Certivo

Acceptable Use Policy

Company: Certivo Inc.

Date: March 2026 (Updated)

Audience: All Platform Users

Certivo Inc. Certivo

Effective Date: March 2026 **Last Updated:** March 2026

1. Introduction

This Acceptable Use Policy ("AUP") governs the use of the Certivo ("Platform"), operated by Certivo Inc. ("Certivo," "we," "us," or "our"), located at 4952 Westbrooke Rd., Blackfalds, Alberta, Canada T4M 0L1.

This AUP applies to all users of the Platform, including but not limited to:

- **Tenant Administrators** accessing the Tenant Suite;
- **Instructors** accessing the Instructor Suite;
- **Clients** accessing the Client Portal; and
- **Platform Administrators** accessing the Super Admin console.

By accessing or using the Platform, you agree to comply with this AUP. This AUP is incorporated by reference into the Certivo Master Subscription Agreement and all applicable terms of service.

2. Definitions

2.1 "Platform" means the Certivo, including all four applications (Tenant Suite, Instructor Suite, Client Portal, and Super Admin), associated APIs, Cloud Functions, integrations, and infrastructure hosted at certivo.ca.

2.2 "User" means any individual or entity that accesses or uses the Platform in any capacity.

2.3 "Tenant" means a safety training company or organization that subscribes to the Platform.

2.4 "Content" means any data, text, files, images, documents, certifications, financial records, or other materials uploaded to, stored on, or transmitted through the Platform.

2.5 "Integrations" means third-party services connected to the Platform, including QuickBooks, Xero, Google Calendar, and Stripe.

3. Permitted Uses

The Platform is designed exclusively for the operation and administration of safety training businesses in Canada. Permitted uses include:

3.1 Operating a safety training business, including scheduling classes, managing course offerings, and tracking student enrollment.

3.2 Managing staff, including instructor onboarding, assignment, payroll administration, and performance tracking.

3.3 Tracking and managing safety training certifications, including issuance, renewal monitoring, expiry notifications, and compliance reporting.

3.4 Processing financial transactions, including client invoicing, payroll calculations, expense tracking, and payment collection through Stripe Connect.

3.5 Communicating with clients, students, and instructors through the Platform's built-in communication tools, including email campaigns and drip campaigns, in compliance with applicable law.

3.6 Generating reports, analytics, and compliance documentation for business operations.

3.7 Using third-party integrations (QuickBooks, Xero, Google Calendar) for accounting synchronization and calendar management.

3.8 Accessing the Client Portal to view certifications, book classes, pay invoices, request quotes, and access training resources as made available by your Service Provider.

---

4. Prohibited Uses

Users shall not use the Platform for any purpose that is unlawful, harmful, or otherwise prohibited by this AUP. The following activities are strictly prohibited:

4.1 Illegal Activities

Using the Platform in connection with any activity that violates any applicable federal, provincial, municipal, or international law or regulation, including but not limited to the Criminal Code of Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA), the Alberta Personal Information Protection Act (PIPA), and applicable occupational health and safety legislation.

4.2 Data Scraping and Automated Data Collection

Using bots, crawlers, scrapers, or any automated means to access, collect, harvest, or extract data from the Platform without prior written authorization from Certivo. This includes bulk downloading of certification records, financial data, user profiles, or any other Platform data.

4.3 Reverse Engineering

Reverse engineering, decompiling, disassembling, or otherwise attempting to derive the source code, algorithms, data structures, or underlying architecture of the Platform or any of its components, including but not limited to TenantGuard, Cloud Functions, security rules, or rate limiting mechanisms.

4.4 Malware and Harmful Code

Uploading, transmitting, or introducing any virus, worm, Trojan horse, ransomware, spyware, adware, keylogger, or other malicious software, code, or file to the Platform. This includes any code designed to disrupt, damage, or gain unauthorized access to the Platform or its underlying infrastructure.

4.5 Multi-Tenant Abuse

Attempting to access, view, modify, delete, or exfiltrate data belonging to another tenant or any user outside of your authorized organizational scope. This includes:

- (a) Attempting to bypass TenantGuard organizational scoping mechanisms;
- (b) Manipulating orgId, locationId, or other tenant identifiers;
- (c) Exploiting API endpoints or Cloud Functions to access cross-tenant data;
- (d) Using Super Admin privileges without proper authorization; and
- (e) Any attempt to enumerate or discover other tenants on the Platform.

