

CLOUD BACKUP SERVICES AGREEMENT

Cloud Backup for Point-of-Sale (POS) Database

Last Updated: May 4, 2026

This Cloud Backup Services Agreement (“Agreement”) is entered into as of the Effective Date set forth below by and between:

Provider:

Armagh Cash Register Limited

operating as Armagh POS Solutions

180 Dundurn Street South, Hamilton, Ontario, Canada L8P 4K3

(“Provider”, “Armagh”, “we”, or “us”)

Customer:

[Customer Legal Name]

operating as [Customer Operating As Name]

[Customer Address, City, Province, Postal Code]

(“Customer”, “you”, or “your”)

Effective Date: [Insert Date, e.g., MM/DD/YYYY or upon execution of applicable Service Order]

1. Introduction and Purpose

This Agreement defines the terms and conditions under which Provider will provide Cloud Backup Services (the “Backup Services”) to Customer. The Backup Services consist of resold commercial-grade cloud backup solutions, configured, monitored, and managed by Provider using Connectwise RMM tools, primarily for the backup of Customer’s Point-of-Sale (POS) database residing on on-premises servers.

This Agreement is intended to be read in conjunction with, and incorporates by reference, the Provider’s current **Privacy Policy**, **Service Level Agreement (“SLA”)**, **Warranty Agreement**, and **Network Services Agreement** (collectively, the “Referenced Agreements”), available at www.armaghpos.com/legal. In the event of any conflict between this Agreement and the Referenced Agreements, or between this Agreement and any applicable Master Services Agreement, Service Order, Quotation, Sales Order, or other Underlying Agreement between the parties (the “Underlying Agreement”), the terms of the Underlying Agreement shall control. This approach avoids unnecessary duplication and ensures consistency across all customer documentation.

Provider typically offers the Backup Services for systems that include an on-premises server hosting a POS database that should be protected. The service is quoted, sold via Sales Order, and billed monthly as part of Customer’s Pre-Authorized Payment (PAP) arrangement.

2. Definitions

For purposes of this Agreement:

- **“Backup Services” or “Services”** means the cloud backup services provided under this Agreement, including initial configuration, ongoing monitoring via RMM, management of cloud backup jobs, and basic restore assistance for the Covered Data.
- **“Covered Data”** means Customer’s Point-of-Sale (POS) database files and related data on the designated on-premises server(s) identified in the applicable Service Order or Sales Order. *Unless Customer provides written direction otherwise, only the POS Database is backed up under this Agreement.*

- “**Monthly Service Fee**” means the recurring monthly fee for the Backup Services as set forth in the applicable Service Order or Sales Order, typically billed monthly in advance via Pre-Authorized Payment (PAP) as part of Customer’s regular monthly billing with Provider.
- “**Service Order**” or “**Sales Order**” means the quotation, order form, or document accepted by Customer that specifies the scope, pricing, Covered Data, and any specific configuration for the Backup Services.
- Other terms defined in the Referenced Agreements (including “Business Day,” “Incident,” “Initial Response Time,” “Force Majeure,” etc.) shall have the same meanings herein unless otherwise specified.

3. Scope of Backup Services

Subject to Customer’s timely payment of the Monthly Service Fee and compliance with this Agreement and the Underlying Agreement, Provider shall provide the Backup Services for the Covered Data during the term of this Agreement:

- **Configuration & Setup:** Initial setup and configuration of cloud backup jobs targeting the POS Database on Customer’s designated on-premises server(s), following industry best practices for database-consistent backups where supported by the POS application.
- **Monitoring & Management:** Ongoing monitoring of backup job status, success/failure alerts, and basic management via Connectwise RMM tools. Provider will use commercially reasonable efforts to maintain backup schedules and retention as quoted.
- **Cloud Storage:** Secure offsite storage of backup images in Vendor’s cloud infrastructure (subject to Vendor’s terms of service and any data residency options selected at time of quote).
- **Restore Assistance:** Basic assistance with restoring the POS Database from backup in the event of data loss or corruption, provided in accordance with SLA response priorities. Complex disaster recovery, frequent test restores, or full system restores may be billable separately.

Important Scope Limitations:

- Unless Customer provides **written direction** (email acceptable if confirmed) specifying additional data, folders, files, or systems to include, Provider will backup **ONLY the POS Database**. Any request to backup additional data requires a separate quote and Sales Order/Service Order at additional cost.
- The Backup Services do **not** include backup of operating system files, applications, user profiles, email systems, non-POS databases, or any other data unless explicitly added via written direction and additional Service Order.
- Provider does not guarantee successful completion of every backup job, successful restoration of all data, or absence of data loss. The service is provided on a “best efforts” basis.

4. No Guarantee Against Data Loss; Disclaimer

CUSTOMER ACKNOWLEDGES AND AGREES THAT PROVIDER DOES NOT GUARANTEE AGAINST DATA LOSS.

