Services to use, transmit, distribute, or store any material that:
- a. is abusive, deceptive, fraudulent, illegal, pornographic, obscene, defamatory, slanderous, offensive, libelous, threatening or otherwise inappropriate;
  - b. Violates or otherwise encroaches on the rights of others, including, but not limited to, infringing or misappropriating any privacy, intellectual property, proprietary right of another;
  - c. Advocates or induces illegal activity;
  - d. Stalks, harasses, or harms anyone, including minors, is discriminatory, encourages violence against anyone;
  - e. Impersonates any person or entity or otherwise misrepresents Client's affiliation with a person or entity.

### 3. SAFETY AND SECURITY

- 3.1. User may not use Services in a manner that:
- a. modifies, alters, tampers with, repairs, or otherwise creates derivative works of any software included in the Services;
  - b. accesses or uses the Services in a way intended to avoid incurring fees or exceeding usage limits or quotas;
  - c. connects to any users, hosts, or networks where User does not have permission for, including, but not limited to:
    - monitors or crawls a Services or any other system so that such Services or any other system is impaired or disrupted;
    - conducts denial of service attacks;
    - intentionally interferes with the proper functioning of any Services or any other system, including any deliberate attempt to overload a Services or any other system by any means;
    - operates network services like open proxies, open mail relays, or open recursive domain name servers;
    - uses means (manual or electronic) to avoid any use limitations placed on a Services, such as access and storage restrictions;
  - d. distributes, publishes, sends, or facilitates unsolicited mass e-mailings, promotions, advertising, or solicitations, including commercial advertising and informational announcements;
  - e. alters or obscures mail headers or assume a sender's identity without the sender's explicit permission.
  - f. interferes with or adversely affects the Services or use of the Services by other users;
  - g. uses any high volume automated means (including robots, spiders, scripts or similar data gathering or extraction methods) to access the Services and any other accounts, computer systems, or networks connected to the Services.

### 4. USE LIMITATIONS

- 4.1. Customer shall not (directly or indirectly):
- a. copy or reproduce the Services except as permitted under this Agreement;
  - b. assign, sell, resell, sublicense, rent, lease, time-share, distribute or otherwise transfer the rights granted to Customer under this Agreement to any third party except as expressly set forth herein;
  - c. modify, reverse engineer or disassemble the Services or any system related thereto;
  - d. except to the limited extent applicable laws specifically prohibit such restriction, decompile, attempt to derive the source code or underlying ideas or algorithms of any part of the Services or any system related thereto, attempt to recreate the Services or any system related thereto or use the Services or any system related thereto for any competitive or benchmark purposes;
  - e. interfere with or disrupt the integrity or performance of the Services or any system related thereto;
  - f. attempt to gain unauthorized access to the Services or any system related thereto or its related systems or networks, or perform unauthorized penetrating testing on the Services or any system related thereto;
  - g. publish, post, upload or otherwise transmit any materials and other data that contains any viruses, Trojan horses, worms, time bombs, corrupted files or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any systems, data, personal information or property of another;
  - h. use Services to render services to any third parties;

- i. go far beyond the use parameters for any given Services as described in corresponding Xeikon's policies, including respective order, Service Level Agreement or any other document made available to the Customer in relation to the Services.
  - j. undertake any action that would aim at unreasonable load on Services.
- 4.2. Customer shall not, directly or indirectly disrupt any Services or use any Services to disrupt services or systems of any third parties, use Services to violate or test integrity of any kind of a system, including by not limited to Services, network, any applications, devices or systems.

## **5. MONITORING AND ENFORCEMENT**

- 5.1. Xeikon shall not be responsible or liable for any material or information, other than material or information provided by Xeikon, which is created, stored, maintained, transmitted, or accessible on or through the Services and shall have no obligation to monitor or exercise any editorial control over such material.
- 5.2. While not obliged to perform audits, Xeikon retains the right to (i) investigate violations of this Policy or misuse of the Services, (ii) investigate and help prevent security threats, fraud, or other illegal, malicious, or inappropriate activity, (iii) remove, disable access to, or modify any material or resource that Xeikon believes violates this Policy, (iv) suspend or terminate provision of Services to User for uses that violate this Policy.
- 5.3. Xeikon may report any activity that is suspected to violate the Laws to appropriate law enforcement officials, regulatory authorities or other relevant third parties. Xeikon's reporting may include disclosure of relevant User information. Xeikon may also cooperate with appropriate law enforcement, regulatory authorities or other relevant third parties to assist in the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this Policy. Nothing in this Policy shall in any way limit Xeikon's rights and remedies that may otherwise be available.
- 5.4. By accepting this Policy Customer and User agrees to cooperate with Xeikon to remedy any violation connected with the User's activity or materials.

## **6. CHANGE OF THE POLICY**

Xeikon may, in its sole discretion, modify this Policy from time to time. Xeikon will post notices of such changes on the [\[website\]](#). If the User objects to such changes, the User's sole remedy will be to discontinue use of the Services. The User's continued use of the Services following the posting of such changes will constitute an acknowledgement of such changes and an agreement to be bound by the terms of such changes.

Edition: February 2023