

Data Processing Agreement

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

Effective Date: September 25, 2026

Version 1.0

This Data Processing Agreement (this "DPA") is between Cambium Data, Inc., a Nebraska corporation ("Cambium"), and the Client named in the Order. It forms part of the Agreement described in Cambium's Master Services Agreement (the "MSA"). Capitalized terms not defined here (including Business Day and Business Hours) have the meanings given in the MSA.

PART A: TERMS THAT APPLY TO ALL REGULATED DATA

A1. When This DPA Applies

A1.1 Activation

This DPA applies only when an Order states that Cambium will store, process, transmit, or have access to Regulated Data, and identifies the law or standard that governs that data. Part A applies whenever this DPA is active, but only to the Regulated Data identified in the Order and to Cambium's processing of it in providing the Services. Each module in Part B applies only if the Order names the law or standard that the module covers. If the Order names Regulated Data but no module fits, Part A applies and the parties will agree on any additional terms in writing.

A1.2 Scope of processing

Cambium processes Regulated Data only as needed to provide the Services. Annex 1 describes the kinds of data, the individuals involved, the purposes, and the duration of processing, and the Order may add details.

A1.3 Priority

On questions about the handling of Regulated Data, the following order applies: (a) mandatory requirements of Applicable Data Law; (b) the SCCs described in Section B5.3, but only for the transfers they cover; (c) the applicable Part B module, for the data it governs; (d) Part A; and (e) the rest of the Agreement.

A2. Definitions

- "Applicable Data Law" means each privacy or security law or contractual standard named in the Order and covered by this DPA.
- "Personal Data" means information in Regulated Data that identifies or can reasonably be linked to a particular individual or household.
- "Processing" means any action taken on Regulated Data, such as collecting, storing, accessing, using, transmitting, altering, or deleting it.

- "Subprocessor" means a third party that Cambium engages that processes Regulated Data on Cambium's behalf. Suppliers that host Client's own tenants under Client's own agreement with them (for example, Client's Microsoft 365 tenant) are not Cambium's Subprocessors.
- "Data Incident" means a confirmed breach of security (confirmed in the sense used in the MSA definition of Security Incident) that leads to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Regulated Data while it is in Cambium's possession or under Cambium's direct control.
- "Unsuccessful Attempt" means an attempted security event that does not result in unauthorized access to Regulated Data or disruption of systems holding it, such as pings, port scans, blocked log-in attempts, denial-of-service attempts that do not succeed, and malware that is blocked.

A3. Roles and Instructions

A3.1 Roles

Client decides why and how Regulated Data is processed. Cambium processes Regulated Data on Client's behalf, as a processor, service provider, business associate, or similar role under the Applicable Data Law.

A3.2 Instructions

Cambium will process Regulated Data only on Client's documented instructions. The Agreement, the Order, and tickets or written requests from Client's authorized contacts are Client's instructions. Cambium may also process Regulated Data when the law requires it, and will tell Client about that requirement before processing unless the law forbids telling Client. If Cambium believes an instruction violates an Applicable Data Law, it will tell Client and may decline to follow the instruction until the parties resolve the issue. If an instruction would materially increase security or compliance risk, or go beyond the Services in the Order, Cambium may ask Client to confirm it in writing and to acknowledge the risk before acting on it, and any added work is billable.

A3.3 No other use

Cambium will not sell Regulated Data, use it for advertising or profiling, combine it with data from other clients, or use it for Cambium's own purposes, except for the limited internal uses the Applicable Data Law permits, such as billing, account administration, security of Cambium's own systems, and compliance with law or legal process. Cambium will access Regulated Data only to the extent reasonably needed for those purposes and the Services.

A4. Cambium Personnel

Cambium will limit access to Regulated Data to personnel who need it to perform the Services, will make sure those personnel are bound by written confidentiality obligations, and will train them on data protection at least once a year.

A5. Security Measures

Cambium will maintain the administrative, technical, and physical safeguards described in Annex 2, which are designed to protect the confidentiality, integrity, and availability of Regulated Data in Cambium's possession

or control in a manner appropriate to the nature of the data and the risks involved. Cambium may update Annex 2 over time, provided the overall level of protection does not decrease. No safeguard can eliminate every risk, and this Section is not a promise that Regulated Data will never be compromised.

A6. Subprocessors

A6.1 Authorization

Client gives general authorization for Cambium to use the Subprocessors identified as processing Regulated Data in the Schedule of Third-Party Services. Before a Subprocessor processes Regulated Data, Cambium will have a written agreement with it that requires data protection at least as protective as this DPA, to the extent applicable to the Subprocessor's services.

