



GHOST
PROTOCOL

ED

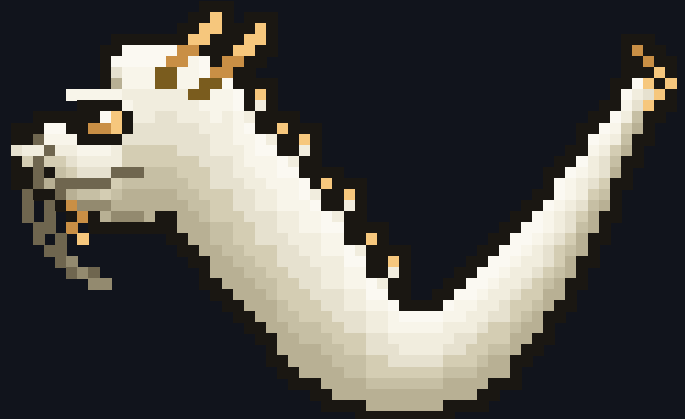
THE FIELD LIBRARY

GROUND RULES

WIN ON THE MERITS, ONLY

Ethics and Disclosure

The ethic beneath the work, boundaries
and consent, coordinated disclosure,
conflicts and temptations, and the codes.



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

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

THE GHOST PROTOCOL FIELD LIBRARY · GROUND RULES

Ethics and Disclosure

The ethic beneath the work, boundaries and consent, coordinated disclosure, conflicts and temptations, and the codes.

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 YOU ARE HERE

F · COMPANIONS

The Reference Pack BUILT

The Lab Workbook BUILT

Case Files BUILT

The Bestiary BUILT

The Glossary and the Ledger BUILT

Contents

- Opening 5
- 1** The Ethic Beneath the Work 6
- 2** Boundaries and Consent 9
- 3** Coordinated Disclosure, Deeper 12
- 4** Conflicts and Temptations 17
- 5** The Profession and Its Codes 21
- Worked answers 26

The win you do not take



Deep in a client's systems, Blink found something that had nothing to do with the test: a private, embarrassing thing about the person who had been difficult all week. The cursor hovered, delighted.

BLINK "We could use this. They would settle in an hour."

SOL "No. We win on the merits, only, and never on what the work happened to show us. That move is not clever negotiating. It is extortion, a crime in its own right, and the instant you make it you stop being the professional with a finding and become the accused. A clean party with a real case already has all the leverage it needs. It accrues on its own. We let it."

Wyrms's eye was cold on the hovering cursor.

WYRM "merits. only."

So the book is the ethic under the whole craft: the boundaries, consent, honest disclosure, and the temptations you will meet and must not take, because the one asset you can never buy back is being trusted.

CHAPTER ONE

The Ethic Beneath the Work

Volume 0 gave you clean conduct as a rule. This chapter is what sits under the rule: why a person with this kind of access holds themselves to more than the law demands, and why in this trade the clean move and the clever move turn out to be the same one.

You spent years learning to reach things other people meant to keep shut. That is a real skill and a rare one, and it is about to become your job. Before it does, sit with the fact of it for a moment, because the whole of your professional character is not in what you can reach. It is in what you choose not to touch once you are inside.

The law is the floor, not the ceiling

Volume 0 taught you a gate: you test only what you are authorised, in writing, to test, and authority is binary. That gate is the law, and the law answers one question only, the question of whether an act is permitted. It is a floor. It tells you where the ground gives way, and it is drawn to catch the worst thing a person in your seat might do, not to describe the best.

Ethics is the second question, and the law never asks it. Not "am I allowed to do this" but "should I". Most of the sharp moments in this work sit in the gap between the two, where an action is plainly inside your authorisation and still wrong, or plainly outside your remit and still the decent thing. The law will not help you there, because the law has already said yes, or has nothing to say at all. What decides it is the ethic you brought in with you.

Access is power, and power with no witness is character

Think about what the job actually hands you. For the length of an engagement you can see inside a company that lets almost no one in: its systems, its mistakes, sometimes its people at their least guarded. You can read things that were never meant for you, not because you broke a rule but because proving a flaw put them in front of you. Nobody is standing behind your chair. The logs record what you touched, but the logs do not record the thing you noticed and let alone, and no one will ever ask you about the file you decided not to open.

