# Rules of Engagement (ROE)

Engagement: ____
Tester / testing organisation: ____
Client: ____
Authorization letter reference: ____
This ROE accompanies the signed authorization letter and is read with it. The authorization letter records permission; this document records how the permitted testing is run.

## 1. Objective

Scope of work: ____
Testing is performed only within the in-scope assets and testing windows stated below and in the authorization letter.

## 2. Scope (in scope)

In-scope assets, applications and addresses: ____
Source IP addresses testing will originate from: ____
Testing accounts or credentials provided: ____

## 3. Out of scope

Explicitly out of scope: ____
Any asset not listed as in scope is out of scope.
Assets belonging to third parties (shared hosting, SaaS providers, CDNs, employees' personal devices) are out of scope unless that party's own written authorization is attached.
Data not required for the test is out of scope; confidential material encountered by chance is handled per clause 11.

## 4. Permitted testing categories

Authorized by default:
[ ] Network / infrastructure scanning
[ ] Web application testing
[ ] API testing
[ ] Authentication / authorization testing
Require separate written approval:
[ ] Intrusive testing (e.g. denial of service) [ ] Social engineering

## 5. Rate limits and restrictions

Maximum automated request rate: ____
Production data may be: read / modified only with prior written approval.
Scans must not be configured in a way that risks availability of an in-scope service.

## 6. Testing windows

Permitted testing days and hours: ____
Excluded dates / change-freeze periods: ____
Time zone for all windows: ____
Testing outside these windows requires written approval from the client contact named below.

## 7. Prohibited actions

Prohibited for this engagement: ____
Unless separately approved in writing, the following are prohibited: denial-of-service or load testing; destructive payloads; modification or deletion of production data; social engineering; persistence mechanisms; testing any out-of-scope asset; and any technique that risks the integrity or availability of a live service.

## 8. Communication

Status updates every ____ via ____
Primary channel: ____
Client primary contact: ____ Backup: ____
Tester primary contact: ____ Backup: ____

## 9. Escalation

If a critical finding or a real security incident is discovered:
Notify ____ within ____ minutes.
Testing will: continue / pause until cleared.

## 10. Emergency stop

The client may halt testing at any time by stating "STOP" to the tester's primary contact. The tester will acknowledge immediately and cease all active testing within the agreed interval.
Testing stops within: ____ minutes.
No testing resumes without written clearance from the client signer.

## 11. Evidence and data handling

Evidence captured: ____
Stored where / accessible to whom: ____
Retention period: ____ Destruction method: ____
Confidential material encountered by chance will be: reported / not retained.

## 12. Reporting

Draft report delivered by: ____
Final report delivered by: ____
Format and delivery channel: ____
Distribution list: ____

## 13. Retest

Retest included: yes / no
Retest window: ____
Eligible findings: confirmed high and critical, unless otherwise agreed.

## 14. Sign-off

Client signer: ____ Name / title / date
Tester lead: ____ Name / title / date
By signing, both parties confirm they have read this ROE and the referenced authorization letter, and that the engagement is performed under them.