Many factors affecting backup success and data recoverability are outside Provider’s reasonable control, including but not limited to: Customer’s server hardware or software stability, changes to the POS application or database structure, network connectivity or firewall issues, power failures or surges, ransomware or malware attacks, Vendor’s platform outages or changes, Connectwise RMM performance, database locking or corruption at backup time, and Force Majeure events.

Cloud backup is a valuable risk mitigation tool used in conjunction with but not as a substitute for proper on-site backups, system redundancy, staff training, system and network security protections including but not limited to anti-virus and anti-malware, firewalls, regular updates of software applications and operating systems, network security, regular testing, and or a comprehensive disaster recovery plan.

Provider strongly recommends that Customer maintains independent local backups whenever possible and periodically test restore procedures.

THE BACKUP SERVICES ARE PROVIDED “AS IS” AND “AS AVAILABLE.” Except as expressly set forth in this Agreement or the Referenced Agreements, Provider makes no warranties, express or implied, including but not limited to warranties of merchantability, fitness for a particular purpose, non-infringement, or that backups will be uninterrupted, error-free, complete, or that any specific data will be recoverable. Customer’s sole remedies for issues with the Backup Services are as set forth in the SLA (Section 6 – Remedies) and the Underlying Agreement.

5. Service Levels and Support

Provider will acknowledge and respond to properly submitted support requests related to the Backup Services (e.g., backup job failures, restore requests, configuration questions) in accordance with the priority levels, Initial Response Times, Resolution Targets, and Status Update frequencies set forth in **Section 4.2 of the Service Level Agreement (SLA)**, which is incorporated herein by reference. Critical (P1) issues must be reported by telephone to 1-888-528-5903 to ensure the fastest response.

Provider will use commercially reasonable efforts to configure backup jobs for reliability (e.g., appropriate scheduling, notifications, and retention policies as quoted). However, specific backup success rates, Recovery Point Objectives (RPO), or Recovery Time Objectives (RTO) are targets only and are not guaranteed.

6. Customer Responsibilities

In addition to the Customer Responsibilities set out in Section 7 of the SLA and Section 9 of the Warranty Agreement (both incorporated by reference), Customer agrees to:

- Identify and confirm in the Service Order/Sales Order the specific on-premises server(s) and exact location/path of the POS Database to be backed up.
- Provide **written direction** (email or signed document) if any data, folders, or systems beyond the POS Database are to be included in the backup. A separate quote and Service Order will be required at additional cost.
- Ensure the designated server(s) remain powered on, connected to a stable internet connection, and accessible during scheduled backup windows. Promptly notify Provider of any server changes, POS software updates, database migrations, network changes, or other modifications that may affect backup operations.
- Maintain valid administrative credentials and remote access permissions as required for Provider to configure and monitor the backup jobs via Connectwise RMM.
- Periodically test restores (or request Provider assistance for test restores) to verify that backups are recoverable and meet business needs.
- Pay all applicable Monthly Service Fees on time via the Pre-Authorized Payment (PAP) process as part of regular monthly billing.

7. Provider Responsibilities

Provider commits to:

- Use commercially reasonable efforts to configure, schedule, monitor, and maintain the cloud backup jobs for the Covered Data using Connectwise RMM tools.
- Respond to Backup Services-related Incidents in accordance with the SLA priority and response targets.
- Protect Customer access credentials and any data in transit or at rest in the backup infrastructure in accordance with the Privacy Policy and applicable Canadian privacy laws (PIPEDA).

- Provide reasonable assistance with data restores when requested, subject to SLA terms and scope.
- Invoice and collect the Monthly Service Fee monthly via Customer's PAP billing arrangement.

8. Billing, Payment, and Fees

The Monthly Service Fee for the Backup Services shall be as set forth in the applicable Service Order or Sales Order. Fees are typically invoiced monthly in advance and collected via Pre-Authorized Payment (PAP) as part of Customer's established monthly billing cycle with Provider, unless otherwise agreed in writing.

Provider reserves the right to suspend or terminate the Backup Services (including monitoring, new backups, and restore assistance) for non-payment after providing written notice and a reasonable cure period (e.g., 10 business days). Late payments may be subject to interest or administrative fees as permitted by the Underlying Agreement or applicable law.

Provider may adjust the Monthly Service Fee upon renewal or with reasonable advance written notice for material changes in scope, storage consumption, or costs; such changes will be documented in a revised Service Order and will apply prospectively.

9. Term and Termination

This Agreement commences on the Effective Date and continues on a month-to-month basis (or for the term specified in the applicable Service Order) until terminated by either party upon thirty (30) days' prior written notice to the other party (email or support portal notice is sufficient if confirmed in writing). Either party may terminate immediately for material breach by the other party if such breach remains uncured for fifteen (15) days after written notice.

