

# BUG BOUNTY AND VULNERABILITY DISCLOSURE AGREEMENT

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 program, and have a licensed attorney in the governing jurisdiction review it before you publish or rely on it. CyberSygn is not a law firm and this template is not legal advice.

This Bug Bounty and Vulnerability Disclosure Agreement (this "**Agreement**") is entered into as of the date a Researcher accepts it (the "**Effective Date**") by and between:

[COMPANY LEGAL NAME], a [STATE] [ENTITY TYPE, e.g. limited liability company] with its principal place of business at [COMPANY ADDRESS] ("**Company**," "**we**," or "**us**"); and

the security researcher who accesses or participates in the Company's bug bounty program (the "**Researcher**" or "**you**").

Company and Researcher are each a "**Party**" and together the "**Parties**."

**Recitals.** The Company operates the systems and applications described in its program scope (the "**Program**") and invites independent security researchers to identify and responsibly report security vulnerabilities. The Researcher wishes to test in-scope systems and report findings in exchange for authorization and potential rewards. By participating in the Program, the Researcher agrees to the terms below. In consideration of the mutual promises below, the Parties agree as follows.

## 1. Authorization and Scope

**1.1 Limited authorization.** Subject to this Agreement, the Company authorizes the Researcher to conduct good-faith security testing of the systems, domains, applications, and assets expressly listed as in scope at [PROGRAM SCOPE URL] (the "**In-Scope Targets**"). This authorization applies only to the In-Scope Targets and only to the activities permitted by this Agreement.

**1.2 Out-of-scope.** Any system, asset, or activity not expressly listed as in scope is out of scope. Testing of out-of-scope assets, third-party services, or other customers' data is not authorized and is not protected by this Agreement.

**1.3 No employment or agency.** This Agreement does not create an employment, agency, partnership, or joint-venture relationship. The Researcher participates as an independent party at the Researcher's own discretion and risk.

**1.4 Revocation.** The Company may modify the scope or suspend or revoke authorization at any time on notice posted to the Program or sent to the Researcher.

## 2. Rules of Engagement

**2.1 Permitted testing.** The Researcher will use only testing techniques reasonably necessary to identify and confirm a vulnerability, and will stop testing once a vulnerability is confirmed.

**2.2 Prohibited conduct.** The Researcher will not: (a) access, modify, delete, or exfiltrate data beyond the minimum necessary to demonstrate a vulnerability; (b) degrade, disrupt, or deny service (for example, through denial-of-service or high-volume automated testing); (c) use social engineering, phishing, or physical attacks against the Company's personnel or facilities; (d) install persistent backdoors or malware; (e) test on accounts or data the Researcher does not own or have permission to use; or (f) publicly disclose a vulnerability except as permitted by Section 5.

**2.3 Data handling.** If the Researcher inadvertently encounters personal, financial, or other sensitive data, the Researcher will stop, will not copy or retain it beyond what is necessary to report, and will promptly inform the Company.

**2.4 Compliance with law.** The Researcher will comply with all applicable laws, including computer-fraud, privacy, and export-control laws. Nothing in this Agreement authorizes any activity that is unlawful in the applicable jurisdiction.

### 3. Reporting

**3.1 Submission.** The Researcher will report each suspected vulnerability promptly and exclusively through **[REPORTING CHANNEL, e.g. security@company.com or the program platform]**, with enough detail for the Company to reproduce and assess it, including steps, affected assets, and any proof-of-concept.

**3.2 One report per issue.** The Researcher will submit a separate report for each distinct vulnerability and will not duplicate reports already acknowledged.

**3.3 Cooperation.** The Researcher will provide reasonable cooperation to help the Company validate and remediate the reported issue, and will not disclose details to third parties before the coordinated-disclosure window in Section 5.

### 4. Rewards and Eligibility

**4.1 Discretionary rewards.** The Company may, in its sole discretion, pay a reward ("**Bounty**") for an eligible report. Reward ranges and criteria are described at **[REWARD TABLE URL]** and may change on prospective notice.

