Acceptable Use Policy

Exhibit C to the Master Services Agreement

Accelerate, LLC

Version 1.0, November 2026

This Acceptable Use Policy (**"AUP"**) is incorporated into that certain Master Services Agreement (the "MSA") by and between Accelerate, LLC ("**Accelerate**") and the Reseller party thereto and that certain Subscription Agreement by and between Accelerate and Reseller (the "**Subscription Agreement**"). This AUP is Exhibit C to the MSA, and applies to all users of the Accelerate ERP Platform, including Reseller and its Authorized Users and End Client personnel accessing the Platform under the End User Terms of Service. Violations may result in suspension or termination as provided in the applicable agreement. Capitalized terms not defined herein shall have the meanings ascribed to them in the MSA and Subscription Agreement.

1. PROHIBITED CONDUCT

Users of the Platform, including Reseller, all End Clients and their personnel, and all Authorized Users, shall not, nor shall they permit any third party to, take any of the following actions:

- Use the Platform in violation of applicable law or for any unauthorized purpose, including data protection, export control, and sanctions laws.
- Upload or transmit data the user does not have the right to process, including Personal Data (as defined in the Data Processing Addendum) collected without required notice or consent.
- Decompile, decrypt, disassemble, reduce or otherwise attempt to reverse engineer the Platform, any portion thereof, or any services or functions provided thereby.
- Modify, adapt, duplicate, republish, display, transmit or distribute all or any part of the Platform or create derivative works based upon the Platform.
- Attempt to gain unauthorized access to, probe, scan, breach, disrupt or interfere with the security of, or otherwise cause harm to, the Platform or its infrastructure, or the internal systems or any website of Accelerate, or any systems resources, accounts, servers or networks connected to or accessible through the systems or websites.
- Access, upload, store, distribute or transmit any materials that (a) violate or infringe in any way upon the rights of others, (b) are unlawful, threatening, abusive, hateful, tortious, defamatory, libelous, deceptive, fraudulent, invasive of another's privacy or publicity rights, harassing, inappropriate, indecent, lascivious, lewd, profane, obscene, racist, or excessively violent, (c) constitute or encourage conduct that would constitute a criminal offense or give rise to civil liability or otherwise violate any law, or (d) contain a virus, Trojan horse, worm, time bomb, cancelbot, easter egg, corruptive file, or other malicious code or harmful or disruptive components.
- Access another customer's data or information, or attempt to do so.
- Share, sell, or transfer account credentials, or permit account sharing among individuals.
- Interfere with or disrupt the integrity or performance of the Platform, including through excessive automated requests.
- Use automated means to scrape, extract, or bulk-export Platform content other than the user's own data through provided export features.

- Impersonate any person or entity or misrepresent its affiliation with any other person or entity, or in any way create a false identity for the purpose of misleading others.
- Misrepresent AI-generated output as independently verified where it has not been reviewed.

2. AI FEATURE USE

In addition, when using the Platform's AI-assisted features, users must not:

- Attempt to extract, manipulate, or reverse engineer underlying models, system prompts, or safety controls (including prompt-injection techniques).
- Submit content intended to generate unlawful, infringing, or harmful output.
- Use AI features to generate output for purposes unrelated to ERP implementation for the applicable End Client.
- Represent Accelerate as the author or guarantor of AI-generated configurations or advice.

3. SECURITY RESPONSIBILITIES

Users, including Reseller, all End Clients and their personnel, and all Authorized Users, must maintain and shall be responsible for reasonable security over their own systems, networks and account credentials. Each user shall promptly notify Accelerate in writing of any suspected compromise of an account or other unauthorized access or use of the Platform, and each user shall use multi-factor authentication where offered.

4. ENFORCEMENT

4.1 Accelerate may investigate suspected violations of this AUP and, in accordance with Section 4.6 of the MSA, Accelerate may suspend access to the Platform immediately where reasonably necessary to protect the Platform, other customers, or third parties, with notice where practicable. Accelerate may restore access when the applicable violation or condition is remedied. Repeated or material violations are grounds for termination for breach of the Subscription Agreement under the MSA.