A6.2 Changes

Cambium will give Client at least fifteen (15) days' notice, by email or by updating the Schedule of Third-Party Services with an email alert, before adding or replacing a Subprocessor that will process Regulated Data. If an urgent change is needed to keep the Services running or secure (for example, because a supplier fails or is compromised), Cambium may make the change first and give notice as soon as practical afterward. Client may object in writing on reasonable data protection grounds within the notice period, and the parties will discuss the objection in good faith; Cambium may offer an alternative, such as a different configuration or supplier. If the objection is not resolved, Client may end the affected Services under the normal termination terms of MSA Section 6. Suppliers that never process Regulated Data, such as general office or accounting vendors, are not Subprocessors.

A6.3 Responsibility

Cambium remains responsible to Client for its Subprocessors' performance of the data protection obligations Cambium has flowed down to them, but only within, and subject to, the limits of MSA Section 13.

A7. Data Incidents

A7.1 Notice to Client

Cambium will notify Client of a Data Incident without unreasonable delay after confirming it and, where practicable, within seventy-two (72) hours after confirmation. Where a Part B module sets a specific period, that period applies to the data the module governs.

A7.2 Content and follow-up

Cambium's notice will include, to the extent known: what happened and when; the types and approximate volume of Regulated Data affected; the individuals affected or the categories of individuals; the steps Cambium has taken to contain the incident; and a contact at Cambium. Cambium will supplement the notice as more information becomes available, take reasonable steps to contain and mitigate the incident, preserve relevant evidence in its control, and cooperate reasonably with Client's investigation and any notifications Client decides to make. Cooperation does not require Cambium to give Client access to other clients' data, to Cambium's privileged materials, or to information that would weaken Cambium's security. If the incident was caused by Client, its users, or its other vendors, Cambium's response work is billable.

A7.3 Notifications to others

Client decides whether to notify individuals, regulators, or others about a Data Incident, and controls the content of those notifications, unless the law requires Cambium to make a notification itself. Cambium will not notify Client's customers or regulators about a Data Incident involving Client's data without Client's approval unless the law requires it.

A7.4 Unsuccessful Attempts

Unsuccessful Attempts happen constantly and do not require individual notice. This paragraph serves as Cambium's ongoing notice to Client that they occur. Cambium will provide summary information about them on reasonable request.

A7.5 Notice is not an admission

Cambium's notice of or response to a Data Incident is not an admission of fault or liability.

A8. Assistance to Client

A8.1 Individual requests

If Cambium receives a request from an individual to exercise privacy rights regarding Regulated Data, Cambium will forward it to Client within five (5) Business Days and will not respond directly except to confirm that the request has been forwarded. Taking into account the nature of the processing, Cambium will provide reasonable help so that Client can respond.

A8.2 Assessments and regulators

Cambium will provide reasonable information and help that Client needs to complete required risk assessments, data protection assessments, and responses to regulators relating to Cambium's processing.

A8.3 Cost

Assistance under this Section A8 and Section A9 is billable at Cambium's standard rates, unless the assistance is needed because of Cambium's breach of this DPA or the Applicable Data Law requires Cambium to provide it at no charge.

A9. Demonstrating Compliance

On written request not more than once per year (or more often if required by a regulator or following a Data Incident), Cambium will provide information reasonably necessary to demonstrate its compliance with this DPA, such as completed security questionnaires, policy summaries, and any third-party assessment reports Cambium has. If that information is not sufficient to meet a requirement of an Applicable Data Law, Client or an independent auditor bound by confidentiality may conduct an assessment of Cambium's relevant controls, on at least thirty (30) days' notice, during Business Hours, in a way that does not unreasonably disrupt Cambium's operations, and at Client's expense. Cambium may satisfy a request with existing reports or documentation where they reasonably address it. An assessment will not include access to other clients' data, to credentials, or to Cambium trade secrets, and any auditor must be reasonably acceptable to Cambium and must not be a Cambium competitor. Client will treat all information received under this Section as Cambium's Confidential Information and use it only to verify compliance with this DPA or meet Applicable

Data Law. Where a State Privacy Law applies, Cambium may instead arrange, at least once a year and at Client's cost, for a qualified independent assessor to assess its controls and share the result.

