Dodu Security
Smart contract audits and pentests

Andrei Dodu
Sweden
andrei@dodu.se
dodu.se

Rules of engagement and authorisation

This is the document that makes the testing lawful. It names who is authorised to approve the work, exactly what may be touched, and what happens when something goes wrong at 3am.

1. AUTHORISATION

The Client confirms that it owns the systems listed in the scope, or has written authority from the owner to permit their testing, and that the person signing below is authorised to grant that permission. Where a target is hosted by a third party, the Client confirms that the hosting provider's terms permit security testing, or has obtained the provider's consent. This confirmation is the Client's responsibility and is given before testing starts.

2. SCOPE

Only the targets named in the accompanying scope document are in scope. That document lists hosts, applications, repositories, contract addresses, networks and the commit under review. Anything not listed is out of scope, including other hosts on the same domain, other contracts deployed by the same team, and any environment the Client has not named.

3. TIME WINDOW

Testing runs between the start and end dates in the scope. Work outside that window requires written agreement. Testing is done from the Auditor's own infrastructure unless the Client provides an environment.

4. PROHIBITED ACTIONS

The following are not performed unless the scope says otherwise in writing:

- anything that destroys, corrupts or deletes client data, or that changes production state beyond what a proof of concept requires;
- denial-of-service, load or stress testing against production;
- social engineering, phishing, or approaching the Client's staff, customers or suppliers;
- physical access attempts, or testing of the Client's offices or networks;
- persistence mechanisms, backdoors or accounts created to survive the engagement;
- access to, or exfiltration of, real user data beyond the minimum needed to prove a finding, and never personal data in bulk;
- testing of third-party services the Client integrates with, unless those services are named in scope.

5. HANDLING OF WHAT IS FOUND

A finding that exposes live user data or an active compromise is reported to the named contact immediately, before the report is written, and testing on that path stops until the Client says how to proceed. Evidence is kept to the minimum that proves the finding: a request and response, a screenshot, a transaction hash, or a short recording. Bulk data is never retained. Evidence is stored encrypted, kept for the term of the engagement plus twelve months for fix verification, then deleted on request or on schedule.

6. EMERGENCY STOP

Either party may suspend the engagement immediately by message to the other's named contact. If the Client believes production is affected, the Auditor stops testing within the hour and confirms in writing. Work resumes only on written instruction.

7. REPORTING AND DISCLOSURE

Findings are delivered to the Client and to nobody else. Nothing is published, posted, shared with a bug-bounty programme, or disclosed to a third party without the Client's written consent, except where disclosure is required by law. After a fix is deployed, the Client may consent to an anonymised case study; consent is optional and its absence changes nothing about the engagement.

8. LIABILITY

The Auditor performs the work with reasonable skill and care and does not warrant that the review will find every vulnerability. The Client remains responsible for its own systems, for the decision to deploy, and for any remediation. Liability under this engagement is capped at the fee paid for the engagement, except for wilful misconduct, and neither party is liable for indirect or consequential loss.

9. INSURANCE AND LAW

The engagement is governed by the law stated in the accompanying scope document. Where the Client requires professional indemnity insurance as a condition of the engagement, that requirement is agreed in writing before the start date, not after.

For the Client: name, title, authority confirmed, date

Signature

For Dodu Security: Andrei Dodu, date

Signature

Dodu Security is the trading name of Andrei Dodu. This document is a template, not legal advice; where the engagement is large enough to warrant it, have a lawyer read it.