

Managed Services Attachment

Cambium Data, Inc. • 6542 S 118th St, Omaha, NE 68137

Effective Date: September 25, 2026

Version 1.0

This Managed Services Attachment (this "Attachment") applies when an Order between Cambium Data, Inc. ("Cambium") and Client lists managed IT services. It forms part of the Agreement described in Cambium's Master Services Agreement (the "MSA"). Capitalized terms not defined here have the meanings given in the MSA. If this Attachment and the MSA conflict on a matter specific to Managed Services, this Attachment controls as provided in MSA Section 1.2. The MSA's terms on lawful and high-risk use (Section 7.9), declined recommendations (Section 7.4), unsupported systems (Section 7.6), suspension (Section 5), and security (Section 8) apply fully to the Managed Services and are not repeated here.

1. Scope of Managed Services

1.1 What is included

Cambium will provide the managed services, service tier, and covered quantities listed in the Order (the "Managed Services"). Depending on the plan you choose, the Managed Services may include help desk support, remote monitoring and management of covered devices, patch management, endpoint protection, email security, backup management, network device management, vendor coordination, documentation, and periodic technology reviews. Only the items listed in the Order are included. Adding services requires a new or amended Order.

1.2 Covered users and devices

The Order states the number of covered users, devices, servers, sites, and licenses. For this Attachment:

- a "User" is an individual employee, contractor, or agent of yours whom you authorize to use covered systems and who has a unique login. Your customers and the public are not Users;
- a "Device" is a workstation, laptop, server, network appliance, printer, mobile device, or other hardware listed or described as covered in the Order, whether owned by you or supplied by Cambium, along with the operating system that runs it.

1.3 Help desk hours and after-hours support

Help desk support is available during Business Hours through the channels listed in the Order (for example, phone, email, or our client portal). Outside Business Hours, support is intended for urgent problems, such as an outage of a critical system or a suspected Cyber Event, and is billed as described in the Order or MSA Section 4.5 unless your plan includes after-hours coverage.

1.4 Remote first, on-site when needed

We resolve most issues remotely. When we determine that a problem cannot reasonably be solved remotely, we will schedule on-site support at your covered location. On-site visits are included only if your Order says so; otherwise they are billed at our standard rates, including reasonable travel time for locations outside the Omaha metropolitan area.

1.5 Response targets

We aim to meet the response targets below during the hours that apply to your plan. "Response" means a Cambium technician has acknowledged the request and begun work, not that the issue is resolved. These are good-faith targets, not guarantees, and missing a target is not a breach of the Agreement unless an Order provides specific service credits.

Priority	Example	Target response
Critical	Business-wide outage, suspected Cyber Event, server down	1 hour
High	Several users or a key application affected, no workaround	4 Business Hours
Normal	Single user issue, workaround available	1 Business Day
Low	Requests, questions, scheduled changes	3 Business Days

1.6 Maintenance windows

Routine maintenance, patching, and reboots take place during maintenance windows that we will communicate to you. Some systems may be unavailable during those windows. We will give at least two (2) Business Days' notice of non-routine maintenance that is expected to cause noticeable downtime, except in an emergency.

2. Onboarding and Minimum Standards

2.1 Onboarding

Before the recurring Managed Services start, we will perform an onboarding project to inventory your environment, install our tools, collect documentation, and set up access. Any onboarding fee stated in the Order is invoiced at signing, and we may wait to begin onboarding until it is paid.

2.2 Backups before we start

Before we install tools or make changes during onboarding, you will confirm that you have a current, complete backup of the systems we will be working on, unless the Order makes Cambium responsible for taking that backup. We may rely on your confirmation without checking the backup ourselves, and we are not responsible for data loss during onboarding that a current, restorable backup would have prevented.

2.3 Minimum standards

To be covered, your environment must meet the following standards (the "Minimum Standards"), or you must agree to bring it up to them within a timeline in the Order:

- all servers, workstations, and laptops run an operating system that is still supported by its manufacturer and receives security updates;
- every application is legitimately licensed and still maintained by its publisher;
- your internet connection is protected by a business-class firewall with an active support and security subscription;
- MFA is enabled for email, remote access, and administrative accounts;

- Cambium's endpoint protection and monitoring agents can be installed on all covered Devices;
- a backup solution exists for business-critical data (Cambium's, if in the Order, or yours); and
- Cambium has administrative access as described in Section 4.

