

Compliance Services Attachment

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

Effective Date: September 25, 2026

Version 1.0

This Compliance Services Attachment (this "Attachment") applies when an Order between Cambium Data, Inc. ("Cambium") and Client lists compliance, risk, or security-program 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. The MSA, including its limits of liability, applies to the Compliance Services; this Attachment adds the terms specific to compliance work.

1. What This Service Is, and What It Is Not

1.1 Purpose

Many small and mid-sized organizations must meet information security and privacy requirements set by laws, regulators, customers, insurers, or industry standards. Cambium's Compliance Services help Client build, operate, and document a security and privacy program that supports those requirements.

1.2 Frameworks covered

The Order will name the laws, regulations, or standards the Compliance Services address (each a "Framework"), for example the HIPAA Security Rule, the FTC Safeguards Rule under the Gramm-Leach-Bliley Act, PCI DSS, the CIS Critical Security Controls, or cyber-insurance control requirements. Cambium performs only the components listed in the Order for the Frameworks named in it. Cambium has no responsibility for any Framework or component not named in the Order, and added scope requires an amended Order.

1.3 Not legal advice, not an audit

Cambium is a technology firm, not a law firm or a certified public accounting firm. The Compliance Services are technical and operational support. They are not legal advice, legal interpretation, an independent audit, or an attestation. Cambium will not certify that Client is compliant with any Framework and does not promise that Client's program will satisfy a regulator, auditor, assessor, customer, or insurer. Client should have its own legal counsel review its obligations, its policies, and any notices to individuals or regulators. When Cambium recommends a safeguard or remediation step, deciding whether and how to carry it out is Client's job; a recommendation does not make Cambium responsible for implementing it unless an Order assigns that work to Cambium.

1.4 Protecting sensitive findings

Risk assessments and gap analyses can reveal weaknesses that Client may prefer to keep confidential. If Client wants its outside counsel to direct an assessment so that Client can try to preserve legal privilege over the results, Client's counsel should engage Cambium through a separate letter that sets out that arrangement before the work begins. Cambium will cooperate with that structure but cannot guarantee that privilege will apply.

2. Service Components

The Order will list which of the following components are included and how often each is performed.

2.1 Risk assessment

Cambium will identify the systems and locations where Client stores, processes, or transmits sensitive information, evaluate reasonably foreseeable threats and vulnerabilities, and rate risks by likelihood and impact. Cambium will deliver a written risk register and a prioritized plan for reducing the most significant risks.

2.2 Written information security program

Cambium will help Client prepare or update a written information security program (WISP) scaled to Client's size and complexity, describing the administrative, technical, and physical safeguards Client uses, such as access control, encryption, logging, secure disposal, vendor oversight, and staff training. Client adopts the program and is responsible for following it.

2.3 Policies and procedures

Cambium will provide templates and help Client tailor security policies and procedures (for example, acceptable use, access control, incident response, backup, and remote work). Where a Framework requires a privacy notice to customers, Cambium can provide technical input about Client's data practices, but Client's legal counsel should prepare or approve the notice itself.

2.4 Security awareness training

Cambium will provide or administer a security awareness program for Client's workforce, which may include online training modules, simulated phishing, and periodic refreshers, and will report on completion rates.

2.5 Vendor risk management

Cambium will help Client build an inventory of vendors that access sensitive information, collect and review vendors' security documentation (such as SOC 2 reports and security questionnaires), and track follow-up items. Cambium can flag security terms that a vendor contract appears to be missing, but negotiating and drafting contract language is the responsibility of Client and its counsel.

2.6 Incident response planning

Cambium will help Client prepare a written incident response plan, identify roles and contacts (including Client's insurer and breach counsel), and, where the Order includes it, run a tabletop exercise. If an incident occurs, Cambium can provide technical information to support Client's counsel in evaluating notification obligations. Hands-on incident response is governed by MSA Section 8.4 or a separate Order.

2.7 Ongoing monitoring and program reviews

Cambium will review the status of Client's program at the frequency stated in the Order, track remediation items, and share relevant updates about changes in regulations, threats, and best practices that come to Cambium's attention.

2.8 Reports and documentation

Cambium will provide status reports at the frequency stated in the Order, covering risk-reduction progress, training completion, and vendor-review status. Cambium will maintain the program documents it prepares in a shared repository so Client can access current versions. Assessments and reports reflect conditions and

information available at the time the work was performed and may not remain accurate as systems, threats, or requirements change. Client owns the final versions of its program documents once Fees for them have been paid; the templates, tools, and methods used to create them remain Cambium Materials under MSA Section 11.3.

3. Client Responsibilities

In addition to its responsibilities under the MSA, Client agrees to the following.

