

## Acceptable Use Policy (AUP)

<http://www.Auth0.com/legal>

This Acceptable Use Policy (“**AUP**”) applies to use of Auth0’s online subscription services (“**Subscription Services**”), Auth0’s website published at and under the auth0.com second level domain (the “**Website**”), and to all other services and products offered by Auth0 and accessible from its Website, including Auth0 Signals (collectively “**Auth0 Services**”). We refer to Auth0 as ‘Auth0,’ ‘we,’ ‘our,’ or ‘us,’ and to customers and users of our Auth0 Services as ‘you’ or ‘your’. If you are using our Subscription Services, then your use and our provision of the subscription services are governed by our Terms of Service (if you are a Free, Developer, or Developer Pro customer) or Subscription Agreement (if you are an Enterprise Customer), available at <https://auth0.com/legal>, or such other applicable agreement between you and Auth0 as applies to your access to and use of the Subscription Services (each, a “**Service Agreement**”).

We may suspend or terminate your use of the Auth0 Services for violation of this AUP, subject to any qualifications specified in your Service Agreement, if applicable.

### A. Use of the Auth0 Services

You may not:

- Interfere or attempt to interfere in any manner with the functionality or proper working of the Subscription Services or Website;
- Upload to the Subscription Services or Website, or use the Subscription Services or Website to store or transmit material in violation of any third-party privacy or data protection rights;
- Upload to the Subscription Services or Website, or use the Subscription Services or Website to store or transmit any malware. Malware means programming (code, scripts, active content, and other software) that is designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, or gain unauthorized access to system resources, or that otherwise exhibits abusive behavior. Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, scareware, crimeware, most rootkits, or other malicious or unwanted software or programs;
- Upload, transmit or otherwise process any Protected Health Information (PHI) or any other regulated data or information in violation of any applicable law or regulation.
- Upload, transmit or otherwise process any Payment Card Information (PCI) in violation of any applicable Payment Card Information Security Standards or other similar requirements.
- Interfere with or disrupt the integrity or performance of the Subscription Services or Website or third-party data stored or processed with the Subscription Services or Website or attempt to gain unauthorized access to the Subscription Services or Website or their related systems or networks, including through denial of service, fuzzing or similar attacks;
- Attempt to probe, scan, penetrate or test the vulnerability of an Auth0 system or network, or to circumvent, avoid or breach Auth0's security or authentication measures, whether by passive or intrusive techniques, or by social engineering, except in accordance with the Auth0 policies published at <https://auth0.com/docs/policies/penetration-testing> and with Auth0's express prior written consent;
- Attempt to reverse engineer any of Auth0’s services or technology (including the Auth0 Platform), including as a means to find vulnerabilities or avoid security measures;
- Use any domain name or URL with any Auth0 tenant you create that includes, or is confusingly similar with, in whole or in part, the trademarks, service marks or names of Auth0, any other Auth0 customer, or any third party (a “Domain Violation”). Auth0 may determine whether a Domain Violation exists in its sole and absolute discretion. Without limiting any of Auth0’s other remedies, Auth0 may immediately suspend or delete any tenant that Auth0 determines constitutes a Domain Violation, at any time, with or without notice, without liability of any kind, in its sole and absolute discretion.

If you use any of the Auth0 Services in connection with any cannabis, hemp, and cannabidiol (CBD) products or services (collectively, “**Cannabis Products**”), then you certify that you will comply with all U.S. state, provincial, and local laws, regulations, and guidelines governing or pertaining to Cannabis Products, and further certify that you are

complying with federal law regarding Cannabis Products, except to the extent that the U.S. federal law conflicts with U.S. state, provincial, and local laws.

#### **B. Shared Resources**

You may not use Auth0 systems, networks or technology in a way that unnecessarily interferes with their normal operation, or that consumes a disproportionate share of their resources. (Your use of Subscription Services will not be considered disproportionate if it is consistent with the usage entitlements for which you have subscribed.) You agree that Auth0 may quarantine or delete any data stored on Auth0's systems or networks if Auth0 reasonably believes that the data is infected with any malware, or is otherwise corrupted, and has the potential to infect or corrupt Auth0 systems, networks or technology or other customers' data that is stored or accessed via Auth0 systems, networks or technology.

#### **C. Abuse**

You may not use Auth0's network or services to engage in, foster, or promote illegal, abusive, or irresponsible behavior, including:

- Unauthorized access to or use of data, systems or networks, including any unauthorized attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures;
- Monitoring data or traffic on any network or system without the express authorization of the owner of the system or network;
- Interference with service to any user of the Subscription Services or Website or other networks;
- Use of an Internet account or computer without the owner's authorization;
- Collecting or using email addresses, screen names or other identifiers without the consent of the person identified (including, phishing, Internet scamming, password robbery, spidering, and harvesting);
- Collecting or using information without the consent of the owner of the information;
- Use of the Subscription Services or Website to distribute software that covertly gathers information about a user or covertly transmits information about the user;
- Use of the Subscription Services or Website to commit fraud;
- Any conduct that is likely to result in retaliation against the Auth0 Subscription Services or Website, or Auth0's employees, officers or other agents, including engaging in behavior that results in any server being the target of a denial of service attack (DoS); or
- Use of the Subscription Services or Website to facilitate competition with Auth0, including through establishment of accounts that do not fairly represent their purpose, or for benchmarking purposes not authorized by Auth0.

You acknowledge and agree that Auth0 has a compelling interest in minimizing opportunities for phishing attacks against Auth0 or any of its customers or users. You therefore agree that, if you are or become the owner of any domain name that includes or (as determined by Auth0 in its reasonable discretion) is confusingly similar to any trademark, service mark or names of Auth0 or any of its products or service offerings then, by subscribing to the Subscription Services, or by renewing your subscription, you hereby grant Auth0 the irrevocable option to purchase such domain name from you, at any time, by delivery of written notice to you to that effect, for a one-time fee of twenty five US dollars (US \$25.00). You hereby agree (i) to execute any documentation required by Auth0 to effect such purchase, (ii) that damages will be an inadequate remedy if you refuse to immediately effect such purchase, and (iii) that Auth0 will have the right, in addition to any other rights it has, to obtain in any court of competent jurisdiction (regardless of any agreement to arbitrate between you and Auth0), an order for specific performance or mandamus to enforce such option, without requirement to post bond or other security of any kind.

#### **D. Offensive Content**

You may not publish, transmit or store on or via Auth0's networks or equipment, or use any Auth0 Services, networks or equipment to enable, control or provide access to, any content or links to any content that Auth0 reasonably believes:

- Is obscene;
- Contains harassing content or hate speech, or is violent, incites violence, or threatens violence;

- Is unfair or deceptive under the consumer protection laws of any jurisdiction;
- Is defamatory or violates a person's privacy;
- Creates a risk to a person's safety or health, creates a risk to public safety or health, is contrary to applicable law, or interferes with an investigation by law enforcement;
- Improperly exposes trade secrets or other confidential or proprietary information of another person;
- Is intended to assist others in defeating technical copyright protections;
- Infringes on another person's copyright, trade or service mark, patent, or other property right, or violates any privacy right;
- Is illegal or solicits conduct that is illegal under laws applicable to you or to Auth0; or
- Is otherwise malicious, fraudulent, or may result in retaliation against Auth0 by offended viewers or recipients.

**E. Other**

You will not be entitled to any credit or other compensation for any interruptions of service resulting from AUP violations.