

Penetration Testing Attachment

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

Effective Date: September 25, 2026

Version 1.0

This Penetration Testing Attachment (this "Attachment") applies when an Order between Cambium Data, Inc. ("Cambium") and Client lists penetration testing, vulnerability assessment, or similar security testing 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 payment, suspension, force majeure, and limitation-of-liability terms, applies to the Testing Services; this Attachment adds terms specific to security testing.

1. The Testing Services

1.1 Purpose

Security testing helps Client understand how an attacker might gain access to its networks, systems, applications, or people, and which weaknesses to fix first. Cambium will perform the security testing described in the Order and the Rules of Engagement (the "Testing Services").

1.2 Types of testing

Depending on the Order, the Testing Services may include one or more of the following:

- external and internal network discovery and vulnerability scanning;
- vulnerability validation and risk rating;
- review of security configurations against recognized benchmarks;
- controlled exploitation of vulnerabilities to show real-world impact (penetration testing), including network, wireless, web application, and cloud testing; and
- social engineering, such as phishing simulations or phone-based pretexting, if expressly listed in the Order.

1.3 Engagement phases

A typical engagement follows these phases: (a) a scoping call to understand Client's environment, key assets, and concerns; (b) preparation of the Rules of Engagement; (c) testing within the agreed window; (d) analysis and risk rating of findings; (e) a readout meeting; (f) delivery of the final report; and (g) where the Order includes it, a retest of fixed findings.

2. Authorization and Rules of Engagement

2.1 Written authorization required

Cambium will not begin testing until Client has signed a written authorization and a Rules of Engagement document. In this Attachment, "Rules of Engagement" means those signed documents together with any written scope changes approved under Section 2.3. They will identify, at a minimum:

- the systems, IP addresses, domains, applications, locations, and (for social engineering) groups of people in scope, and any items specifically excluded;
- the testing window, including dates, times, and any blackout periods;
- the testing techniques permitted and any that are prohibited (for example, denial-of-service or destructive testing);
- emergency contacts for both parties who are reachable throughout the testing window; and
- how findings of critical risk found during testing will be reported.

2.2 Authority over targets

Client represents that it owns or has legal authority to authorize testing of every system, network, application, and account listed as in scope. Where in-scope assets are hosted or operated by a third party (such as a cloud provider, colocation facility, managed firewall provider, or software-as-a-service vendor), Client is responsible for confirming that the third party's terms allow testing, and for obtaining any required third-party consent or notice, before testing begins.

2.3 Staying within scope

Cambium will test only the targets and use only the techniques authorized in the Rules of Engagement. If Cambium discovers that a target appears to belong to someone other than Client, Cambium will stop testing that target and notify Client. Any change to scope, schedule, or techniques must be approved in writing (email is sufficient) by Client's authorized contact, and Cambium may adjust Fees and timelines to reflect the change.

2.4 Stopping testing

Either party may pause testing at any time through the emergency contacts if testing appears to be causing a disruption or if a real attack is suspected. Cambium may also pause, suspend, or decline any part of the testing that it reasonably believes has become unsafe, unlawful, or unauthorized, or if Client's emergency contact cannot be reached when needed. If Client or its staff direct testing outside the Rules of Engagement or materially breach them, Cambium may end the engagement, and Client will pay for work performed and costs incurred to that point. If Cambium discovers evidence that Client may already be compromised, Cambium will stop the related testing and notify Client's emergency contact promptly so Client can decide how to respond. Incident response is not part of the Testing Services and is governed by MSA Section 8.4 or a separate Order.

3. Testing Risks and Client Preparation

3.1 Inherent risks

Security testing deliberately probes systems for weaknesses. Even with careful planning and non-destructive techniques, testing can occasionally slow or interrupt systems, trigger security alerts or account lockouts, or cause unexpected application behavior. Client acknowledges these risks when it authorizes the Testing Services, and they are allocated as described in Section 6. Automated reactions by Client's own security controls, such as account lockouts, device quarantine, or blocked addresses, are an expected part of testing within the Rules of Engagement. Cambium will use reasonable care to minimize disruption and will follow the Rules of Engagement.

3.2 Client preparation

Before testing begins, Client will:

- confirm that current, restorable backups exist for all in-scope systems;
- tell Cambium about fragile, legacy, or business-critical systems and any sensitive data that needs special care;
- tell internal staff and security vendors who need to know (for example, its managed detection provider) so that testing activity is not mistaken for a real attack, or agree with Cambium that testing will be unannounced;
- provide access, test accounts, and credentials that the Rules of Engagement require;
- tell Cambium about any significant change to in-scope systems before or during testing; and
- for on-site testing, provide building access, badges, parking, and a workspace during agreed times, tell Cambium of any known workplace hazards, and avoid interrupting testing once it has started; and
- keep the emergency contacts named in the Rules of Engagement reachable throughout the testing window.

Cambium may rely on the information Client provides about its environment and authority. If Client does not complete these steps, gives inaccurate information, or changes in-scope systems without telling Cambium, Cambium is not responsible for the resulting delays, gaps in coverage, or disruption, and may charge for extra time or rescheduling. Cambium may exclude from testing any asset it reasonably believes is too fragile, unsupported, or defective to test safely, and will note the exclusion in the report.

3.3 Legal compliance

Client is responsible for making sure that its authorization of the Testing Services complies with laws and contracts that apply to Client, including any workplace notice or consent requirements for testing that involves its employees. Social engineering will target only the groups of people named in the Rules of Engagement, and Cambium will not impersonate law enforcement or government agencies, threaten anyone, or use techniques the Rules of Engagement prohibit.