A10. Return and Deletion

When the Services involving Regulated Data end, Cambium will, at Client's choice, return Regulated Data in its possession to Client or delete it, within thirty (30) days after Client's request (data-export fees under MSA Section 6.8 apply to returns). If Client does not make a choice within thirty (30) days after the Services end, Cambium will delete the Regulated Data. Cambium may keep copies that the law or a legal hold requires it to keep, and copies in routine backups until they are overwritten in the normal cycle (Cambium need not restore backups just to delete data from them), and will continue to protect those copies under this DPA until they are deleted. Cambium will confirm deletion in writing on request.

A11. Client Responsibilities

Client is responsible for: (a) having a lawful basis and any required notices and consents for the Regulated Data it provides or makes available to Cambium; (b) giving instructions that comply with Applicable Data Law; (c) sharing only the Regulated Data that Cambium needs; (d) telling Cambium about restrictions on the use of Regulated Data that Client has agreed to with individuals or regulators, to the extent they affect Cambium; (e) its own compliance obligations as the party that controls the data, including deciding which laws apply to it and identifying them in the Order; and (f) the security of systems, accounts, and users that Cambium does not manage. Client will not ask Cambium to process Regulated Data in a way that would violate Applicable Data Law if Client did it itself.

A12. Insurance

In addition to MSA Section 15.2, while this DPA is active Client will maintain cyber and privacy liability insurance covering data breach response costs, notification costs, regulatory defense and penalties where insurable, and third-party privacy claims, with limits of at least two million dollars (\$2,000,000) per claim or occurrence. Cambium will maintain the insurance described in MSA Section 15.1.

A13. Liability

All liability arising out of or relating to this DPA, including under any Part B module, is subject to the exclusions and the single aggregate cap in MSA Section 13, and counts toward that cap; this DPA does not create a separate or additional cap. The exclusion of indirect and consequential damages in MSA Section 13.1 applies. Nothing in this DPA limits either party's liability to individuals or regulators where the law does not allow that liability to be limited. This DPA gives no rights to anyone other than the parties, except rights that an Applicable Data Law (or the SCCs) expressly grants to individuals.

A14. Term and Termination

A14.1 Term

This DPA takes effect on the date the first Order that activates it takes effect and continues for as long as Cambium processes Regulated Data for Client.

A14.2 Termination for breach

If Cambium materially breaches this DPA and does not cure the breach within ten (10) Business Days after written notice from Client, Client may end the Services that involve Regulated Data without an early termination fee, in addition to its rights under MSA Section 6.4. Nothing in this DPA limits a termination right that an Applicable Data Law requires.

A14.3 Changes in law

If an Applicable Data Law changes in a way that requires this DPA to be amended, the parties will negotiate an amendment in good faith. If they cannot agree within thirty (30) days, either party may end the affected Services on thirty (30) days' written notice without an early termination fee.

A14.4 Survival

Cambium's obligations under this DPA continue for as long as it holds any Regulated Data.

A15. Operating Boundaries

This DPA sets rules for how Cambium handles Regulated Data within the Services a client has ordered. It does not add services, expand the scope of any Order, or make Cambium responsible for Client's compliance program. Work that this DPA requires Client to ask for, beyond what the Order includes, is billable at Cambium's standard rates unless this DPA says otherwise. Each party will cooperate reasonably with the other in meeting its obligations under Applicable Data Law.

PART B: LAW-SPECIFIC MODULES

Each module below applies only if the Order names the law or standard it covers.

B1. HIPAA Business Associate Terms

B1.1 Application

This module applies if Client is a HIPAA covered entity or business associate and Cambium creates, receives, maintains, or transmits protected health information ("PHI") on Client's behalf. In this module, Client is the "Covered Entity" (or the upstream business associate), Cambium is the "Business Associate," and terms such as PHI, Breach, Unsecured PHI, Security Incident, Designated Record Set, and Individual have the meanings given in the HIPAA Rules at 45 C.F.R. Parts 160 and 164, as amended, including by the HITECH Act (together, "HIPAA"). References to HIPAA provisions mean those provisions as in effect at the relevant time.

B1.2 Permitted uses and disclosures

Cambium may use and disclose PHI only: (a) to perform the Services; (b) for Cambium's proper management and administration and to carry out its legal responsibilities, provided that any disclosure for those purposes is required by law or Cambium first obtains written assurance from the recipient that it will keep the PHI confidential, use it only for the purpose for which it was disclosed or as required by law, and tell Cambium of any breach of confidentiality it learns of; (c) to report violations of law to authorities as permitted by 45 C.F.R. § 164.502(j)(1); and (d) as required by law. Cambium will follow the minimum necessary standard and will not use or disclose PHI in any way that would violate HIPAA if done by the Covered Entity. Cambium will not aggregate Client's PHI with other clients' PHI or de-identify it unless the Order permits it.

