

Co-Managed Services Attachment

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

Effective Date: September 25, 2026

Version 1.0

This Co-Managed Services Attachment (this "Attachment") applies when an Order between Cambium Data, Inc. ("Cambium") and Client lists co-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.

1. Purpose and Structure

1.1 What co-managed means

In a co-managed engagement, Client has its own internal IT staff or another IT provider ("Client IT"), and Cambium supports, supplements, or backs up Client IT in the areas listed in the Order (the "Co-Managed Services"). Because two teams share one environment, this Attachment focuses on who is responsible for what, how changes are coordinated, and how risk is divided.

1.2 Scope

Cambium will provide only the Co-Managed Services listed in the Order. The responsibility matrix in Section 3 is the default division of work. The Order may change it for your engagement, and any area not assigned to Cambium in the Order or matrix is Client's responsibility. The written Order and matrix control over informal practice: if Cambium helps with a task outside its assigned areas as a courtesy, that does not make the task Cambium's ongoing responsibility.

1.3 Relationship to the Managed Services Attachment

Where the Order includes services that are also described in Cambium's Managed Services Attachment (for example, monitoring, patching, backup, or VoIP), the terms of the Managed Services Attachment for those services also apply, except that this Attachment controls on questions of shared responsibility, administrative access, and changes made by Client IT.

2. Working Together

2.1 Named contacts

Each party will name a primary technical contact and a backup. Client's primary contact must have authority to approve changes and set priorities for Client IT.

2.2 Communication rhythm

The parties will agree on a regular check-in (monthly by default) to review open tickets, upcoming projects, risks, and recommendations. Each party will share documentation, passwords (through a secure vault, never by plain email), network diagrams, and vendor information that the other reasonably needs.

2.3 Ticket routing and escalation

The Order or onboarding documents will state how Client IT submits requests to Cambium, which issues Cambium handles first, and how urgent issues are escalated after hours. Unless agreed otherwise, Client IT is the first point of contact for Client's end users, and Cambium receives escalations from Client IT.

2.4 Change management

Both parties will follow a shared change process. At minimum:

- any change that could affect availability, security, or the other party's area of responsibility is recorded in advance in the agreed ticketing or change system, with a description, planned time, rollback plan, and approver;
- the party making the change notifies the other party at least two (2) Business Days in advance (or as soon as possible for an emergency change) and considers any concerns raised;
- emergency changes made to contain a Cyber Event or restore service may be made immediately and documented afterward; and
- each party keeps a record of the changes it makes.

2.5 Conflicting instructions

If Client IT and Cambium disagree on a technical approach, Cambium will explain its concerns in writing. Client's primary contact makes the final decision. If Client decides to proceed against Cambium's written recommendation, MSA Section 7.4 applies, and Cambium may decline to carry out a change that it reasonably believes would create a serious security risk or violate law or a license.

3. Responsibility Matrix

The table below shows the default split of responsibilities. "Cambium" and "Client" mean the party that is responsible for performing the task. Where both are listed, the first party leads and the second supports.

Area	Cambium responsibilities	Client responsibilities
Monitoring and maintenance of network devices and servers	Monitor covered devices for availability, performance, and security alerts; apply updates and patches to covered devices; provide remote support and, where the Order includes it, on-site support	Provide physical and remote access; notify Cambium before changing covered devices; keep an accurate inventory of devices and applications
Security operations	Manage the security tools listed in the Order (such as firewalls, endpoint protection, and email security); keep protection tools current on covered devices; perform the vulnerability scans in the Order and recommend fixes	Adopt security policies Cambium recommends or document a risk decision; give Cambium access to security consoles; report suspected incidents to Cambium within 24 hours
Identity and access	Manage administrator accounts for Cambium-managed systems; enforce MFA where Cambium manages the platform	Manage day-to-day user accounts unless the Order assigns this to Cambium; remove departing users within 1 Business Day; approve who holds administrator rights
Backup and disaster recovery	Build a backup and recovery plan with Client; monitor backup jobs for covered	Identify critical systems, data, and recovery priorities; give access needed

	systems; test restores on the schedule in the Order	for backups; take part in recovery tests; back up any systems not covered by the Order
End-user support	Support escalations from Client IT; handle first-line user support only if the Order says so	Provide first-line user support; triage and escalate to Cambium with useful details
Strategy and planning	Offer guidance on technology roadmaps, budgeting, and product selection based on Client's goals	Make final decisions on technology purchases and priorities; communicate plans to Client's leadership and staff
Vendors and licensing	Coordinate with vendors for the systems Cambium manages	Keep software properly licensed; manage vendor contracts not assigned to Cambium

4. Access to Cambium Tools by Client IT

4.1 Shared tool access

Where the Order includes it, Cambium may give named Client IT staff accounts in Cambium's monitoring, ticketing, documentation, or security tools. Those accounts remain Cambium's, are for use only on Client's environment, and end when the Co-Managed Services end or when Cambium reasonably believes the account is being misused.

