Last Updated January 1, 2021.

This Acceptable Use Policy ("***AUP***") governs Customer's access, use, or receipt of Avalara's services and Customer's access or use of Avalara Technology (defined below).

1. **Definitions.** Capitalized terms in this AUP have the following meanings:
    a. ***"Avalara"*** means Avalara, Inc. and its Affiliates.
    b. ***"Customer"*** means a legal entity that purchases or uses Avalara's services (including professional services).
    c. ***"Avalara Technology"*** means the technology and intellectual property used in providing the products and services offered by Avalara, including computer software programs, connectors, websites, networks, and equipment. Avalara Technology does not include third-party applications.
    d. ***"Affiliate"*** means an entity that controls, is controlled by, or is under common control with Avalara. For this definition, "control" means direct or indirect ownership of more than 50% of the voting interests of the subject entity.
    e. ***"Malware"*** means programming (code, scripts, active content, and other software) that is designed to disrupt or deny operation, gather or transmit information about a user 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, adware, scareware, crimeware, rootkits, and other malicious or unwanted software or programs.
2. **Use of the Services**. Customer shall not:
    a. Interfere or attempt to interfere with the functionality, integrity, or performance of Avalara's services or Avalara Technology;
    b. Upload material to Avalara's services or the Avalara Technology, or use Avalara's services to store or transmit material, in violation of a third party's rights;
    c. Upload Malware to the Avalara Technology or use Avalara's services to store, transmit, or distribute any Malware;
    d. Interfere or attempt to interfere with any third-party data stored within or processed by Avalara's services or Avalara Technology or attempt to gain unauthorized access to Avalara's services or Avalara Technology;
    e. Attempt to probe, scan, penetrate, or test the vulnerability of the Avalara Technology or circumvent, avoid, or breach Avalara's security or authentication measures, whether by passive or intrusive techniques or by social engineering, without Avalara's prior written consent.
3. **Shared Resources.** Customer may not use Avalara's services or Avalara Technology in a way that unnecessarily interferes with normal operation, or that consumes a disproportionate share of Avalara's resources. For example, Avalara may require Customer to repair a coding abnormality in its integration code if such abnormality causes unnecessary conflicts with other customers' use of Avalara Technology or Avalara's services. Customer agrees that Avalara may quarantine or delete any data stored on Avalara's services or Avalara Technology if the data is (i) infected with any Malware or is corrupted, or (ii) has the potential to infect or corrupt (x) Avalara Technology or Avalara's services or (y) third-party data that is stored or accessed via Avalara Technology or Avalara's services. Customer shall comply with any written security or network access requirements that Avalara provides to Customer in connection with its use of the services.

4. **Other Networks**. Customer must comply with the rules of any other system or network it accesses when using Avalara's services.
5. **Abuse**. Customer shall not use Avalara's services or Avalara Technology to engage in, foster, or promote illegal, abusive, or irresponsible behavior, including:
    a. Unauthorized monitoring, access to, or use of data, systems, or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network;
    b. Interference with service to any user of the Avalara Technology or Avalara's services through a denial of service attack;
    c. Use of an internet account or computer without the owner's authorization;
    d. 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);
    e. Collecting or using information without the consent of the owner of the information;
    f. Use of any false, misleading, or deceptive TCP/IP packet header information in an email or a newsgroup posting;
    g. Engaging in any conduct that is likely to result in retaliation against Avalara Technology or Avalara's or Avalara's Affiliates' employees, officers, directors, or agents, including engaging in behavior that results in any Avalara service or service provider being the target of a denial of service attack.
6. **Offensive Content**. Customer shall not publish, transmit, or store, on or via the Avalara Technology, Avalara's services, or any service provider's technology or system, any content or links to any content that Avalara reasonably believes:
    a. Is obscene;
    b. Contains harassing content or hate speech, or is violent, incites violence, or threatens violence;
    c. Is unfair or deceptive under the consumer protection laws of any jurisdiction;
    d. Is defamatory or violates a person's privacy;
    e. 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;
    f. Improperly exposes trade secrets or other confidential or proprietary information of another person or entity;
    g. Is intended to assist others in defeating technical copyright protections;
    h. Infringes on another person's or entity's copyright, trade or service mark, patent, or other property right;
    i. Is illegal or solicits conduct that is illegal under laws applicable to Customer or to Avalara or its Affiliates; or
    j. Is otherwise malicious, fraudulent, or may result in retaliation against Avalara or its Affiliates by offended viewers or recipients.
7. **Service Suspension or Termination**. If Customer violates this AUP, Avalara may suspend or terminate Customer's access to and use of Avalara's services. Customer is not entitled to any credit or other compensation for any interruption or termination of service resulting from Customer's AUP violation.