4. Findings, Reports, and Data

4.1 Critical findings

If Cambium identifies a vulnerability that it believes poses an immediate, serious risk, Cambium will notify Client's emergency contact during the engagement rather than waiting for the final report.

4.2 Report

Cambium will deliver a written report that summarizes the engagement for leadership, describes the scope and methods used, lists findings with risk ratings and supporting evidence, and gives practical remediation recommendations. Unless the Order says otherwise, Cambium will deliver a draft report within fifteen (15) Business Days after testing ends, provided Client has supplied the access and information the engagement needed. Client will have ten (10) Business Days to comment on factual accuracy before Cambium issues the final report. Cambium will correct factual errors, but risk ratings and conclusions reflect Cambium's professional judgment, and Client's comments do not require Cambium to change them.

4.3 Retesting

If the Order includes a retest, Client may request it within ninety (90) days after the final report. The retest confirms whether specific findings have been fixed and does not repeat the full engagement. Retests requested later, or that add new targets, are billable.

4.4 Confidentiality of results

Reports, findings, and testing data are Confidential Information of Client under MSA Section 9, except that Cambium's methods, tools, and report templates remain Cambium Materials. Cambium will store testing data securely, limit access to personnel working on the engagement, and delete raw testing data (such as captured credentials, screenshots, and scan output) within ninety (90) days after the final report unless Client asks in writing that it be kept longer, it is needed to support a retest, or law or a legal hold requires it to be kept; copies in routine backups are deleted as those backups expire. If testing incidentally exposes personal, health, financial, or other sensitive information, Cambium will access only what is needed to show the finding and will handle it as Client Data. Cambium will not use captured credentials for any purpose other than the authorized testing.

4.5 Sharing reports with third parties

Client may share the final report with its auditors, insurers, regulators, customers, and advisors who need it. Reports describe conditions at the time of testing only and are prepared for Client's benefit. Cambium owes no duty to any third party who receives a report, no third party may rely on a report as a guarantee of Client's security, and Client will not represent that the report is a certification. Client's right to share the report is a license under MSA Section 11.3; the methods and templates behind it remain Cambium Materials.

4.6 Tools and testers

Cambium may use commercial, open-source, and internally developed testing tools, and, with Client's prior approval (which may be given in the Rules of Engagement), qualified subcontracted testers who are bound by confidentiality obligations at least as protective as those in the MSA.

5. What the Testing Services Do Not Include

Unless the Order expressly says otherwise, the Testing Services do not include:

- fixing identified vulnerabilities or implementing security measures, which Cambium can provide under a separate Order;
- repairing, modifying, or replacing Client's hardware or software;
- continuous or long-term monitoring after the testing window;
- testing of systems not listed in the Rules of Engagement;
- a certification or attestation of compliance with any standard (such as PCI DSS or HIPAA), although results may support Client's own compliance efforts;
- training services; or
- hardware, software, or third-party costs, including charges from hosting providers, carriers, or vendors triggered by testing, and costs of rescheduling caused by Client.

6. Allocation of Risk

6.1 No guarantee

Testing is a point-in-time exercise that is limited by scope, time, and techniques. Cambium does not warrant that it will find every vulnerability or that Client's systems will be secure after testing. Risk ratings are Cambium's professional judgment based on the information available during testing. Cambium is not responsible for security incidents or data loss that occur during or after the Testing Services except as provided in MSA Sections 8.6 and 13.

6.2 Disruption during authorized testing

To the extent permitted by law, Cambium is not liable for service disruption, lockouts, alerts, or data issues that result from testing performed within the Rules of Engagement, unless caused by Cambium's gross negligence or willful misconduct. Client's backups required under Section 3.2 are Client's primary protection against those risks.

6.3 Authorization indemnity

In addition to MSA Section 14.1, Client will defend and indemnify Cambium against third-party claims (including claims by hosting providers, vendors, or employees) arising from testing that Cambium performed within the Rules of Engagement, to the extent the claim results from Client's lack of authority over a target, Client's failure to obtain required consents, or inaccurate information Client provided about scope, except to the extent the claim results from Cambium acting outside the Rules of Engagement or from Cambium's gross negligence or willful misconduct.

6.4 Equipment condition

Cambium is not responsible for the failure of in-scope hardware that is out of warranty, unsupported, or not in working order at the time of testing, or for testing tools behaving as designed within the Rules of Engagement.

7. Fees, Term, and Termination

7.1 Fees

Fees are stated in the Order. Unless the Order says otherwise, fixed-fee engagements are invoiced fifty percent (50%) at signing and fifty percent (50%) on delivery of the draft report. If Client cancels or reschedules a confirmed testing window with less than five (5) Business Days' notice, Cambium may charge a rescheduling fee stated in the Order to cover reserved tester time, plus any non-refundable travel or third-party costs already incurred. MSA Sections 4.3 and 5 apply to late payment.

7.2 One-time engagements

A one-time engagement ends when Cambium delivers the final report and any included retest is completed or the retest period expires. The automatic renewal and early termination fee provisions of MSA Section 6 do not apply to one-time engagements. If Client cancels a one-time engagement before completion, Client will pay for work performed and non-cancellable costs incurred through the cancellation date.

7.3 Recurring testing programs

If the Order provides for recurring testing (for example, quarterly scans or annual penetration tests), the Service Term, automatic renewal, early termination, and suspension provisions of MSA Sections 5 and 6 apply.