



SOFTWARE AS A SERVICE AGREEMENT

READYCHEK INC. ENTERPRISE SAAS TERMS & CONDITIONS

Document Version: 1.4
Effective Date: August 2026
Governing Law: Ontario, Canada
Data Residency: 100% Canada
Cyber Insurance: \$2,000,000 CAD
Support: support@readychek.com

IMPORTANT – READ THIS SOFTWARE AS A SERVICE AGREEMENT (THIS “AGREEMENT”) CAREFULLY. THIS AGREEMENT IS RELATED TO AND DEEMED INCORPORATED INTO THE PURCHASE AGREEMENT (“PURCHASE AGREEMENT”) BETWEEN READYCHEK INC. (“READYCHEK”) AND THE CLIENT SPECIFIED IN THE PURCHASE AGREEMENT (“CLIENT”). CLIENT’S EXECUTION OF A PURCHASE AGREEMENT REFERENCING THIS AGREEMENT SHALL BE DEEMED CLIENT’S AGREEMENT TO THE TERMS AND CONDITIONS OF THIS AGREEMENT.

■ **1-Hour Availability SLA:** ReadyChek commits to a Mean Time to Restore (MTTR) of one (1) hour during the SaaS Term.

■ **Enterprise Security & \$2M Insurance:** \$2M Cybersecurity Insurance, TLS 1.3 / AES-256 encryption, 24h breach notice.

■ **Canadian Data Residency:** 100% Canadian data storage (PIPEDA compliant) with 6-month post-term audit access.

1. DEFINITIONS

For purposes of this Agreement, the terms below shall have the meanings defined below. Additional terms are defined throughout this Agreement.

1. “Client Content”	means any data, information, trade-marks, logos, files, images, text or other content provided by Client or its authorized users for use with the Software.
2. “SaaS Term”	means the period during which access to the Software and Services is provided by ReadyChek to Client, including Initial Term and Renewal Terms.
3. “Services”	means the hosting, maintenance, system administration, security controls, and support services provided by ReadyChek pursuant to this Agreement.
4. “Software”	means ReadyChek's proprietary commercial vehicle inspection, daily logbook, and fleet compliance software specified in the Purchase Agreement.
5. “Personal Information”	means information about an identifiable individual compiled or stored using the Services, governed by Canadian privacy laws.
6. “User Documentation”	means ReadyChek user manuals, online help guides, and technical specifications relating to the Software.

2. MOBILE AND WEB-BASED LICENSE

ReadyChek grants to Client, and Client accepts, a non-transferable, non-exclusive license to access the Software via the Internet and use the Software and User Documentation as authorized in this Agreement for its internal business operations during the SaaS Term. Client acknowledges that access is mobile and web-based only, hosted by ReadyChek on secure infrastructure.

3. ACCESSIBILITY, ENTERPRISE SECURITY & CANADIAN DATA RESIDENCY

ReadyChek will make the Software available for Client's use on a 24/7 basis, except for scheduled Maintenance Windows. ReadyChek will provide secure administrator credentials and management controls.

3.1 Security Controls & \$2,000,000 Cybersecurity Insurance

ReadyChek maintains administrative, logical, and physical safeguards incorporating role-based access control, least privilege, network segregation, TLS 1.3 data encryption in transit, and AES-256 data encryption at rest. ReadyChek shall procure and maintain in full force throughout the term a **cybersecurity insurance policy with coverage of no less than \$2,000,000 CAD**.

3.2 24-Hour Security & Privacy Breach Protocol

In the event of an actual or suspected security breach, unauthorized data access, or critical vulnerability affecting Client Content or Personal Information, ReadyChek shall:

- a. Notify Client in writing within **twenty-four (24) hours** of discovery;
- b. Conduct an immediate forensics examination to determine scope and impact;
- c. Provide Client with a detailed incident report and corrective action plan within ten (10) calendar days; and
- d. Cooperate fully with Client, regulators, and law enforcement in accordance with applicable Canadian privacy laws (*PIPEDA* / *MFIPPA*).

3.3 100% Canadian Data Residency

ReadyChek shall hold and process all Client Content and Personal Information in secure electronic and physical environments located strictly within **Canada**. Personnel access from outside Canada is prohibited unless required for temporary business travel, in which case prior written notice shall be provided to Client.

4. FEES AND PAYMENT

Client shall pay a Subscription Fee on a monthly or agreed billing schedule as described in the Purchase Agreement. The Subscription Fee is fixed for the Initial Term.

