



GHOST
PROTOCOL

REF

THE FIELD LIBRARY

COMPANION

KEEP IT OPEN

The Reference Pack

Templates, checklists, cheat-sheets and
quick-references to keep open while you
work.



Ghost Protocol (Pvt) Ltd · Colombo · ghosts.lk

Security internship training · The Field Library · Edition 1 · 2026

THE GHOST PROTOCOL FIELD LIBRARY · COMPANION

The Reference Pack

Templates, checklists, cheat-sheets and quick-references to keep open while you work.

Ghost Protocol (Pvt) Ltd · Colombo

The Field Library, Edition 1 · 2026

Copyright 2026 Ghost Protocol (Private) Limited. All rights reserved.

Sold as a PDF for the buyer's own reading. Please do not share or resell the file.

The library

The Field Library is a whole shelf, not one book. The Core Path is the spine everyone reads. The rest is depth and breadth, taken on as the work calls for it. The shelf is complete now, and you are reading the one marked here.

A · THE CORE PATH

O The Oath BUILT

I Groundwork BUILT

II The Web BUILT

III The Wider Field BUILT

IV The Work BUILT

V The Craft BUILT

B · DEEP TRACKS

AI and Agents BUILT

Reading Code BUILT

Internal and Active Directory BUILT

The Web, Deeper BUILT

Cloud and Containers BUILT

Mobile and APIs BUILT

Reverse Engineering BUILT

Hardware and the Edges BUILT

C · THE OPERATIONS

Red and Purple Team BUILT

OSINT and Recon BUILT

Report Writing Mastery BUILT

The Consulting Craft BUILT

Bug Bounty BUILT

D · THE OTHER SIDE

Detection and Response BUILT

Threat Hunting and Forensics BUILT

Hardening and Architecture BUILT

E · THE GROUND RULES

The Law, Deeper BUILT

Standards and Compliance BUILT

Ethics and Disclosure BUILT

F · COMPANIONS

The Reference Pack YOU ARE HERE

The Lab Workbook BUILT

Case Files BUILT

The Bestiary BUILT

The Glossary and the Ledger BUILT

Contents

- Opening 5
- 1** The Pre-Engagement Checklist 6
- 2** Rules of Engagement and Authorisation 9
- 3** The Report Template 14
- 4** Command Cheat-Sheets 18
- 5** Severity and CVSS 22
- 6** Legal Quick-Reference, Glossary and Further Reading 25
- On exercises 29

Keep it open



This one is not a book you read through. It is the pack you keep open on the second screen while you work: the checklist before the first packet, the templates you fill in, the report shape you copy, the few commands you always half remember, the severity card, and the law in one page.

Everything here is taught properly somewhere else in the Library. Volume O is the law and the line, Volume IV is the engagement and the report, Volume II is the method. This is the quick card for the day you are in the middle of the work and need the thing, not the lesson.

WYRM "the card, not the book."

Use it, and never let a template do the thinking the work still needs from you.

CHECKLIST

The Pre-Engagement Checklist

Everything that must be true before the first packet. Run it top to bottom. If a line is not clear, you are not cleared to start, no matter the deadline.

This is the card you clear before any active testing begins. It is the operational form of the one rule from Volume 0: you test only what you are authorised, in writing, to test. Tick every box against the paper in front of you, not from memory. A "mostly" is a no.

Each box below is a yes-or-no you can answer from the signed Rules of Engagement, the Test Authorisation, and the scoping notes. Print it, work down it, and keep the ticked copy with the engagement file.

Authorisation in writing

CLEAR	THE GATE
☐	A signed Test Authorisation exists, is dated, and you have read it in full.
☐	The signatory has the authority to grant testing of these systems: the owner or a person with the authority to grant it, not a developer's "sure, go ahead".
☐	The authorisation ties to this engagement's scope and window, not a stale or generic letter.
☐	If a free scan is part of this, someone with authority over the target said yes to it in writing before it ran, it stayed passive, and no active test is planned before the signature is in hand.

