Blaxel Acceptable Use Policy

Last amended on November 7, 2025

This Acceptable Use Policy ("**AUP**") sets forth rules that apply to the use of any of Beamlit, Inc., a Delaware corporation, d/b/a Blaxel ("**Blaxel**") services, technology, and products (the "**Services**") by you (collectively, "**you**"). Capitalized terms not defined in this AUP have the meanings given in the Blaxel Standard Terms and Conditions and the applicable Order under which Blaxel provides the Services to you (the "**Agreement**").

Your use of the Services, including any Customer Data, Customer Logs, Customer Workloads, and Customer Applications used in connection with the Services, must comply with this AUP. This AUP is not exhaustive, and Blaxel reserves the right to take remedial action in connection with content or uses not specifically described below. Blaxel may modify this AUP at any time by posting a revised version on Blaxel's website.

When accessing or using the Services, you (and your Users and End Users) will not, and your Customer Applications, Customer Logs, Customer Workloads, and Customer Data will not, directly or indirectly:

- probe, scan, or test the vulnerability of any system or network used to provide the Services;
- breach or otherwise circumvent any security or authentication measures of the Services;
- interfere with or disrupt any user, host, or network, for example by sending a virus, overloading, flooding, spamming, or mail-bombing any part of the Services;
- utilize the Service's resources, such as computing power or network bandwidth, for automated excessive bulk activity and coordinated inauthentic activity, including to mine any cryptocurrency;
- access, search, or create accounts for the Services by any means other than our publicly supported interfaces (for example, "scraping" or creating accounts in bulk);
- send unsolicited communications, promotions or advertisements, or spam to other people;
- send altered, deceptive or false source-identifying information, including "spoofing" or "phishing" scrams;
- engage in any type of payment fraud, including unauthorized use of credit cards or other payment methods, illegitimate chargebacks, or any other method of obtaining the Services without required payment;
- publish or share materials in connection with the Services that constitute child sexually exploitative material (including material which may not be illegal child sexual abuse material but which nonetheless sexually exploits or promotes the sexual exploitation of minors), unlawful pornography, or are otherwise indecent;
- publish or share content in connection with the Services that contains or promotes extreme acts of violence or terrorist activity, including terrorist or violent extremist propaganda;

- advocate bigotry, hatred, or the incitement of violence against any person or group of people based on their race, religion, ethnicity, national origin, sex, gender identity, sexual orientation, disability, impairment, or any other protected class or characteristic(s) associated with systemic discrimination or marginalization in connection with the Services;
- facilitate illegal activities or violations of law (for example, providing instructions for synthesizing or accessing illegal or regulated substances, goods, or services);
- violate the privacy or infringe the rights of others, including publishing, sharing, or storing other people's confidential information, identifying information, or intimate imagery without authorization for the purposes of harassing, exposing, harming, or exploiting them;
- otherwise violate the law in any way, including publishing or sharing content which depicts, promotes, or instructs on illegal activity, is fraudulent, defamatory, misleading, or exploitative, or that infringes the intellectual property rights of others; or
- permit or encourage others to commit any of the actions above.

***