

# PENETRATION TEST AUTHORIZATION

This is a customizable starting template, not a finished legal document. Replace every [BRACKETED] field with your specifics, delete or adapt any clause that does not fit your engagement, and have a licensed attorney in the governing jurisdiction review it before you or anyone else signs. CyberSygn is not a law firm and this template is not legal advice.

This Penetration Test Authorization (this "**Authorization**") is entered into as of [EFFECTIVE DATE] (the "**Effective Date**") by and between:

[CLIENT LEGAL NAME], a [STATE] [ENTITY TYPE, e.g. limited liability company] with its principal place of business at [CLIENT ADDRESS] (the "**Client**"); and

[TESTER LEGAL NAME], a [STATE] [ENTITY TYPE] with its principal place of business at [TESTER ADDRESS] (the "**Tester**").

Client and Tester are each a "**Party**" and together the "**Parties**."

**Recitals.** Client owns or controls the systems, networks, and applications described in **Schedule A (Scope)** and wishes to authorize Tester to perform authorized security testing against them to identify vulnerabilities. Because much unauthorized access to computer systems is unlawful, this Authorization is intended to grant Tester clear, written, and limited permission to perform the testing described below. In consideration of the mutual promises below, the Parties agree as follows.

## 1. Grant of Authorization

**1.1 Authorized testing.** Client authorizes Tester to perform the security assessment and penetration testing activities described in this Authorization and Schedule A (the "**Testing**") against the in-scope targets, solely during the authorized window and within the authorized scope.

**1.2 Ownership and right to authorize.** Client represents that it owns or has the lawful right to authorize Testing against each in-scope target, and that no third-party consent is required, or that all required third-party consents (including from hosting providers and cloud platforms) have been obtained. Client will provide copies of any third-party authorizations on Tester's request.

**1.3 Limited license.** This Authorization grants Tester a limited, revocable, non-transferable right to access the in-scope targets only as needed to perform the Testing. It grants no other rights in Client's systems or data.

## 2. Scope of Work

**2.1 In-scope targets.** The Testing is limited to the systems, IP ranges, domains, applications, and accounts listed in Schedule A. Anything not listed is out of scope.

**2.2 Test types.** The authorized test types are: [e.g. external network, internal network, web application, API, wireless, social engineering, physical]. Any test type not listed is not authorized.

**2.3 Exclusions.** The following are expressly excluded from Testing: [LIST EXCLUDED SYSTEMS, THIRD-PARTY SERVICES, PRODUCTION DATABASES, ETC.]. Tester will not knowingly test any out-of-scope system.

**2.4 Changes to scope.** Any change to scope takes effect only when both Parties sign a written change to Schedule A or exchange written confirmation through the designated points of contact.

### 3. Rules of Engagement

**3.1 Testing window.** Testing is authorized only during the window stated in Schedule A (the "**Testing Window**"), in the time zone stated there. Tester will not test outside the Testing Window without prior written approval.

**3.2 Prohibited techniques.** Unless Schedule A expressly authorizes them, Tester will not perform denial-of-service or load-based attacks, destructive actions, data exfiltration beyond proof-of-concept, modification or deletion of Client data, or any action likely to cause material service disruption.

**3.3 Data handling.** If Tester encounters personal data, regulated data, or sensitive Client information during Testing, Tester will limit its access to what is necessary to demonstrate a finding, will not retain it longer than necessary, and will protect it under Section 6.

**3.4 Stop conditions.** Tester will pause Testing and notify Client's point of contact immediately if it discovers an active third-party compromise, evidence of prior unauthorized access, a risk of material harm, or a critical vulnerability that warrants immediate attention.

**3.5 Points of contact.** Each Party designates an authorized point of contact in Schedule A who is available during the Testing Window to coordinate and respond to escalations.

### 4. Tester Obligations

**4.1 Professional standard.** Tester will perform the Testing with reasonable skill and care, in a professional manner consistent with generally accepted practices for security testing.

**4.2 Stay in scope.** Tester will take reasonable steps to confirm that targets are in scope before testing them and will promptly notify Client if it believes it has accessed an out-of-scope system inadvertently.

**4.3 Authorization letter.** Tester's personnel performing the Testing may carry a copy of this Authorization (a "get-out-of-jail letter") to evidence Client's permission, and will present it to Client representatives on request.

### 5. Client Obligations

**5.1 Access and information.** Client will provide the credentials, access, and information described in Schedule A and reasonably necessary to perform the Testing.