Upon termination or expiration of this Agreement or the applicable Service Order:

- All Backup Services, including monitoring, new backup jobs, and restore assistance, shall immediately cease.
- Customer remains responsible for any accrued but unpaid Monthly Service Fees or other charges.
- Provider will, upon reasonable request and subject to the Cloud Vendor's terms, provide limited assistance to export or transfer existing backup data (additional fees may apply). Provider has no obligation to retain or provide access to backups after a reasonable wind-down period following termination.
- Customer acknowledges that upon termination, Provider will disable backup jobs, and any remaining cloud backups will be subject to Vendor's data retention and deletion policies. Customer should confirm retention needs with Provider prior to termination.

10. Exclusions and Limitations of Liability

This Agreement and the Backup Services do not cover, and Provider shall have no obligation or liability for, any of the following (in addition to the exclusions set forth in the Referenced Agreements):

- Backup failures, incomplete backups, or inability to restore due to issues with Customer's server hardware/software, POS application changes, database corruption or locking, insufficient storage/disk space, network interruptions, or changes made without Provider's prior knowledge.
- Data loss, corruption, or unrecoverability caused by ransomware, malware, hardware failure, user error, accidental deletion, or any cause not directly resulting from Provider's gross negligence or willful misconduct.
- Third-party platform issues, including Vendor's cloud service outages, performance degradation, API changes, or modifications to Vendor's terms of service (Customer's use of the Vendor's

platform is also subject to the Vendor's End User License Agreement and terms, which Customer accepts by purchasing and using the service).

- RMM or other management tool outages, performance issues, or limitations.
- Any data, files, or systems not explicitly designated as Covered Data in the applicable Service Order or Sales Order.
- Costs of recreating lost data, lost profits, business interruption, regulatory fines, or other consequential, incidental, special, or punitive damages arising from data loss or backup issues.

Liability Limitation: Provider's aggregate liability arising out of or related to this Agreement or the Backup Services shall not exceed the total Monthly Service Fees paid by Customer to Provider for the specific Backup Services giving rise to the claim during the twelve (12) months preceding the claim. In no event shall Provider be liable for indirect, incidental, special, consequential, or punitive damages, including lost profits, data loss, or business interruption, regardless of the form of action or theory of liability. For complete limitations on liability and additional remedies, please refer to the Underlying Agreement and the Referenced Agreements (particularly Section 8 of the Warranty Agreement and Section 6 of the SLA).

11. Privacy and Data Protection

During the course of providing Backup Services, Provider may have access to Customer's systems, POS Database, configurations, and backup images (which may contain personal information, transaction data, or other sensitive business data). Provider will collect, use, disclose, and safeguard any personal information in accordance with its **Privacy Policy** (available at www.armaghpos.com/legal) and applicable Canadian privacy laws, including PIPEDA.

Customer acknowledges that:

- Backups of the POS Database may include sensitive transaction data, customer information, or other personal data subject to privacy laws.
- It is Customer's sole responsibility to ensure its POS system and database are configured appropriately, to comply with its own privacy and data protection obligations, and to obtain any necessary consents from data subjects.
- Provider is not responsible for the content or accuracy of the data being backed up.
- For full details on data handling practices, please refer to the Privacy Policy.

12. Governing Law and Dispute Resolution

This Agreement shall be governed by and construed in accordance with the laws of the Province of Ontario and the federal laws of Canada applicable therein, without regard to conflict of law principles. Any dispute arising out of or relating to this Agreement shall be resolved exclusively in the courts of the Province of Ontario sitting in the City of Hamilton or Toronto, and each party irrevocably attorns to the jurisdiction of such courts, as more particularly set out in Section 11 of the SLA.

13. General Provisions

This Agreement, together with the Underlying Agreement and the Referenced Agreements (Privacy Policy, SLA, Warranty Agreement, and Network Services Agreement), constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior or contemporaneous warranties, representations, or agreements (whether written or oral) relating to the Backup Services. If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect. Neither party may assign this Agreement without the prior written consent of the other, except that Provider may assign to an affiliate or successor in connection with a merger or sale of substantially all assets. This Agreement may be executed in counterparts, including electronic signatures, each of which shall be deemed an original.

No modification of this Agreement shall be valid unless in writing and signed by authorized representatives of both parties.

IN WITNESS WHEREOF, the parties have executed this Cloud Backup Services Agreement as of the Effective Date first written above.

PROVIDER: Armagh Cash Register Limited o/a Armagh POS Solutions Per: _____ Name: _____ Title: _____ Date: _____	CUSTOMER: [Customer Legal Name] o/a [Customer Operating As Name] Per: _____ Name: _____ Title: _____ Date: _____
--	---

— End of Cloud Backup Services Agreement —

Armagh POS Solutions — Remarkable POS solutions for retail, grocery & hospitality since 1979.