4.6 Credential Sharing and Password Security

- (a) Sharing login credentials (email and password) with unauthorized individuals;
- (b) Sharing Client Portal login credentials with individuals not authorized to access the associated client account;
- (c) Attempting to guess, brute-force, or otherwise compromise another user's credentials or password;
- (d) Using another person's credentials or password without their explicit authorization; and
- (e) Failing to maintain the confidentiality of your own credentials and passwords.

4.7 Exceeding Rate Limits

Deliberately or repeatedly exceeding API rate limits, Cloud Function invocation limits, or other resource throttling mechanisms implemented by the Platform. Rate limits are enforced per function category (e.g., 5 requests per 5 minutes for authentication functions, 10 per minute for financial functions, 20 per minute for data functions) and are subject to change.

4.8 AI/ML Training

Using Platform data, including but not limited to certification records, financial data, scheduling information, user profiles, or any other content, to train, develop, fine-tune, or otherwise improve artificial intelligence or machine learning models without the prior written consent of Certivo and all affected data subjects.

4.9 Prohibited Content

Uploading, storing, or transmitting through the Platform:

- (a) Content that is illegal under Canadian federal or provincial law;
- (b) Content that violates the privacy rights of any individual, including content that contravenes PIPEDA, PIPA, or equivalent provincial privacy legislation;
- (c) Content that is defamatory, obscene, threatening, harassing, or discriminatory;
- (d) Content that infringes on the intellectual property rights of any third party; and
- (e) Content that contains personal health information not related to occupational safety training records.

4.10 Reselling Access

Reselling, sublicensing, redistributing, or otherwise providing access to the Platform or any Platform features to third parties without prior written authorization from Certivo. This does not prohibit tenants from providing Client Portal access to their clients in the ordinary course of business.

4.11 Circumventing Security Controls

Attempting to bypass, disable, interfere with, or circumvent any security feature or control implemented by the Platform, including but not limited to:

- (a) TenantGuard multi-tenancy isolation;
- (b) Firestore Security Rules;
- (c) Cloud Function rate limiting (enforceRateLimit);
- (d) Authentication mechanisms, including Firebase Auth brute-force protections;
- (e) Role-based access controls (RBAC);
- (f) Session management and idle timeout controls; and
- (g) Environment separation between development, staging, and production.

---

5. Resource Usage

5.1 Users are expected to use the Platform's computing, storage, and network resources in a reasonable manner consistent with normal business operations of a safety training company.

5.2 Certivo reserves the right to throttle, suspend, or restrict access for any user or tenant whose usage patterns indicate infrastructure abuse, including but not limited to:

- (a) Excessive API calls beyond what is reasonably expected for the tenant's subscription tier;
- (b) Uploading excessively large files or an unreasonable volume of data;
- (c) Running automated processes that consume disproportionate Platform resources; and
- (d) Using the Platform in a manner that degrades performance for other tenants.

5.3 Specific resource limits may vary by subscription tier (Starter at $49/month, Professional at $149/month, and Enterprise at custom pricing). Tenants exceeding their tier's resource allocations may be required to upgrade their subscription.

---

6. Integration Usage

6.1 When using third-party integrations available through the Platform (QuickBooks, Xero, Google Calendar, Stripe), users must comply with the terms of service, acceptable use policies, and privacy policies of each respective third-party provider.

6.2 Certivo is not responsible for any violation of third-party terms arising from a user's actions through the Platform's integration features.

6.3 Users are responsible for maintaining the security of their integration credentials and OAuth tokens. Compromised integration credentials must be reported to Certivo and revoked immediately.

---

7. Email and Communications Usage

7.1 All email communications sent through the Platform, including drip campaigns, batch emails, invoice notifications, and certification expiry reminders, must comply with Canada's Anti-Spam Legislation (CASL), S.C. 2010, c. 23.

7.2 Tenants are responsible for:

- (a) Obtaining express or implied consent from recipients before sending commercial electronic messages through the Platform;
- (b) Ensuring all commercial electronic messages include proper identification of the sender and a functioning unsubscribe mechanism;
- (c) Honoring unsubscribe requests within 10 business days as required by CASL;
- (d) Maintaining records of consent for all recipients; and
- (e) Ensuring the content of all communications is accurate and not misleading.

7.3 Certivo reserves the right to suspend email sending capabilities for any tenant found to be in violation of CASL or engaging in unsolicited bulk messaging.