**5.2 Internal notice.** Client is responsible for notifying its own personnel, monitoring teams, and service providers as appropriate so that the Testing is not misidentified or escalated in a way that harms either Party.

**5.3 Backups.** Client is responsible for maintaining current backups of in-scope systems and data before the Testing Window.

### 6. Confidentiality

**6.1 Confidential Information.** Each Party will treat as confidential the other Party's non-public information learned in connection with the Testing, including Client's systems information, the test results, and the report.

**6.2 Use and protection.** The receiving Party will use Confidential Information only to perform or act on the Testing, protect it with at least reasonable care, and disclose it only to personnel and advisors who need it and are bound by confidentiality obligations at least as protective as these.

**6.3 Report handling.** Tester will deliver the findings report only to Client's designated recipients and will securely delete or return Client data and working copies of the report within **[NUMBER, e.g. 30]** days after delivery, except for one archival copy retained securely solely for legal and quality purposes.

## 7. Deliverables and Findings

**7.1 Report.** Tester will deliver a written report describing the methodology, the vulnerabilities identified, their severity, supporting evidence, and recommended remediation, by **[DELIVERY DATE]**.

**7.2 Critical findings.** Tester will notify Client's point of contact promptly, and before final delivery, of any critical or actively exploitable vulnerability.

**7.3 Retesting.** The Parties may agree in writing to a retest of remediated findings, the scope and fee for which will be stated in Schedule A or a separate writing.

## 8. Liability and Risk Allocation

**8.1 Inherent risk.** Client acknowledges that security testing carries inherent risk, including the possibility of service interruption, performance degradation, or data effects, even when performed carefully, and that Tester cannot guarantee the absence of such effects.

**8.2 No warranty of completeness.** Testing reflects conditions during the Testing Window only. Tester does not warrant that it will identify every vulnerability or that systems are secure after remediation.

**8.3 Limitation of liability.** Except for breaches of confidentiality, gross negligence, or willful misconduct, neither Party is liable for indirect, incidental, special, consequential, or punitive damages, and each Party's total aggregate liability arising out of this Authorization will not exceed the fees paid or payable for the Testing.

**8.4 Authorized-conduct protection.** Client agrees that Testing performed within the scope and Testing Window is authorized conduct and will not, as between the Parties, be treated as unauthorized access; this does not waive any rights against genuinely unauthorized acts outside scope.

## 9. Term, Termination, and General Provisions

**9.1 Term and revocation.** This Authorization is effective on the Effective Date and continues through completion of the Testing and delivery of the report. Client may revoke or suspend the Testing at any time by written notice to Tester's point of contact, on receipt of which Tester will promptly stop Testing.

**9.2 Compliance with law.** Each Party will comply with applicable laws in connection with the Testing. Nothing in this Authorization authorizes any unlawful act.

**9.3 Governing law and venue.** This Authorization is governed by the laws of the State of **[STATE]**, without regard to its conflict-of-laws rules, and the Parties submit to the exclusive jurisdiction of the state and federal courts located in **[COUNTY, STATE]**.

**9.4 Entire agreement; amendment.** This Authorization, with its Schedules, is the entire agreement on its subject and may be amended only by a writing signed by both Parties.

**9.5 Severability and waiver.** If any provision is unenforceable, the rest remains in effect. A Party's failure to enforce a provision is not a waiver.

**9.6 Counterparts and electronic signature.** This Authorization may be signed in counterparts and by electronic signature, each of which is an original and all of which together form one agreement.

**Schedule A — Scope and Rules of Engagement.** In-scope targets (IPs, domains, apps, accounts): [LIST]. Authorized test types: [LIST]. Exclusions: [LIST]. Testing Window and time zone: [LIST]. Authorized prohibited techniques (if any): [LIST]. Client point of contact: [NAME, PHONE, EMAIL]. Tester point of contact: [NAME, PHONE, EMAIL]. Credentials/access provided: [LIST].

**IN WITNESS WHEREOF,** the Parties have executed this Authorization as of the Effective Date.

CLIENT	TESTER
Signature: _____	Signature: _____
Printed name: [NAME]	Printed name: [NAME]
Title: [TITLE]	Title: [TITLE]
Date: _____	Date: _____

*Template provided by CyberSygn. Not legal advice. CyberSygn is not a law firm. Consult a licensed attorney in your jurisdiction before relying on this document.*