REMOTE MONITORING AND MANAGEMENT SERVICES AGREEMENT

Remote Monitoring and Management (RMM) Services for Point-of-Sale Systems

Last Updated: May 5, 2026

This Remote Monitoring and Management 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")

and

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 Sales Order]

1. Introduction and Purpose

This Agreement defines the terms and conditions under which Provider will provide Remote Monitoring and Management Services (the "RMM Services") to Customer. The RMM Services (also commonly referred to as Proactive Computer Management) consist of resold remote monitoring and management platform services, configured, monitored, and managed by Provider, primarily for Customer's Windows-based Point-of-Sale (POS) terminals and Database Servers. The RMM Services include deployment of an endpoint protection solution as part of the managed service.

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, Cloud Backup Services 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 RMM Services for systems that include Windows-based POS terminals and/or on-premises servers hosting POS databases. The service is quoted, sold via Sales Order, and billed monthly as part of Customer's Pre-Authorized Payment (PAP) arrangement.

Note that Provider uses the RMM platform to facilitate management of certain other services, such as Cloud Backup Services where applicable.

2. Definitions

For purposes of this Agreement:

- **""RMM Services" or "Services""** means the remote monitoring and management services provided under this Agreement, including initial deployment and configuration of the RMM agent and endpoint protection on designated devices, ongoing monitoring, alerting, patch management, remote assistance, and basic remediation for the Covered Devices.
- **""Covered Devices""** means the specific Windows-based Point-of-Sale (POS) terminals and Database Servers identified in the applicable Service Order or Sales Order. Unless Customer provides written direction otherwise, only POS terminals and Database Servers are included under this Agreement.
- **""Endpoint Protection""** means the endpoint security solution (including anti-malware capabilities) deployed and managed as part of the RMM Services.
- **""Monthly Service Fee""** means the recurring monthly fee for the RMM 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 Devices, and any specific configuration for the RMM 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 RMM 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 RMM Services for the Covered Devices during the term of this Agreement:

- **Deployment & Configuration:** Initial deployment of the RMM agent and Endpoint Protection on the designated Covered Devices (Windows OS currently supported by Microsoft), following industry best practices.
- **Monitoring & Management:** Ongoing remote monitoring of device health, performance, security status, and alerts via the RMM platform. Includes patch management for supported operating systems and applications where feasible, and basic remote troubleshooting and remediation.
- **Endpoint Protection Management:** Management of the Endpoint Protection solution, including policy enforcement, updates, and response to detected threats on a best-efforts basis.

- **Integration with Other Services:** Use of the RMM platform to support management of Provider's other services, such as Cloud Backup Services (as described in the Cloud Backup Services Agreement), where applicable to the Covered Devices.
- **Remote Support:** Remote assistance for issues related to the Covered Devices, in accordance with SLA priorities.

Important Scope Limitations:

- Unless Customer provides written direction (email acceptable if confirmed) specifying additional devices or systems to include, Provider will deploy RMM and Endpoint Protection ONLY on the POS terminals and Database Servers identified as Covered Devices. Any request to cover additional machines (which may include alternative or additional endpoint protection solutions) requires a separate quote and Sales Order/Service Order at additional cost.
- The RMM Services do not include management of non-Windows devices, unsupported operating systems, or devices not explicitly designated as Covered Devices.
- Provider does not guarantee successful prevention or remediation of all security threats, viruses, malware, or ransomware. The service is provided on a "best efforts" basis.

3.1 Remote Access Configuration (ScreenConnect)

By default, Provider configures the remote access component of the RMM Services in unattended mode. This allows Provider's technicians to connect to Covered Devices for the purposes of technical support, maintenance, troubleshooting, software updates, and staff training without requiring real-time customer intervention or consent for each session. This default configuration is selected because the majority of Provider's customers prefer the convenience, operational efficiency, and reduced response times it affords. Customers have consistently expressed trust in Provider's technicians and processes and value the higher level of service efficiency that unattended remote access provides.

If Customer prefers attended remote access mode (in which Customer must actively consent to and participate in each remote connection, typically by navigating to Provider's secure Technical Support Portal at https://armaghpos.com/services/system-support/ and granting consent for the specific session), Customer must notify Provider in writing. Upon receipt of such written request, Provider will configure (or reconfigure) the remote access utility on the affected Covered Devices to attended mode, or modify the existing unattended setup, so that technician access requires Customer's express consent and active participation for every connection.

Provider recommends that Customer carefully evaluate its operational requirements, internal security policies, and any applicable regulatory or compliance obligations (including PCI DSS requirements applicable to remote access in cardholder data environments) when deciding between unattended and attended remote access modes. Provider will implement Customer's written preference at no additional charge.