7A. Community Forum Usage

7A.1 The Community Forum feature is provided for the discussion of topics relevant to safety training, certification management, regulatory compliance, and Platform usage. All Forum content must be relevant to the safety training industry or Platform operations.

7A.2 Users shall not post or transmit through the Forum:

- (a) spam, unsolicited advertising, or promotional content unrelated to safety training;
- (b) content that is hateful, discriminatory, threatening, harassing, or abusive toward any individual or group;
- (c) content that violates the privacy of any individual, including posting personal information without consent;
- (d) content that infringes on the intellectual property rights of any third party; or
- (e) content that is false, misleading, or intended to deceive other users.

7A.3 Certivo reserves the right to moderate, edit, or remove any Forum content that violates this AUP, without prior notice. Repeated violations may result in the suspension or revocation of Forum privileges.

7B. Instructor Portfolio Usage

7B.1 Instructors who publish portfolio profiles on the Platform must ensure that all information presented is **truthful, accurate, and current**, including qualifications, certifications, experience, and course offerings.

7B.2 Instructors shall not:

- (a) misrepresent their qualifications, certifications, or regulatory credentials;
- (b) include false or misleading claims about their experience or training outcomes;
- (c) use another instructor's identity, likeness, or credentials; or
- (d) include content that violates the Acceptable Use Policy or any applicable law.

7B.3 Certivo reserves the right to remove or suspend any instructor portfolio that contains false credentials, misleading information, or content that violates this AUP. Instructors whose profiles are removed for credential misrepresentation may be permanently barred from the Marketplace.

7C. Marketplace Listing Usage

7C.1 All course listings published on the Certification Marketplace must include **accurate descriptions** of course content, duration, prerequisites, certification outcomes, and pricing.

7C.2 Instructors publishing Marketplace listings shall not:

- (a) misrepresent the regulatory status, accreditation, or recognition of a course or certification;
- (b) list courses that the instructor is not qualified or authorized to deliver;
- (c) engage in deceptive pricing practices, including hidden fees or bait-and-switch tactics; or

- (d) publish duplicate, spam, or placeholder listings.

7C.3 Certivo reserves the right to remove non-compliant Marketplace listings without prior notice. Courses that receive consistent negative reviews or fail to meet applicable safety training standards may also be removed at Certivo's sole discretion.

---

8. Enforcement

Certivo reserves the right to investigate any suspected violation of this AUP and to take appropriate action, which may include:

8.1 Warning. For first-time or minor violations, Certivo may issue a written warning to the user or tenant administrator, specifying the violation and required corrective action.

8.2 Suspension. For repeated violations, serious violations, or failure to correct a previously warned violation, Certivo may temporarily suspend the user's or tenant's access to the Platform, in whole or in part, until the violation is resolved.

8.3 Termination. For severe violations, persistent violations after suspension, or violations that pose a risk to other users, the Platform's integrity, or Certivo's legal obligations, Certivo may permanently terminate the user's or tenant's access to the Platform. Termination under this section does not entitle the user or tenant to any refund of prepaid fees.

8.4 Certivo may, at its sole discretion, skip any step in the enforcement process if the severity of the violation warrants immediate action.

8.5 Certivo will cooperate with law enforcement authorities where required by law or where violations involve illegal activity.

---

9. Reporting Violations

If you become aware of any violation of this AUP, please report it to:

Privacy Officer: Aaron Hoyte **Email:** aaron@certivo.ca **Subject Line:** AUP Violation Report

Reports will be reviewed within five (5) business days, and the reporting party will be notified of any action taken, subject to privacy and confidentiality obligations.

---

10. Modifications

Certivo reserves the right to modify this AUP at any time. Material changes will be communicated to users via email or Platform notification at least thirty (30) days prior to the effective date of the change. Continued use of the Platform after the effective date of any modification constitutes acceptance of the modified AUP.

11. Governing Law

This Acceptable Use Policy shall be governed by and construed in accordance with the laws of the Province of Alberta and the federal laws of Canada applicable therein. Any disputes arising under this AUP shall be subject to the exclusive jurisdiction of the courts of the Province of Alberta.

12. Contact Information

Certivo Inc. 4952 Westbrooke Rd. Blackfalds, Alberta, Canada T4M 0L1

Privacy Officer: Aaron Hoyte **Email:** aaron@certivo.ca **Website:** certivo.ca

Last Updated: March 2026 Certivo Inc.