PerkinElmer
For the Better

Acceptable Use Policy

Overview: This Acceptable Use Policy (“**AUP**”) outlines acceptable uses of PerkinElmer Informatics, Inc.’s (together with its affiliates, “**PerkinElmer**”) software as a service offerings (collectively for the purposes of this policy, the “**Services**”) and is incorporated by reference into Customer’s software as a service license agreement governing its use of the Service(s) (“**Agreement**”). This AUP prohibits uses and activities involving the Services that are illegal, infringe the rights of others, or interfere with or diminish the use and enjoyment of the Services by others. PerkinElmer reserves the right to change or modify the terms of this AUP from time to time, effective when posted on PerkinElmer’s website (the “**Site**”). Customer’s use of the Services after changes to the AUP are posted shall constitute acceptance of any changed or additional terms. Any capitalized terms not otherwise defined in this AUP shall have the meaning ascribed to them in Customer’s Agreement.

Prohibited Uses

1. **Unlawful Activities:** The Services shall not be used in violation of any applicable local, state, provincial, federal, national or international law, treaty, court order, ordinance, regulation or administrative rule. This includes, but is not limited to:
   a) Child pornography
   b) Unlawful gambling activities
   c) Threats, harassment, or abuse of any individual, organization or business
   d) Fraudulent activities
   e) Terrorist websites or other sites advocating human violence or hate crimes based upon race, religion, ethnicity, country of origin, political opinion, sex, gender, sexual orientation or identity, gender identity, or any other protected class
   f) Unlawful high yield investment plans, Ponzi schemes, or linking to or advertising such schemes

2. **Pornography**: The Services shall not be used to publish, submit, receive, upload, download, post, use, copy or otherwise produce, transmit, distribute or store pornography.

3. **Unsolicited Email**: The Services shall not be used to send or receive mass unsolicited email (“**SPAM**”). This prohibition includes the direct or indirect sending and receiving of such messages, support of such messages via web page, splash page, or other related sites, or the advertisement of such services. The falsifying of packet header, sender, or user information, in whole or in part, to mask the identity of the sender, originator, or point of origin, or knowingly deleting any author attributions, legal notices, proprietary designations, or labels in a file that the Customer mails or sends is expressly prohibited.

4. **Email Bombing**: The Services shall not be used for sending, returning, bouncing, or forwarding email to specified user(s) in an attempt to interfere with or overflow email services.

5. **Proxy Email**: The Services shall not be used as a proxy email server to forward email to unrelated third parties.

6. **UseNet SPAM**: The Services shall not be used to send, receive, forward, or post UseNet unsolicited email or posts. This includes UseNet services located within the PerkinElmer network.

7. **Hacking**: The Services shall not be used for hacking, attacking, gaining access to, breaching, circumventing, or testing the vulnerability of the user authentication or security of any host, network, server, personal computer, network access and control devices, software, or data without the express authorization of the owner of the system or network.

8. **Threatening Material or Content**: The Services shall not be used to host, post, transmit, or retransmit any content or material that harasses or threatens the health or safety of others. In addition, PerkinElmer reserves the right to decline to provide Services if Customer's use is determined by PerkinElmer in its sole reasonable discretion to be obscene, indecent, vulgar, abusive, hateful, malicious, racist or otherwise promoting bigotry, defamatory, fraudulent, libelous, treasonous, tortious, excessively violent or promoting the use of violence, or otherwise harmful to others.

9. **Violation of Intellectual Property Rights**: The Services shall not be used to publish, submit, receive, upload, download, post, use, copy or otherwise reproduce, transmit, retransmit, distribute, or store any content or material or to engage in any activity that infringes, misappropriates, or otherwise violates the intellectual property rights or publicity rights of PerkinElmer or any third party, including but not limited to any rights protected by any copyright, patent, trademark, trade secret, trade dress, right of publicity, moral rights, or other intellectual property right now known or later recognized by statute, judicial decision or regulation.

10. **Violation of Privacy Rights**: The Services shall not be used to violate any individual's privacy rights and all use of the Services shall comply with all applicable privacy laws and regulations applicable to the use of the Service or Customer Data.

11. **Distribution of Malware:** The Services shall not be used for the storage, distribution, fabrication, or use of malware, including without limitation virus software, worms, Trojan horses, root kits, password crackers, adware, key stroke capture programs, or other programs normally used in malicious activity. The use of such programs in the ordinary course of business, however, may be requested by Customer and approved by PerkinElmer on a case by case basis.

12. **Phishing:** The Services shall not be used for any activity designed to collect personal information (name, account numbers, usernames, passwords, etc.) under false pretense. Splash pages, phishing forms, email distribution, proxy email, or any activity related to phishing activities may result in the immediate suspension of Customer's account.

13. **Server Abuse:** Abuse or excessive use of PerkinElmer's servers, network, and infrastructure is prohibited.

14. **Network Abuse:** Any activity that involves making network connections to any third party without permission is prohibited. Such activity includes, but is not limited to, intentional network interference, port scanning, monitoring, crawling, denial of service, network penetration, sniffing, spoofing, virus deployment, hack attempts, vulnerability scanning, and avoidance of third-party network security restrictions or limitations.

15. **Security Abuse:** Any activity that involves violating the security or integrity of any PerkinElmer network, system, application, device or other technology, account, password protection, or computer is prohibited. Such activity includes, but is not limited to, unauthorized access, internet scamming, password robbery, spidering, harvesting, collection of e-mail addresses or other identifiers, probing, scanning, penetrating, testing, interception, monitoring, network, packet header or e-mail origin falsification (excluding proper use of aliases), covert user information gathering, or otherwise trying to breach the security of PerkinElmer's network, system, applications, or other security features.

16. **Vulnerability Testing:** Customer may not perform any kind of vulnerability testing, penetration testing, or network scans, whether by passive or intrusive techniques, to test the vulnerability of any PerkinElmer system or PerkinElmer's network without PerkinElmer's express written consent.

Reporting Violations of the Acceptable Use Policy. PerkinElmer accepts reports of alleged violations of this AUP via email. Please go to www.perkinelmer.com/informatics/support/contact for contact information. Reports of alleged violations must be verified and must include the name and contact information of the complaining party, the IP address or website allegedly in violation, and a description of the alleged violation. Unless otherwise required by law, such as the DMCA, PerkinElmer owes no duty to third parties reporting alleged violations. PerkinElmer will review all verified third-party reports and will take such actions as it deems appropriate in its reasonable discretion. PerkinElmer will comply with and respond to valid (as PerkinElmer determines in its reasonable discretion) subpoenas, warrants, or court orders. If permitted by applicable law or regulation, PerkinElmer may forward such subpoenas, warrants, or orders to Customer and Customer may respond; however, PerkinElmer reserves the right to respond to any such subpoena, warrant or order if it is the named party in such subpoena, warrant, or order.

Violations and PerkinElmer's Rights. PerkinElmer reserves the right, but does not assume the obligation, to investigate any violation of this AUP. PerkinElmer will act as the sole arbiter as to what constitutes a violation of this AUP. At any time after a violation has occurred, and during the time that any violation is being investigated, PerkinElmer reserves the right to suspend, restrict, or terminate any Services at any time, including without limitation the "blackholing" or "suspension" of suspected IP addresses or hosts, without liability to Customer, in accordance with the terms of the Agreement.

Last Updated: September 23, 2020