Acceptable Use Policy

This Acceptable Use Policy ("AUP") describes rules that apply to any party ("you", "your", "yours", or "Merchant") using software as a service applications developed by oneapp or any its affiliates, provided on or through the oneapp platform as applicable ("SaaS"), and any user of the SaaS, including via any software application, products, or services provided by Merchant ("End User"). oneapp together with its affiliates will be referred to as "oneapp" in this AUP. The prohibited conduct in this AUP is not exhaustive. Merchant is responsible for its End Users' compliance with this AUP. If Merchant or any End User violates this AUP, oneapp may suspend Merchant's and End User's use of the SaaS. This AUP may be updated by oneapp from time to time upon reasonable notice, which may be provided via End User's account, email, or by posting an updated version of this AUP at https://legal.withoneapp.com/#aup.

No Inappropriate Content or Users. Do not use the SaaS to transmit or store any content or communications (commercial or otherwise) that is illegal, harmful, unwanted, inappropriate, or objectionable, including, but not limited to, content or communications which oneapp determines (a) is false or inaccurate; (b) is hateful or encourages hatred or violence against individuals or groups; or (c) could endanger public safety. This prohibition includes use of the SaaS by a hate group. Merchant and its End Users are also prohibited from using the SaaS to promote, or enable the transmission of or access to, any prohibited content or communications described in this paragraph.

Prohibited Activities. Do not use the SaaS to engage in or encourage any activity that is illegal, deceptive, harmful, a violation of others' rights, or harmful to oneapp's business operations or reputation, including:

- **Violations of Laws or Standards.** Violating laws, regulations, governmental orders, industry standards, or telecommunications providers' requirements or guidance in any applicable jurisdiction, including any of the foregoing that require (a) consent be obtained prior to transmitting, recording, collecting, or monitoring data or communications or (b) compliance with opt-out requests for any data or communications.

- **Interference with the SaaS.** Interfering with or otherwise negatively impacting any aspect of the SaaS or any third-party networks that are linked to the SaaS.

- **Reverse Engineering.** Reverse engineering, copying, disassembling, or decompiling the SaaS.

- **Falsification of Identity or Origin.** Creating a false identity or any attempt to mislead others as to the identity of the End User or the origin of any data or communications.

No Service Integrity Violations. Do not violate the integrity of the SaaS, including:

- **Bypassing Service Limitations.** Attempting to bypass, exploit, defeat, or disable limitations or restrictions placed on the SaaS.

- **Security Vulnerabilities.** Finding security vulnerabilities to exploit the SaaS or attempting to bypass any security mechanism or filtering capabilities.

- **Disabling the SaaS.** Any denial of service (DoS) attack on the SaaS or any other conduct that attempts to disrupt, disable, or overload the SaaS.

- **Harmful Code or Bots.** Transmitting code, files, scripts, agents, or programs intended to do harm, including viruses or malware, or using automated means, such as bots, to gain access to or use the SaaS.

- **Unauthorized Access.** Attempting to gain unauthorized access to the SaaS.

Data Safeguards. Merchant is responsible for determining whether the SaaS offers appropriate safeguards for Merchant's use of the

SaaS, including, but not limited to, any safeguards required by applicable law or regulation, prior to transmitting or processing, or prior to permitting End Users to transmit or process, any data, communications or transactions via the SaaS.

SaaS and Area Specific Requirements. Additional requirements for specific (a) SaaS applications, including requirements for geographic areas, and (b) SaaS that are purchased from oneapp, but provided, or otherwise made available, by a third party are, in either case, set forth at https://legal.withoneapp.com/#saas-area-specific-terms and apply solely to the extent End User uses those specific (i) SaaS or (ii) third-party products and services.

Violations of this AUP, including any prohibited content or communications, may be reported to support@withoneapp.com. End User agrees to immediately report any violation of this AUP to oneapp and provide cooperation, as requested by oneapp, to investigate and/or remedy that violation.