■ THE LINE

Before any action against any system that is not your own lab, you can answer all three, out loud, from the paper:

- Is this exact system named in a written authorisation I have read?
- Is this action inside the scope and the time window it grants?
- Was it signed by someone with the authority to grant it?

Three yeses, or you do not touch it. A promise to sign is not a signature.

No scan of any client or prospect, not even the free scan, until someone with authority over the target has said yes in writing. Visiting a prospect's public website the way any visitor would is not a test; anything more waits for that written yes.

Scope confirmed

CLEAR	THE GATE
☐	The in-scope targets are listed exactly: hostnames, URLs, IP ranges, applications, and any test accounts you were given.
☐	The out-of-scope list is written as plainly as the in-scope one. Out of scope binds as hard as in scope.

CLEAR	THE GATE
☐	You recorded whether you were pointed at production or a staging copy, and which one you may touch.
☐	Any third-party-hosted system or shared infrastructure is flagged, and who may authorise it is settled, not assumed.

How loud you may be

CLEAR	THE GATE
☐	Passive-only or active probing is agreed, and automated scanning is either permitted at a stated rate or it is not.
☐	Whether you may exploit a finding to prove impact, or only demonstrate it safely, is written down.
☐	The loud techniques are forbidden unless named as allowed: denial of service, anything destructive, social engineering of staff, touching real customer data.

The window

CLEAR	THE GATE
☐	The dates and hours you may work are fixed, with the time zone stated.
☐	Blackout dates are recorded: a sale, a release, a month-end run, the client's busiest day.
☐	The people who must be told before you start are told, so your traffic is not mistaken for a real attack.

Contacts

CLEAR	THE GATE
☐	You have a named point of contact and a way to reach them fast.
☐	You have an out-of-hours number for the moments you have to stop and call at once.
☐	The reporting cadence is agreed: how often you check in, and through which channel.
☐	You know when something goes to Ryan rather than being resolved at the keyboard.

Stop-and-report triggers agreed in advance

These five are settled with the client before you start, not improvised the moment one fires. When one happens, you halt and report; you do not keep going to be sure.

THE TRIGGER	WHAT YOU DO
Signs that someone else is already inside (a real intrusion, past or in progress)	Stop, touch nothing, preserve your own logs, phone the contact at once. You may be standing in a crime scene.
You reach something clearly out of scope, by accident or because scope was unclear	Stop, do not explore it, report, and get the scope settled before continuing.
An action could cause an outage or data loss	Stop before it does, not after.

THE TRIGGER	WHAT YOU DO
You hit especially sensitive data (medical, financial at scale, anything about children)	Take the minimum to prove it exists, then report.
You find something that could endanger a person's safety	People before findings, always. Report immediately.

Data handling

CLEAR	THE GATE
[]	You know where evidence is stored for this engagement, and that it goes nowhere else.
[]	You will take only what proves the finding: one screenshot, one record, not the whole table.
[]	No copies on your personal machine, no pasting into a chat, no "I will clean it up later".
[]	Destruction at the close of the engagement is agreed. You keep the report, not the spoils, and never a souvenir.

■ NOTE

A template with the blanks unfilled is not authorisation, and a checklist you ticked from memory is not a checklist. Each box above points at a specific line in the paperwork. If you cannot find the line, the box is not clear. The cost of checking is a few minutes. The cost of guessing wrong is in Volume O, Chapter Two.



WHAT WYRM KEEPS

Nothing active happens until the whole card is clear: written authorisation, confirmed scope, an agreed loudness, a window, contacts, the five stop triggers, and data handling.

- Three yeses before the first packet: named in writing, inside scope and window, signed by someone with the authority.
- Out of scope binds as hard as in scope. A promise to sign is not a signature.
- The stop-and-report triggers are agreed before you start, not in the moment one fires.