B1.3 Safeguards

Cambium will comply with the HIPAA Security Rule (Subpart C of 45 C.F.R. Part 164) for electronic PHI and will use appropriate safeguards so that PHI is used and disclosed only in the ways this module allows.

B1.4 Reporting

Cambium will report to Client in writing: (a) any use or disclosure of PHI not permitted by this module, and any Security Incident involving electronic PHI (other than Unsuccessful Attempts, for which Section A7.4 serves as notice), within five (5) Business Days after Cambium becomes aware of it; and (b) any Breach of Unsecured PHI without unreasonable delay and no later than thirty (30) calendar days after discovery, with the information required by 45 C.F.R. § 164.410 to the extent available, supplemented as information becomes available. Cambium will mitigate, to the extent practicable, harmful effects of improper uses or disclosures known to it.

B1.5 Breach costs

If a Breach of Unsecured PHI was directly caused by Cambium's material breach of this module, Cambium will reimburse Client's reasonable, documented out-of-pocket costs of the notifications that HIPAA requires Client to make (and of credit or identity monitoring only where a law requires it to be offered), subject to MSA Section 13. Where the Breach resulted from a Cyber Event (as defined in the MSA), this Section applies only to the extent Cambium is liable for that Cyber Event under MSA Section 8.6.

B1.6 Subcontractors

Cambium will ensure that any subcontractor that creates, receives, maintains, or transmits PHI on Cambium's behalf agrees in writing, as required by 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), to restrictions and conditions at least as protective as those in this module. Cambium will identify these subcontractors in the Schedule of Third-Party Services or on request.

B1.7 Individual rights

To the extent Cambium itself maintains PHI in a Designated Record Set (as opposed to PHI stored in Client's own systems, which Client can access directly), Cambium will: (a) within ten (10) Business Days after Client's written request, make that PHI available to Client so Client can respond to an Individual's access request under 45 C.F.R. § 164.524; and (b) within fifteen (15) Business Days after Client's written request, make amendments to that PHI that Client directs under 45 C.F.R. § 164.526. Cambium will document disclosures of PHI required to be accounted for and, within ten (10) Business Days after Client's request, provide the information Client needs to give an accounting under 45 C.F.R. § 164.528. If an Individual contacts Cambium

directly with any of these requests, Cambium will forward the request to Client within ten (10) Business Days, and Client is responsible for responding.

B1.8 Covered Entity obligations

If Cambium carries out any of Client's obligations under the HIPAA Privacy Rule, Cambium will comply with the requirements of that rule that apply to Client in performing that obligation. Client will tell Cambium about any limitation in its notice of privacy practices, any change in or revocation of an Individual's permission, and any restriction Client has agreed to, in each case to the extent it affects Cambium's use or disclosure of PHI.

B1.9 Access by HHS

Cambium will make its internal practices, policies and procedures, books, and records relating to PHI available to the Secretary of Health and Human Services for purposes of determining compliance with HIPAA.

B1.10 Termination and return of PHI

Client may terminate the Services involving PHI if Cambium violates a material term of this module and does not cure the violation within the period in Section A14.2. When the Services end, Cambium will return or destroy all PHI it maintains, as Client directs. If return or destruction is not feasible (for example, for PHI in backups not yet overwritten), Cambium will extend the protections of this module to that PHI and limit further uses and disclosures to the purposes that make return or destruction infeasible, for as long as Cambium keeps it.

B1.11 No ownership; no third-party rights

Cambium acquires no ownership rights in PHI. This module does not give rights to anyone other than the parties.

B2. Gramm-Leach-Bliley Act (Financial Information)

B2.1 Application

This module applies if Client is a financial institution under the Gramm-Leach-Bliley Act and Cambium receives or has access to Client's customers' nonpublic personal information ("NPI"). Terms used in this module have the meanings given in the Act and the regulations that apply to Client, including the FTC Standards for Safeguarding Customer Information (16 C.F.R. Part 314) where applicable.

B2.2 Use and disclosure

Cambium will use NPI only to perform the Services and for purposes permitted under the exceptions in 15 U.S.C. § 6802(e) and the related regulations, and will disclose NPI only to its Subprocessors as needed for the Services or as required by law.