4.2 Conditions

Client IT users of Cambium tools must: (a) use MFA and not share their accounts; (b) use the tools only as trained and within the permissions granted; (c) follow the change process in Section 2.4; and (d) comply with the license terms of the underlying tools. Client will tell Cambium the same day a Client IT user with tool access leaves or changes roles. Cambium may log and review activity by Client IT users in its tools. If Cambium believes a Client IT account or credential has been compromised or misused, it may disable or reset that account right away and will tell Client promptly.

4.3 Responsibility for Client IT actions

Client is responsible for all actions taken by Client IT, including actions taken through Cambium's tools or through administrator access Client holds. Cambium is not responsible for outages, data loss, security incidents, or other harm caused by Client IT, and time Cambium spends correcting those issues is billable. Client's obligations under this Section are part of Client's indemnity under MSA Section 14.1.

4.4 Administrative credentials

Because administrator access is shared in a co-managed environment, each party will hold only the administrator accounts it needs for its assigned responsibilities, each account will be individually named, and neither party will change the other's administrator accounts without notice. Administrator credentials for Client's own systems and tenants belong to Client. Section 4 of the Managed Services Attachment (credential release at the end of service) applies to administrator accounts that Cambium controls.

5. Security and Data Protection in a Shared Environment

5.1 Shared responsibility for security

Because Cambium does not control every part of a co-managed environment, overall security of the environment remains Client's responsibility, with Cambium responsible for performing the security tasks assigned to it in the Order and matrix with reasonable care. This allocation does not reduce any obligation that applicable law places directly on either party. MSA Sections 7.2, 7.4, and 8 apply, and Cambium's liability for Cyber Events is governed by MSA Section 8.6.

5.2 Compromised systems

If a server or other system is compromised or appears to be under active attack, Cambium may immediately investigate and isolate it, disable accounts, block network traffic, and take other reasonable emergency steps to contain the threat, even if the system is in Client IT's area, and Client authorizes these steps. Cambium will tell Client IT what it did as soon as practical. If a compromise results from weak passwords, missing MFA, outdated or unsupported applications, or other conditions in Client IT's area of responsibility, Cambium's investigation and remediation work is billable. If Client does not address those conditions after written notice, Cambium may end the affected Co-Managed Services for cause under MSA Section 6.4.

5.3 Data loss and recovery

Cambium's role in restoring data is limited to performing the restore services included in a Cambium backup service under the Order, for the systems that service covers, using the backups that are available. For all other systems, restoring data is Client's responsibility. A successful test restore shows that a backup worked at the time of the test; it does not guarantee that every future restore will succeed. Cambium is not responsible for data loss that results from Client IT's actions or from systems outside Cambium's assigned areas, and any liability Cambium does have for data loss is subject to MSA Section 13. Client should keep insurance and business-continuity arrangements, such as redundant or off-site systems, appropriate to the value of its data and the cost of downtime, particularly for revenue-generating applications.

6. Exclusions and Additional Charges

6.1 Conditions outside Cambium's responsibility

In addition to the conditions listed in Section 7.1 of the Managed Services Attachment, Cambium is not responsible for failures or delays to the extent caused by: (a) work, changes, or decisions of Client IT or other Client vendors; (b) systems outside Cambium's assigned areas; (c) Client's failure to follow the change process in Section 2.4; (d) delays by Client IT in reporting problems or escalating them to Cambium; or (e) decisions or priorities set by Client or Client IT, including a choice to proceed against Cambium's written recommendation.

6.2 Work that is billed separately

The items listed in Section 7.2 and the costs listed in Section 7.3 of the Managed Services Attachment are also excluded from the recurring Fees for Co-Managed Services. Temporary coverage for Client IT (for example, during vacations or staff turnover) is available under a separate Order or at our standard rates unless the Order includes it.

7. Network Resources

7.1 IP addresses

Any public IP addresses that Cambium assigns to Client from Cambium's own allocations remain under Cambium's control. Client may use them only in connection with the Co-Managed Services during the Service Term, and Cambium may change or reclaim them with reasonable notice (or without notice where needed to address abuse or a security threat). IP addresses assigned by Client's own internet provider are not affected. Using Cambium-assigned addresses does not give Client any ownership of them.

7.2 Domain names

Client is responsible for its domain names, including registration, renewal, payment, and the accuracy of registrar contact information, unless an Order assigns domain management to Cambium. Client should keep ownership of its registrar account in its own name.

7.3 Acceptable use

Client and Client IT will use the Co-Managed Services and any Cambium-provided resources lawfully and in line with the acceptable use terms of the Third-Party Services involved.

8. Fees, Term, and Termination

8.1 Fees

Fees are stated in the Order. Section 9 of the Managed Services Attachment (quantity true-ups and Minimum Commitment) applies to Co-Managed Services that are priced per User, Device, or site.

8.2 Term, renewal, and termination

The Service Term, automatic renewal, early termination, suspension, Off-Boarding, and data-return rules in MSA Sections 5 and 6 apply to the Co-Managed Services. Section 10 of the Managed Services Attachment also applies.

8.3 Transition

When the Co-Managed Services end, Cambium will cooperate with Client IT to hand over documentation and access for the areas Cambium managed, as part of Off-Boarding under MSA Section 6.7, which is billable and subject to payment of all Fees then due, including any remaining Third-Party Service commitments under Section 10.4 of the Managed Services Attachment.