**4.2 Eligibility conditions.** To be eligible for a Bounty, a report must: (a) concern an In-Scope Target; (b) describe a previously unknown, valid, and reproducible vulnerability; (c) be the first valid report of that issue; and (d) comply with this Agreement. Duplicate, out-of-scope, theoretical, or low-impact findings may not qualify.

**4.3 Taxes.** The Researcher is solely responsible for any taxes on Bounties. The Company may require tax or identity documentation before paying a Bounty, and may withhold or report amounts as required by applicable law.

**4.4 Ineligible participants.** Bounties may not be available to Company personnel, contractors, immediate family of personnel, or persons in jurisdictions where the Program is prohibited or who are subject to applicable sanctions.

### 5. Coordinated Disclosure

**5.1 Confidentiality of findings.** The Researcher will keep each vulnerability and all related information confidential and will not disclose it publicly or to any third party until the Company has remediated it and authorized disclosure, or until **[NUMBER, e.g. 90]** days after the report, whichever is earlier, unless the Parties agree otherwise in writing.

**5.2 Public write-ups.** Any public write-up must omit sensitive details that could enable exploitation and, where requested by the Company, must be reviewed before publication. The Company will not unreasonably withhold consent to a responsible write-up after remediation.

**5.3 Recognition.** With the Researcher's consent, the Company may acknowledge the Researcher in a security hall of fame or similar listing.

## 6. Intellectual Property and Safe Harbor

**6.1 License to findings.** The Researcher grants the Company a perpetual, irrevocable, worldwide, royalty-free license to use the contents of each report to investigate, remediate, and improve security. The Company retains all rights in its systems and data.

**6.2 Safe harbor.** If the Researcher conducts security research and disclosure in good-faith compliance with this Agreement, the Company will: (a) consider the activity authorized; (b) not pursue or support civil action against the Researcher for that activity; and (c) where lawful, assist in conveying that the activity was authorized if a third party brings action arising from it. This safe harbor does not apply to activity that violates this Agreement or applicable law.

**6.3 No waiver of third-party rights.** This safe harbor binds only the Company and does not bind third parties, including other customers, vendors, or government authorities.

## 7. Disclaimers and Limitation of Liability

**7.1 As-is.** The In-Scope Targets and any test environment are provided "**as is**" for testing. The Company makes no warranties regarding their availability or fitness for the Researcher's purposes.

**7.2 Researcher risk.** The Researcher participates at the Researcher's own risk and is responsible for any tools, infrastructure, or costs the Researcher uses.

**7.3 Limitation.** To the maximum extent permitted by applicable law, neither Party is liable to the other for indirect, incidental, special, consequential, or punitive damages arising out of the Program. The Company's total aggregate liability arising out of or related to this Agreement will not exceed the total Bounties actually paid to the Researcher.

## 8. Term, Termination, and General Provisions

**8.1 Term and termination.** This Agreement applies while the Researcher participates in the Program. Either Party may stop participating at any time. Sections 3.3, 5, 6, 7, and this Section 8 survive termination.

**8.2 Confidentiality.** The Researcher will keep non-public information about the Company's systems confidential indefinitely, consistent with Section 5.

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

**8.4 Entire agreement; amendment.** This Agreement, together with the published Program rules and scope, is the entire agreement between the Parties on its subject. The Company may amend the Program rules on prospective notice; continued participation constitutes acceptance.

**8.5 Assignment; severability; waiver.** The Researcher may not assign this Agreement. If any provision is unenforceable, the rest remains in effect. A failure to enforce a provision is not a waiver.

8.6 **Electronic acceptance.** Acceptance through the Program platform or by electronic signature is binding and has the same effect as a handwritten signature.

**IN WITNESS WHEREOF**, the Parties have accepted this Agreement as of the Effective Date. Where a countersigned record is desired, the Parties may execute the block below.

COMPANY	RESEARCHER
Signature: _____	Signature: _____
Printed name: <b>[NAME]</b>	Printed name: <b>[NAME]</b>
Title: <b>[TITLE]</b>	Title: <b>[TITLE OR N/A]</b>
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.*