Clients subject to specific rules may need additional controls. For example, healthcare clients need centralized identity management (such as Microsoft Entra ID or Active Directory), and clients that accept payment cards need their payment systems separated from their general and guest networks.

2.4 Bringing the environment up to standard

Work and purchases needed to meet the Minimum Standards are not included in recurring Fees. We will quote them separately.

2.5 If the environment falls below standard

If a Device or system stops meeting the Minimum Standards, we will tell you and recommend a fix. If the issue is not fixed within five (5) Business Days after our written notice, we may remove the affected item from coverage or suspend the affected Managed Services until it is fixed; for an active and serious security risk, such as a disabled firewall or missing MFA on an administrator account, we may act sooner under MSA Section 5.1(b). Recurring Fees continue during that suspension. If the problem affects your environment as a whole and is not fixed within thirty (30) days after our notice, we may terminate this Attachment for cause under MSA Section 6.4.

3. How We Work Together

3.1 Your contact

You will designate a primary contact and a backup who can approve changes, purchases, and user additions or removals. We may rely on instructions from these contacts.

3.2 User changes

You will tell us promptly, and in any event within one (1) Business Day, when a User leaves your organization so we can disable their access. We are not responsible for access that stays active because we were not told, or for what a former User does with that access, and any cleanup work that results is billable.

3.3 Changes to your environment

Please tell us in advance about any significant planned change to your network, systems, or applications, such as a new line-of-business application, an office move, a new internet provider, or new equipment, so that we can comment and plan. Changes that you or another vendor make without telling us may cause problems that are outside the scope of the Managed Services. Researching, evaluating, designing, and implementing significant changes, including reviewing products or vendors you are considering, is project work, billed separately.

3.4 Server and network hardware changes

Please do not upgrade, repair, or replace servers or network equipment, or allow another vendor to do so, without first coordinating with us.

3.5 Software media and keys

You will keep, and give us when asked, installation media, license keys, and vendor account information for software that Cambium did not provide.

3.6 Acting on your behalf with vendors

You authorize Cambium to act as your agent to contact your internet, phone, software, and hardware vendors to open support tickets, check the status of services, and order services you have approved. We will not sign contracts in your name without your written approval. Resolving billing disputes with your vendors is not included.

4. Credentials and Administrative Access

4.1 Administrative accounts

To manage your environment securely and keep a reliable record of changes, Cambium will control the administrator-level accounts for covered systems while the Managed Services are in effect, including domain, firewall, and cloud-tenant global administrator accounts (such as Microsoft 365 global admin). Other people, including your staff and other vendors, will not be given administrator access unless we agree in writing, because unmanaged administrative access is a leading cause of security incidents and makes it impossible for us to stand behind the environment.

4.2 Emergency access

If your Order includes it, or if we agree to your written request, we will set up one emergency ("break-glass") administrator account for each of your cloud tenants, with credentials stored in a sealed or vaulted form that an officer you name can retrieve. Any use of that account must be reported to us promptly. We are not responsible for changes made or problems caused by use of emergency access, and any work needed to correct them is billable.

4.3 User credentials

Individual user login credentials belong to you. We will not withhold them.

4.4 Release at the end of service

When the Managed Services end, we will transfer administrator credentials for your systems and tenants to you or your new provider as part of Off-Boarding, once all Fees then due (including any early termination fee, remaining committed Third-Party Service charges, and Off-Boarding charges) have been paid. Until those amounts are paid, we may postpone the transfer of administrator rights and other non-essential Off-Boarding work, but we will not use that delay to block you from reaching your own Client Data in your own tenants or systems.

4.5 Cambium's own tool accounts

To be clear about the three kinds of credentials: (a) administrator credentials for your own systems and tenants are handled under Sections 4.1 and 4.4; (b) individual user credentials are yours under Section 4.3; and (c) logins to the tools Cambium licenses for its own use in delivering services, such as our remote monitoring, ticketing, documentation, and security platforms, belong to Cambium and are never released to clients.

5. Cambium-Supplied Tools, Equipment, and Third-Party Components

5.1 Right to use

During the Service Term, you may use the software, cloud services, and Equipment we provide as part of the Managed Services, solely for your internal business purposes. Some of these are hosted by third parties. Cambium keeps all rights in its tools and in Cambium Materials, and you receive no other rights. MSA Section 11 applies. In addition, you will not frame or mirror any Cambium portal, give third parties access to our tools or portals, or remove proprietary notices.

