Bynder Acceptable Use Policy

This Acceptable Use Policy ("AUP") relates to any Product offered by Bynder, whether it is provided directly or through another party. By accessing or using the Product, Customer (on behalf of itself and its Users) agrees to the terms of this AUP and will be held responsible for any violations hereof. Capitalized terms not otherwise defined herein shall have the meanings ascribed to them in the Agreement between Customer and Bynder.

1. **Prohibited use and content**. For the purposes of this AUP, Customer Content, as may also be referred to as Customer Data in some other documents, is defined as any data (including Personal Data), such as electronic data, text, documents, pictures, videos, files or other materials uploaded to, generated by, and/or stored within the Product by Customer. Bynder does not access Customer Content without explicit instructions from Customer or upon reasonable written notice to the extent required by applicable law, and accordingly relies on Customer's compliance with this AUP with respect to Customer Content.

Customer shall not upload Customer Content or use the Product in a manner that:

1.1 violates any local, state, national or international applicable laws and regulations, including any regulation on data protection, privacy, direct marketing, artificial intelligence, or any provision of the Agreement;

1.2 fails to secure any required consents from data subjects, when applicable;

1.3 advocates or induces illegal activity;

1.4 infringes or misappropriates the Intellectual Property Rights of another party (for purposes of this AUP, "Intellectual Property Rights" means all and any copyright, know-how, rights in inventions, patents, trade secrets, trademarks and trade names, service marks, design rights, rights in get-up, database rights and rights in data, the right to sue for passing off, utility models, domain names, rights in goodwill and all similar or equivalent rights and in each case, whether registered or not, including any application to protect or register such rights and all renewals and extensions of such rights or applications, whether vested, contingent or future, and wherever existing), by, among other things, publishing, posting, uploading, or otherwise distributing any software, music, videos, or other material protected by intellectual property rights;

1.5 is threatening, abusive, harassing, defamatory, deceptive, false, misleading, or fraudulent;

1.6 involves uploading files that contain viruses, malware, corrupted files, or any other similar software or programs that may damage the operation of another person's computer;

1.7 downloads any file that Customer knows, or reasonably should know, cannot be legally distributed in that way;

1.8 falsifies or deletes any author attributions, legal or proprietary designations, labels of the origin or source of software, or other material contained in a file that is uploaded;

1.9 harvests or otherwise collects information about others, including e-mail addresses, without a valid legal basis to do so, or store data for any purposes

other than using the Product.

2. **Product Security and Integrity.** Customer will use the Product for Customer's internal business purposes only and will not violate the security or integrity of the Product in any way, including but not limited to:
    - 2.1 willfully tampering with the security of the Product or generally abuse the Product;
    - 2.2 interfering with or disrupts the Product or servers or networks connected to the Product;
    - 2.3 using any high-volume automated means (including robots, spiders, scripts or similar data gathering or extraction methods) to access the Product or any other accounts, computer systems, or networks connected to the Product (each a "System")
    - 2.4 accessing data on the Product not intended for Customer;
    - 2.5 logging into a server or account on the Product that Customer is not authorized to access;
    - 2.6 attempting to probe, scan, or test the vulnerability of any Product or to breach the security or authentication measures or breach or circumvent any security or authentication measures, including without limitation, by scanning, penetrating testing and/or submitting the Product to bug bounty programs;
    - 2.7 attempting to gain unauthorized access to any portion of the Product whether through hacking, password mining, or any other means; or
    - 2.8 interfering with or creating an undue burden on the Product, including without limitation, by sending a virus, overloading or denying service, spamming or by scripting, or
    - 2.9 monitoring data or traffic on a system without permission.

Customer shall comply with Bynder's Responsible Disclosure Policy located at www.bynder.com/en/legal/responsible-disclosure-policy.

3. **Prohibited Commercial Use**

Unless Customer has Bynder's express prior written permission, Customer shall not in any way:

- 3.1 use, remove, or alter any name, logo, tagline, or other mark of Bynder within the Product, or ,rebrand, white label, or otherwise market or distribute the Product under any other name, mark, or brand;
- 3.2 identify itself or its User(s) as Bynder's employee(s), contractor(s), or agent(s);
- 3.3 lease, distribute, license, sell, or otherwise commercially exploit the Product or make the Product available to a third party other than as contemplated in the Agreement;
- 3.4 access the Product for the purposes of building a competitive product or service or reproducing any features, functions or graphics.

4. **API & Integration Services**
    - 4.1 Bynder's software development kits ("SDK") and application programming interface ("API") documentation are available on developer.bynder.com. The documentation describes how Customer may use the SDK and API and build

integrations with third party applications.

4.2 Bynder sets and enforces limits on Customer's use of the API in Bynder's sole discretion. Customer agrees to, and will not attempt to circumvent, such limitations, including without limitation any traffic limits included in the Order Form between Customer and Bynder.

4.3 Customer shall not:

- use the API to replicate or compete with any Product(s) offered by Bynder;
- sell access or sublicense the API for use by a third party; or
- transmit any malware or other computer program that may damage, harmfully interfere with, surreptitiously intercept, or expropriate any system or data.

4.4 Bynder may monitor Customer's use of the API to ensure quality, improve Bynder's products and services, and verify Customer's compliance with the Agreement.

4.5 Customer shall keep confidential all API access credentials, passwords, and tokens.

4.6 Bynder reserves the right to improve and modify the API at any point. Customer may be required to use those modified versions.

5. Monitoring and Enforcement

5.1 Bynder has the sole discretion to determine whether Customer Content or Customer's use of the Product violates this AUP. All Customer Content or actions that are performed by Customer's Users, are the sole responsibility of Customer.

5.2 Customer shall notify Bynder promptly of any access or use of the Product in violation of this AUP that it is becoming aware of.

5.3 Bynder may:

- investigate violations of this AUP or misuse of the Product;
- take measures to prevent security threats, fraud, or other illegal, malicious, or inappropriate activity and to ensure compliance with this AUP;
- notify Customer of violations of this AUP or misuse of the Product and, as the case may be, immediately or after a reasonable remedy timeframe, suspend or terminate use of the Product, or
  disclose, subject to due validation by Bynder's Chief Legal Officer or an external law firm representative, any Customer activity that it suspects violates any law or regulation to appropriate law enforcement officials, regulators or judicial or administrative courts or other appropriate third parties. If Bynder makes this type of required disclosure Bynder will notify Customer, unless Bynder is required to keep the disclosure confidential.

6. Fair Use

The Customer is subject to the traffic and usage limitations set forth in any written agreement between the Parties.

7. Updates to the AUP

Bynder may update and change any part or all of this AUP. If Bynder updates or changes this AUP, the updated AUP will be made available at bynder.com/en/legal. Bynder will notify Customer with an email or a notification in the Bynder Product of any material changes or updates. The updated AUP will become effective and binding thirty (30) days after it has been posted. When Bynder changes this AUP, the "Updated" date below will be changed to reflect the date of the most recent version (“Update Effective Date”). Bynder encourages Customer to review the online AUP periodically.

This Acceptable Use Policy was last updated in October, 2025.