5. TERM AND TERMINATION

5.1 Initial Term & Renewal. The SaaS Term commences on the Commencement Date indicated in the Purchase Agreement and continues until terminated as provided herein.

5.2 Termination for Breach. Either party may terminate for material breach upon ninety (90) days written notice (or thirty (30) days for payment failure) if uncured.

5.3 Termination for Convenience. Either party may terminate upon ninety (90) days written notice without cause.

5.4 Effect of Termination & 6-Month Audit Access. Upon termination for convenience by Client or material breach by Client, Client shall pay outstanding Subscription Fees. Upon termination for any reason, Client shall retain administrative access to the platform for **six (6) months following termination** to perform any required Ministry of Transportation (MTO) or National Safety Code (NSC) facility audits. All completed inspection reports and Hours of Service (HOS) records remain available for download as PDFs through the portal's reporting functionality during this 6-month period. Beyond this 6-month audit window, access shall cease.

6. MAINTENANCE WINDOWS & AVAILABILITY SLA

ReadyChek will announce planned system maintenance fourteen (14) days in advance via email. ReadyChek commits to a **Mean Time to Restore (MTTR) of one (1) hour** in the event of an unscheduled system outage.

7. BACKUPS & DISASTER RECOVERY

ReadyChek maintains off-site automated backups and disaster recovery procedures tested periodically to ensure business continuity.

8. SUPPORT & UPGRADES

ReadyChek provides online, email, and telephone support during the SaaS Term and deploys Software patches and feature updates at no extra cost.

9. INTELLECTUAL PROPERTY & RESTRICTIONS

ReadyChek retains exclusive ownership of the Software, User Documentation, and Work Product. Client retains sole ownership of all Client Content and Personal Information. Client shall not reverse engineer, sublicense, or use the Software beyond authorized internal operations.

10. WARRANTIES AND DISCLAIMERS

ReadyChek warrants that the Software will perform substantially in accordance with User Documentation and Services will be delivered professionally.

Warranty Disclaimer: EXCEPT AS EXPRESSLY STATED HEREIN, THE SOFTWARE AND SERVICES ARE PROVIDED “AS IS”. READYCHEK DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

11. CONFIDENTIALITY & PRIVACY

Both parties agree to safeguard confidential information with reasonable care. Privacy Law obligations under Canadian PIPEDA survive termination.

12. INDEMNIFICATION & LIABILITY

ReadyChek indemnifies Client against Canadian patent or copyright infringement claims arising from Software use.

LIMITATION OF LIABILITY: EXCEPT FOR INDEMNIFICATION OBLIGATIONS, READYCHEK’S MAXIMUM LIABILITY SHALL NOT EXCEED THE TOTAL FEES PAID BY CLIENT IN THE TWELVE (12) MONTH PERIOD PRECEDING THE CLAIM. IN NO EVENT SHALL READYCHEK BE LIABLE FOR INDIRECT OR CONSEQUENTIAL DAMAGES.

13. GENERAL PROVISIONS

Governed by the laws of the Province of Ontario and Canada. Amendments must be in writing signed by authorized representatives of both parties.

SCHEDULE A – ENTERPRISE INFORMATION SECURITY SAFEGUARDS

- 1. **Security Governance:** ReadyChek maintains formal information security policies and procedures reviewed annually.
- 2. **\$2,000,000 Cybersecurity Insurance:** Procures and maintains a minimum \$2M CAD cybersecurity insurance policy.
- 3. **24-Hour Breach & Critical Patch SLA:** Written notice within 24 hours of suspected breaches or critical vulnerabilities; 24h remediation SLA.
- 4. **Access Controls:** Role-based access control (RBAC), multi-factor authentication for administrative access, and immediate revocation upon employee termination.
- 5. **Penetration Testing:** Annual internal control reviews and periodic external vulnerability scans.
- 6. **Data Destruction:** Secure data scrubbing and disposal meeting DOD/NIST standards upon contract expiry.

SCHEDULE B – CANADIAN PRIVACY & DATA PROTECTION

- 1. **100% Canadian Data Residency:** Personal Information hosted exclusively within Canadian data centres.
- 2. **PIPEDA / MFIPPA Compliance:** Strict compliance with Canadian federal and provincial privacy legislation.
- 3. **24-Hour Incident Notice:** Immediate written notice of any privacy inquiries, loss, or unauthorized access.
- 4. **Data Return & Officer Certification:** Upon contract expiry, all Personal Information is returned or securely destroyed with an officer’s certificate of destruction upon request.