3.1 Compliance is Client's responsibility

Client remains responsible for its own compliance with every law, regulation, contract, and standard that applies to it, including decisions about which risks to accept and which controls to adopt. Cambium will perform the Compliance Services to the standard in MSA Section 12.1, but Cambium's work supports Client's program; it does not transfer Client's compliance obligations to Cambium.

3.2 Program owner and decision-making

Client will designate a program owner with authority to make decisions, approve documents, and assign internal tasks. Client will review drafts and respond to requests for information within the timeframes agreed in the project plan. If Client's responses are late, deliverable dates move back accordingly, and MSA Section 4.9 applies to any extra time the delay causes.

3.3 Accurate and complete information

Client will provide accurate, complete, and timely information, documents, and access to people, systems, and facilities that Cambium reasonably needs. Cambium may rely, without independent verification, on information provided by Client and by Client's other vendors, advisors, and service providers, and is not responsible for errors in its work that result from inaccurate or incomplete information from those sources. Client will make sure Cambium's access complies with Client's own security policies.

3.4 Implementing safeguards

Client is responsible for implementing, operating, and maintaining the safeguards, policies, and procedures in its program, except for specific tasks that an Order assigns to Cambium. This includes using systems as Cambium recommends, protecting them from misuse, backing up data, and applying access controls and encryption.

3.5 Telling Cambium about changes and issues

Client will promptly tell Cambium about changes that could affect its compliance posture (such as new locations, systems, types of data, vendors, mergers, or regulatory inquiries) and about any suspected security incident, audit finding, or concern with the Compliance Services.

3.6 Permits and approvals

Client will obtain any consents, approvals, or internal authorizations needed for Cambium to perform the Compliance Services.

3.7 Insurance

In addition to the insurance required by MSA Section 15.2, Client will maintain privacy liability and regulatory-defense coverage (including coverage for fines and penalties where insurable by law) appropriate to the Regulated Data it handles, as part of or in addition to its cyber liability policy.

4. Allocation of Risk

4.1 Regulatory matters

Cambium is not responsible for fines, penalties, or other regulatory actions against Client, except to the extent they directly result from Cambium's failure to perform the Compliance Services as described in this Attachment and the Order. Client's indemnity under MSA Section 14.1(c) includes claims and costs arising from a regulatory investigation of Client, subject to that same exception.

4.2 Exclusions

Cambium is not responsible for, and the Compliance Services do not cover, any consequences to the extent resulting from:

- Frameworks not named in the Order;
- Client's failure to meet its obligations under the Agreement or applicable law;
- misuse of, unauthorized access to, or changes to systems or data by Client, its users, or its vendors;
- loss or corruption of data, and the cost of recovering it, unless directly caused by Cambium's gross negligence or willful misconduct;
- gaps in Client's own backup, recovery, or continuity planning;
- acts or omissions of vendors that Client engages, unless directly caused by Cambium's gross negligence or willful misconduct;
- Client's failure to tell Cambium about changes to its business, systems, or processes; or
- events outside Cambium's reasonable control, as described in MSA Section 17.3.

4.3 Disclaimer

In addition to MSA Section 12.4, Cambium does not warrant that the Compliance Services or any documents it prepares will meet the requirements of any regulator, auditor, assessor, customer, or insurer.

4.4 Deliverable review

Client will review each written deliverable within fifteen (15) Business Days after delivery and tell Cambium in writing of any material inaccuracy. Cambium will correct, at no charge, factual errors in the deliverable that were caused by Cambium; corrections needed because of inaccurate or incomplete information from Client or its vendors, or because circumstances changed after delivery, are billable. A deliverable is considered complete if Client does not respond within that period or begins using it. Completion confirms only that the deliverable was provided; it does not waive any right that cannot lawfully be waived.

5. Fees, Term, and Termination

5.1 Fees

Fees are stated in the Order and may be recurring, fixed-fee, or time-and-materials. Additional Frameworks, locations, or scope require an amended Order. If a Framework changes, or a regulator, customer, or insurer imposes new requirements during the Service Term, Cambium will tell Client how the change affects the work, and any added effort will be quoted as a change to the Order.

5.2 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 recurring Compliance Services. For Compliance Services purchased as a one-time project, the Order ends when Cambium delivers the final deliverable and it is complete under Section 4.4, and MSA Section 6.3 applies only to any unpaid milestones for work already performed plus the cost of non-cancellable third-party commitments (such as training platform licenses).

5.3 Documents at the end

When the Compliance Services end, Cambium will provide Client with copies of its final program documents and reports that Client has paid for, in a commonly used format, as part of Off-Boarding. MSA Sections 6.7 and 6.8 govern Off-Boarding fees and the thirty-day window for requesting copies. Any non-cancellable third-party commitments made for the Compliance Services, such as training platform licenses, remain payable under MSA Section 13.4.