B2.3 Safeguards

Cambium will maintain safeguards for NPI that are appropriate to its role as a service provider and to the NPI it handles, as described in Annex 2, with the goals of keeping NPI secure and confidential, guarding against foreseeable threats and unauthorized access that could harm Client's customers, and disposing of NPI securely. Cambium will cooperate with Client's reasonable oversight of Cambium as a service provider, including periodic assessment under Section A9.

B2.4 Notice

Cambium will notify Client of any Data Incident involving NPI within the timeline in Section A7.1, with enough information to allow Client to meet any notification obligations it has, including the FTC notification requirement in 16 C.F.R. § 314.4(j) where it applies.

B3. U.S. State Consumer Privacy Laws

B3.1 Application

This module applies to Personal Data governed by a U.S. state consumer privacy law named in the Order, such as the California Consumer Privacy Act as amended by the California Privacy Rights Act, the Nebraska Data Privacy Act (Neb. Rev. Stat. § 87-1101 et seq.), and the consumer data privacy laws of Colorado, Connecticut, Virginia, Texas, and other states (each a "State Privacy Law"). Terms such as controller, processor, business, service provider, sell, share, and consumer have the meanings given in the applicable State Privacy Law.

B3.2 Role and business purpose

Client is the business or controller, and Cambium is the service provider or processor. Client discloses Personal Data to Cambium only for the limited and specified business purpose of receiving the Services described in the Order and Annex 1.

B3.3 Restrictions

Cambium will not: (a) sell or share Personal Data; (b) retain, use, or disclose Personal Data for any purpose other than the business purpose in Section B3.2 or as otherwise permitted by the State Privacy Law; (c) retain, use, or disclose Personal Data outside of its direct business relationship with Client; or (d) combine Personal Data with personal information it receives from other sources, except as the State Privacy Law permits. Cambium certifies that it understands and will comply with these restrictions.

B3.4 Processor duties

Cambium will: (a) comply with the State Privacy Law as it applies to Cambium and provide the same level of privacy protection the law requires of Client; (b) keep Personal Data confidential and bind its personnel to confidentiality; (c) engage Subprocessors only as described in Section A6; (d) help Client respond to consumer requests (Section A8.1), meet its security and breach notification obligations, and complete data protection assessments (Section A8.2); (e) return or delete Personal Data as described in Section A10; (f) make available information and allow assessments (including an independent assessment where the State Privacy Law provides for one) as described in Section A9; and (g) keep Personal Data only as long as needed for the business purpose.

B3.5 Notice and remediation

Cambium will notify Client if it determines it can no longer meet its obligations under a State Privacy Law. Client may then, on notice, take reasonable steps to stop and remediate any unauthorized use of Personal Data, including suspending the affected processing.

B4. New York SHIELD Act

If the Order names the New York SHIELD Act, Cambium will maintain reasonable administrative, technical, and physical safeguards for the private information of New York residents that it holds on Client's behalf, as described in Annex 2, appropriate to Cambium's size and complexity, the nature and scope of its activities, and the sensitivity of the information. Cambium will notify Client of any Data Incident involving that information under Section A7.

B5. EU and UK GDPR

B5.1 Application

This module applies if the Order names the EU General Data Protection Regulation (Regulation (EU) 2016/679) or the UK GDPR and Data Protection Act 2018 (together, "GDPR"), and Cambium processes Personal Data subject to GDPR on Client's behalf. Terms such as controller, processor, personal data breach, and supervisory authority have the meanings given in GDPR.

B5.2 Processor terms

Client is the controller (or a processor acting for its customer), and Cambium is the processor (or subprocessor). Part A of this DPA sets out the terms required by Article 28(3) of GDPR: processing only on documented instructions (A3), confidentiality of personnel (A4), security under Article 32 (A5 and Annex 2), Subprocessor conditions with notice and an opportunity to object (A6), help with data subject requests (A8.1), help with security, breach notification, impact assessments, and prior consultation (A7 and A8.2), deletion or return at the end (A10), and information and audits (A9). Cambium will notify Client of a personal data breach under Section A7.1 so that Client can meet its 72-hour obligation to the supervisory authority where it applies. Cambium will keep the records of processing required by Article 30(2) and make them available on request.