5.2 Equipment

Equipment listed in the Order is provided on a rental basis. Unless the Order says otherwise, its monthly Fee includes the hardware, its operating software, and the labor to install and maintain it. Only Cambium may service, move, or reconfigure Equipment, and you will not connect third-party accessories to it without our consent. You are responsible for backing up any business data stored on Equipment. Equipment remains Cambium's property at all times and must be returned when the Order ends, as described in MSA Section 11.1.

5.3 Site preparation

If an Order includes installing Equipment or cabling, you will provide suitable space, power circuits, cable pathways, environmental conditions, and access to the premises, and you are responsible for any building work, permits, and landlord approvals. We are not required to make structural changes or to restore your premises when Equipment is removed, other than repairing damage caused by our negligence.

5.4 Third-party components and support

Cambium provides front-line support for the Third-Party Services included in your Managed Services, and escalates to the supplier when needed. Suppliers' warranties and service commitments come from the suppliers, not Cambium. You consent to our sharing your name, contact details, and service information with suppliers when their terms require it or when needed to deliver or support the Third-Party Service.

5.5 Software publisher terms

Some publishers, including Microsoft, require that their customer terms be accepted by the end customer. By using licenses we provide, you agree to the publisher's customer terms, which are linked from the Schedule of Third-Party Services. Where a publisher's terms require it, the publisher may enforce its license terms directly against you. Where its terms allow, a publisher may verify your compliance, and you will cooperate with that verification. If a publisher reasonably believes you are not complying with its terms, we will cooperate with the publisher to investigate and correct the issue.

5.6 License quantities and commitments

Many subscriptions we resell, such as annual-term Microsoft 365 licenses, can be increased at any time but cannot be reduced or cancelled until the end of their commitment period. You are responsible for all license commitments we make at your request, for their full term, even if you reduce users or end the Managed Services early.

6. Security, Backup, and Incident Support

6.1 Security tools

If your plan includes endpoint protection, email security, DNS filtering, security monitoring, or similar tools, we will deploy and maintain them on covered Devices and respond to alerts under the response targets in Section 1.5. MSA Sections 7.2 and 8 apply to all security work.

6.2 Patch management

If your plan includes patching, we will apply operating-system and supported third-party application updates on a routine schedule, generally after a short testing period, and will apply critical fixes more quickly when warranted. The approval and risk rules in MSA Section 7.3 apply. We are not responsible for defects in patches released by manufacturers. If an update that we deployed through the patching service causes a problem on a covered Device, rolling it back is included; recovery work beyond a rollback is billable under Section 7.2.

6.3 Backup services

If your plan includes backup, the Order will describe what is backed up, how often, and how long copies are kept. We will monitor backup jobs, address failures within the response targets, and perform a test restore at least quarterly. Backups can fail for reasons outside our control, so we do not guarantee that every file can be recovered or that restores will finish within a particular time. If your plan does not include backup, you are responsible for backing up your data.

6.4 Incident support

MSA Section 8.4 describes the incident triage included in recurring Fees. Breach-notification planning, forensic investigation, rebuilding systems, and extended recovery work are billable and may require a separate Order.

7. What the Managed Services Do Not Cover

7.1 Conditions outside our control

We are not responsible for failures or delays in the Managed Services to the extent caused by:

- hardware or software that is out of warranty, unsupported, or not in working order;
- changes, repairs, or installations made by you, your other vendors, or anyone else other than Cambium without our approval;
- defects in hardware, software, or Third-Party Services that Cambium did not cause;
- resources, systems, or vendors that Cambium does not manage;
- your decision to prioritize or delay tasks differently than we recommended;
- a force majeure event under MSA Section 17.3;
- actions or inaction by you or your Users, including failure to meet your responsibilities under the Agreement;
- loss of internet service or power at your location, including failed battery backups; or
- a Cyber Event, except as provided in MSA Section 8.6.

We are also not responsible for the time between when a problem begins and when you report it to us, unless our monitoring should reasonably have detected it.