4. No Guarantee of Security Outcomes; Disclaimer

CUSTOMER ACKNOWLEDGES AND AGREES THAT PROVIDER DOES NOT GUARANTEE PROTECTION AGAINST VIRUSES, MALWARE, RANSOMWARE, OR OTHER CYBER THREATS.

Many factors affecting device security and threat prevention are outside Provider's reasonable control, including but not limited to: Customer's network environment, user behavior, phishing or social engineering attacks, zero-day vulnerabilities, configuration changes made without Provider's knowledge, third-party software conflicts, internet connectivity, and Force Majeure events.

The RMM Services and Endpoint Protection are valuable risk mitigation tools used in conjunction with but not as a substitute for proper security hygiene, staff training, network firewalls, regular updates, strong access controls, insurance, and a comprehensive cybersecurity plan. Provider strongly recommends that Customer maintains good security practices and considers additional layers of protection as needed.

THE RMM 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 the Services will be uninterrupted, error-free, or that any specific threat will be prevented or remediated. Customer's sole remedies for issues with the RMM 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 RMM Services (e.g., device alerts, remediation needs, 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 maintain the RMM platform connectivity and monitoring for Covered Devices. However, specific monitoring coverage, alert response times, or security outcomes 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 Covered Devices (POS terminals and Database Servers) to be included.
- Provide written direction (email or signed document) if any additional devices or systems beyond the standard Covered Devices are to be included in the RMM Services. A separate quote and Sales Order will be required and at additional cost.
- Ensure the designated devices remain powered on, connected to a stable internet connection, and accessible for remote management. Promptly notify Provider of any device changes, operating system upgrades/downgrades, network changes, or other modifications that may affect RMM operations.

- Maintain valid administrative credentials and remote access permissions as required for Provider to deploy, configure, and monitor the RMM agent and Endpoint Protection.
- Follow security best practices, including not disabling Endpoint Protection or RMM components without Provider's knowledge, and promptly reporting any suspected security incidents.
- 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 deploy, configure, monitor, and maintain the RMM agent and Endpoint Protection on the Covered Devices using the RMM platform.
- Respond to RMM Services-related Incidents in accordance with the SLA priority and response targets.
- Protect Customer access credentials and any data accessed during monitoring or remediation in accordance with the Privacy Policy and applicable Canadian privacy laws (PIPEDA).
- Provide reasonable remote assistance and basic remediation for issues detected on Covered Devices, 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 RMM 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 RMM Services (including monitoring, management, and Endpoint Protection) 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, number of devices, or costs; such changes will be documented in a revised Sales 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 Sales 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 Sales Order:

- All RMM Services, including monitoring, management, Endpoint Protection deployment/management, and remote support, shall immediately cease. The RMM agent and Endpoint Protection may be automatically or manually uninstalled from Covered Devices.
- Customer remains responsible for any accrued but unpaid Monthly Service Fees or other charges.
- Provider has no obligation to retain monitoring data or provide access after a reasonable wind-down period following termination. Customer should confirm any data export needs with Provider prior to termination.

10. Exclusions and Limitations of Liability

This Agreement and the RMM 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):

- Security incidents, data breaches, malware infections, ransomware attacks, or other cyber threats, or any resulting data loss, business interruption, or damages, except to the extent directly caused by Provider's gross negligence or willful misconduct in the performance of the RMM Services.
- Failures or issues arising from Customer's network, hardware, software configurations, user actions, unsupported operating systems, or changes made without Provider's prior knowledge.
- Third-party platform issues, including RMM platform outages, performance degradation, API changes, or modifications to the underlying platform terms (Customer's use is also subject to the applicable End User License Agreement and terms of the RMM and Endpoint Protection providers, which Customer accepts by purchasing and using the service).
- Any devices, systems, or data not explicitly designated as Covered Devices in the applicable Service Order or Sales Order.
- Costs of remediation beyond basic remote support, lost profits, regulatory fines, or other consequential, incidental, special, or punitive damages arising from security issues or service limitations.

Liability Limitation: Provider's aggregate liability arising out of or related to this Agreement or the RMM Services shall not exceed the total Monthly Service Fees paid by Customer to Provider for the specific RMM 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 RMM Services, Provider may have access to Customer's systems, devices, configurations, logs, and potentially 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:

- Monitoring may involve collection of device telemetry, performance data, security events, and other operational information.

- It is Customer's sole responsibility to ensure its systems are configured appropriately to comply with its own privacy and data protection obligations.
- Provider is not responsible for the content or accuracy of data on monitored devices.
- 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, Cloud Backup Services 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 RMM 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 Remote Monitoring and Management Services Agreement as of the Effective Date first written above.

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

— End of Remote Monitoring and Management Services Agreement —

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