B5.3 International transfers

Cambium is located in the United States. To the extent Client transfers Personal Data subject to GDPR to Cambium, and no other lawful transfer mechanism applies, the parties agree that the Standard Contractual Clauses adopted by the European Commission in Decision (EU) 2021/914 (the "SCCs") are incorporated into this DPA by reference, as follows: (a) Module Two (controller to processor) applies where Client is a controller, and Module Three (processor to processor) applies where Client is a processor; (b) the optional docking clause in Clause 7 applies; (c) under Clause 9, general written authorization applies, with the notice period in Section A6.2; (d) the optional language in Clause 11 does not apply; (e) under Clauses 17 and 18, the SCCs are governed by the law of Ireland and disputes are resolved by the courts of Ireland; and (f) Annexes I and II of the SCCs are completed by Annex 1 and Annex 2 of this DPA, and the competent supervisory authority is determined under Clause 13. For transfers subject to UK GDPR, the International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner, or another transfer mechanism that UK law recognizes, applies, completed with the information in this DPA. If the SCCs conflict with this DPA, the SCCs control. The choice of Irish law and courts in item (e) applies only to disputes under the SCCs; MSA Section 17.8 continues to govern all other disputes. Before engaging a Subprocessor outside the United States to process Personal Data subject to GDPR, Cambium will follow Section A6 and put in place a transfer mechanism that GDPR recognizes.

B5.4 Cooperation on claims

If either party faces a claim by a data subject or supervisory authority relating to processing under this module, the other party will promptly provide reasonable information and cooperation relevant to the defense of the claim. Each party bears its own costs of cooperating, unless the claim results from the other party's breach.

ANNEX 1: DESCRIPTION OF PROCESSING

The Order may supplement or override this default description.

Item	Description
Subject matter and purpose	Delivery of the managed IT, co-managed, compliance, security testing, and related Services described in the Order, including support, monitoring, maintenance, backup, and security of Client's systems
Nature of processing	Access, storage, transmission, backup, restoration, monitoring, and deletion of data incidental to supporting Client's systems; Cambium's access to content is generally incidental to support work, and Cambium does not intentionally analyze the content of Regulated Data except as needed for a specific support request
Categories of individuals	Client's employees and contractors; Client's customers, patients, or clients; other individuals whose data Client stores in systems Cambium supports
Categories of data	Client decides what data it places in systems Cambium supports. As identified in the Order, which may include contact details, account credentials, financial account information, health information, government identifiers, and other data Client stores in systems Cambium supports
Sensitive data	Only as identified in the Order
Duration	For the term of the Services and the return/deletion period in Section A10
Subprocessors	As listed in the Schedule of Third-Party Services and marked as processing Regulated Data

ANNEX 2: CAMBIUM SECURITY MEASURES

Cambium maintains the following measures on its own systems, applied on a risk basis and scaled to a managed service provider of its size. These measures describe Cambium's program, not a warranty about the security of Client's environment, and may evolve over time without reducing the overall level of protection. Where a tool does not support a listed measure, Cambium uses a reasonable compensating control.

- Governance: a named security lead responsible for Cambium's written information security program, reviewed at least annually and after significant changes.
- Personnel: background checks on personnel with access to client systems or Client Data; written confidentiality commitments; security and privacy training at hire and at least annually; prompt removal of access when a role changes or ends.

- Access control: unique named accounts; multi-factor authentication for all Cambium administrative tools, remote access, and email; least-privilege access to client environments; privileged credentials stored in an encrypted password vault with access logging; periodic review of who holds privileged access.
- Endpoint security: full-disk encryption, managed endpoint detection and response, and automatic security updates on all Cambium laptops and workstations; no storage of Regulated Data on removable media unless encrypted and approved.
- Tool security: Cambium's remote monitoring, remote access, and ticketing platforms are configured with MFA, role-based permissions, and audit logging; Cambium reviews tool vendors' security posture before adoption and monitors vendor security advisories.
- Logging and monitoring: logging of administrative access to client environments where supported by the tools, and review of alerts and anomalous activity.
- Vulnerability management: patching of Cambium's own systems prioritized by risk and severity, and periodic vulnerability scanning of Cambium's internet-facing systems.
- Data protection: encryption of Regulated Data in transit using current industry protocols and at rest where Cambium stores it; secure transfer methods for data exchanges.
- Incident response: a written incident response plan with defined roles, escalation, evidence preservation, and client notification steps, tested at least annually.
- Business continuity: backups of Cambium's own critical systems and documentation, with recovery procedures tested at least annually.
- Secure disposal: secure wiping or physical destruction of media before disposal or reuse, with records kept for devices that held Regulated Data.
- AI Tools: Cambium personnel may enter Regulated Data only into AI Tools that Cambium has approved for that use, and those tools are treated as Subprocessors where this DPA requires.