7.2 Work that is billed separately

The following are not included in recurring Fees and will be quoted as projects or billed at our standard rates:

- new installations, migrations, and implementations of replacement software or systems;
- hardware refreshes and equipment deployments beyond routine replacement of a single workstation, unless the Order includes them;
- office moves and new-site setups;
- software development, website work, and custom programming;
- end-user or administrator training, unless the Order includes it;
- repair work caused by unauthorized changes, misuse, or a Cyber Event;
- recovery work caused by a failed software update, beyond rolling back an update we deployed (Section 6.2);
- support for home computers and personal devices not listed in the Order;
- support for line-of-business applications beyond basic troubleshooting and vendor coordination;
- compliance assessments, penetration testing, and audits, which are covered by separate Service Attachments; and
- litigation holds, e-discovery, and testimony (MSA Section 10.5).

7.3 Costs not included

Unless the Order says otherwise, recurring Fees do not include hardware, parts, shipping, software licenses and renewals, third-party support or incident fees, or the cost of replacement equipment or service contracts.

7.4 Services we do not provide

Cambium does not repair printer hardware (we do support printer connectivity and drivers) and does not manage disputes over charges with third-party vendors.

8. Voice (VoIP) Services

This Section applies only if your Order includes hosted voice or VoIP service.

8.1 Installation dates

Cut-over and installation dates in an Order are estimates. We will keep you informed, but we are not liable for delays caused by carriers, number porting, equipment supply, or other causes outside our reasonable control.

8.2 Emergency calling (911)

VoIP emergency calling works differently from traditional phone lines. You acknowledge that:

- 911 calls rely on the registered location we have on file for each phone number or device. You must give us an accurate street address and, for multi-floor or multi-suite locations, a dispatchable location (such as floor or suite) for each device, and must tell us before moving a device or adding a location. Updates can take up to three (3) Business Days to take effect;

- if a device is moved without updating its location, a 911 call may be sent to the wrong emergency center or arrive without accurate location information;
- 911 calling will not work during a power outage, an internet outage, a service suspension (including suspension for non-payment), or if the device is not working;
- where your phone system has multi-line capability, you are responsible for configuring it so users can dial 911 directly without a prefix and for any on-site notification required by federal law, and we will help you set this up; and
- you will tell all Users about these limitations and place any warning labels we provide on devices.

8.3 Unregistered 911 calls

Our carrier charges us for 911 calls placed from numbers or devices without a registered location. You will pay a fee of \$500 for each such call, which reflects those carrier charges and our handling costs.

8.4 Use restrictions

You will not resell voice service, use it for autodialing, robocalling, or traffic-pumping schemes, or use it unlawfully. To prevent fraud or network harm or to comply with law, we may block calls to high-risk destinations or suspend suspicious traffic without notice. International calling is subject to limits imposed by foreign carriers and is billed at the rates in the Order. Collect-call and operator services are not available.

8.5 Voice indemnity

In addition to MSA Section 14.1, you will defend and indemnify Cambium and its carriers and suppliers against third-party claims arising from the failure or unavailability of 911 or other emergency calling through the service, except to the extent caused by Cambium's gross negligence or willful misconduct.

9. Fees and Adjustments

9.1 Quantity true-ups

Each month we will compare the actual number of Users, Devices, sites, and licenses in your environment to the quantities in the Order. If actual quantities are higher, we will bill the added items at the per-unit rates in the Order, starting in the month they were added. If actual quantities fall, we will reduce Fees starting the following month when you ask, but recurring Fees will not go below the quantities you committed to when you signed the Order (the "Minimum Commitment"), and license commitments are governed by Section 5.6.

9.2 Other adjustments

MSA Section 4.8 applies to price changes.

10. Term and Termination

10.1 Term and renewal

The Service Term, automatic renewal, and early termination rules for the Managed Services are in MSA Section 6.

10.2 Additional suspension rights

In addition to MSA Section 5, we may suspend the affected Managed Services on ten (10) days' written notice if you violate a Third-Party Service supplier's license terms and do not correct the violation within that period, or if your actions or inaction prevent us from delivering the Managed Services and the problem is not corrected within fifteen (15) days after we notify you.

10.3 Removal of tools

When the Managed Services end, our access to our tools on your behalf ends, and we will remove our agents and software as described in MSA Section 6.7. You will cooperate with removal and will return or destroy any copies of Cambium-supplied software.

10.4 Third-party charges at the end

When the Managed Services end, you will pay any remaining committed Third-Party Service charges and any termination or transfer charges imposed by suppliers. We may review your use of Third-Party Services during Off-Boarding to confirm those amounts.