TEMPLATES

Rules of Engagement and Authorisation

A working skeleton for the two documents that make a test lawful. Fill every bracket with this engagement's facts. The binding legal wording is set by Ryan and counsel, and no price ever goes in either document.

Two documents turn a conversation into lawful work: the Rules of Engagement, which describes the test both sides agree to, and the Test Authorisation, which is the signed grant of permission to run it. Volume IV teaches how each is built; this card is the fill-in form. A template with the blanks unfilled is not authorisation.

■ HOW TO USE THIS

These are skeletons, not a signed contract. The exact legal wording, and the form that actually goes to a client, are set by Ryan and the lawyer. Your job is to make sure every item below is present, specific, and true for this engagement. Replace every `[bracket]`. Delete nothing that applies. Never write a figure into either document: Ryan signs the scope and names any price separately. A document with a stray price in it is a document you do not send.

Template A: Rules of Engagement

Working title: `Rules of Engagement, [Client legal name] security test, [YYYY-MM-DD]`. Version and date it, because scope changes are tracked by version.

1. Parties

This Rules of Engagement is agreed between `[Client legal name]` (the client) of `[client address]`, and Ghost Protocol (Pvt) Ltd (the tester). Primary client signatory: `[name, title]`. Tester lead: `[name]`.

2. Asset ownership and authority

The client confirms that it owns, or otherwise has the authority to permit security testing of, every system listed in scope below. Where any in-scope system is hosted or operated by a third party, the client confirms that the necessary permission is in place: `[name the third party and the permission, or state "none"]`.

3. In-scope targets

Testing is authorised against these targets only:

- Web and application hosts: `[hostnames / URLs]`
- IP ranges: `[CIDR ranges, or "none"]`
- APIs: `[base URLs / documented endpoints]`
- Environment: `[production / staging], at [base URL]`
- Test accounts provided: `[roles and how they are issued]`

4. Out of scope

The following are explicitly excluded and must not be touched. Anything not named in scope above is out of scope by default, even if it belongs to the client.

- [hosts / domains / subdomains excluded]
- [shared infrastructure, third-party systems, production databases]
- [any high-risk feature the client is nervous about]

5. Testing window

Work is authorised from [start date and time] to [end date and time], time zone [e.g. Asia/Colombo, UTC+5:30], during [hours, e.g. 20:00 to 06:00 only]. Blackout dates on which no testing occurs: [dates, or "none"].

6. Permitted and forbidden techniques

Permitted: [e.g. unauthenticated and authenticated web testing, manual testing supported by tooling]. The following are forbidden unless named here as allowed, in which case the condition is stated:

- Denial of service or load testing: [forbidden / allowed under condition]
- Destructive or state-changing actions on live data: [forbidden / allowed under condition]
- Social engineering or phishing of staff: [forbidden / allowed under condition]
- Access to, or exfiltration of, real customer data: [forbidden / allowed under condition]

7. Intensity and rate

Automated scanning is [permitted / not permitted], capped at [rate, e.g. 1 to 2 requests per second per host]. Exploitation to prove impact is [permitted / limited to safe demonstration only]. The tester backs off on rising latency and honours the target's own rate signals.

8. Communication and points of contact

- Primary contact: [name, role, phone, email]
- Out-of-hours contact for stop-and-report: [name, phone]
- Reporting cadence: [e.g. a short daily note, plus the final report]
- Channel: [agreed secure channel]
- Tester source IP addresses: [the fixed addresses all testing comes from]
- Told before testing starts: [named people at the client, the hosting or cloud provider, any managed security provider]
- Deliberately not told, if the client is testing its own detection: [names and roles, or "none"]

9. Stop-and-report triggers

The tester halts and contacts the client at once on any of: evidence of a prior or ongoing intrusion; reaching anything clearly out of scope; an action that could cause an outage or data loss; especially sensitive data; anything that could endanger a person. On any trigger the tester stops, does not dig further, preserves its own logs, and reports.