That is the real exam, and it is sat in private. A person who behaves well only when watched has manners, not ethics. The test of the thing is the unwatched moment, the late night alone on a client's network with something interesting one click away and no one who would ever know. What you do then is who you are, and it is the one part of your reputation you build where nobody can see.



leave it.

The file you could open, that proves nothing and belongs to someone else, is the one to close. Curiosity is not authority, and "no one would know" is the sentence that has ended more careers in this trade than any exploit.

Win on the merits, taken to its root

Ghost Protocol's standing rule is that we win on the merits, only on the merits. Volume 0 stated it. Here is why it holds all the way down. A finding that is true carries itself: the evidence is there, the severity argues itself from what the flaw can reach, and nothing you add makes it more true. A finding that is inflated is not a stronger version of a true one. It is a different object, a claim the evidence does not support, which is to say a lie with a number on it. Once you have filed one, no one can tell which of your trues is true, and the value of everything you report collapses to nothing. The merits are not the polite option. They are the only ground that bears weight, because they are the only ground that stays standing when someone leans on it.

The same root runs under the rule you will meet again in Chapter Four: you never reach for anything outside the work to win. Not a counterparty's private embarrassment, not a threat dressed as a hint. The strength of a clean party with a real case accrues on its own, and the word is doing its literal work in that sentence. You do not manufacture leverage. You let the true thing be as strong as it is, and you refuse every shortcut that would trade that strength for a faster, dirtier win.

The skill is neutral; you are not

The ability you have built is the same ability a criminal builds. The tools are the same, the knowledge is the same, the thrill of getting in is the same. Nothing in the craft itself points it anywhere. The direction is supplied entirely by the person holding it, which means the difference between a professional and the thing the professional is hired to stop is not talent. It is restraint, consent, and the willingness to stop. The trade exists only in the narrow place where real capability is pointed at a target that agreed to it, by a person who will put the gloves down the moment the paper says to. Take away the restraint and you have not got a lesser professional. You have got the attacker, with a nicer laptop.

Trust is what the client actually buys

A report is the thing the client can hold, but it is not the thing they are paying for. They are paying to let a stranger deep inside their defences and trust that the stranger will be honest about what was found, silent about everything else, and gone cleanly at the end. That trust is the product. Findings are just its receipt. A house that is known to be straight, to never overstate, to keep its mouth shut, is a house people will let in again, and in a trade built entirely on being let in, that is the whole business. Credibility is the one asset here you cannot buy back once it is spent, and the ethic in this chapter is, before it is anything noble, the discipline of not spending it.



SOL SAYS

People expect this part of the job to feel like a constant moral strain, a daily fight against temptation. It is not, once it is settled. The operators I trust most are not the ones wrestling their conscience on every engagement. They decided the big things in advance, in the quiet, when nothing was at stake, so that on the hard night the decision was already made and there was nothing left to argue with themselves about. Settle it now, while it costs you nothing. That is what this chapter is for.

■ THE LINE

Whenever "can I" and "should I" give you different answers, the one that governs is "should I". The law having said yes is not the end of the question; it is barely the start of it. If an action is inside your authorisation and your gut has still gone quiet, that quiet is information. Stop, name what is bothering you, and if you cannot clear it in a sentence, take it to Ryan before you act, not after.

■ ON YOUR FEET

Late on an authorised engagement, alone, you realise the scope technically lets you read a senior executive's private message archive. It has nothing to do with the flaw you are proving, you do not need it for the report, and no rule in the law or the Rules of Engagement would be tripped by a look. No one would ever know you read it. What decides whether you open it, and what do you do?



WHAT WYRM KEEPS

The law answers "may I"; ethics answers "should I", and the gap between them is where this work is really judged. The test is the unwatched moment.

- The law is a floor built for the worst case, not a description of good conduct. Where it says yes, or says nothing, the ethic still governs.
- Access is power exercised in private. Character is what you refuse to touch when no one would ever know you touched it.
- Win on the merits all the way down: a true finding carries itself, an inflated one is a lie with a number on it, and one lie voids every true you ever filed.
- The skill is morally neutral; you supply the direction. Trust is the product, and credibility is the one asset you cannot buy back.

CHAPTER TWO

Boundaries and Consent

Authorisation and scope are law in Volume O and in The Law, Deeper. They are also ethics. A boundary protects the people a test can hurt, most of whom never signed anything, and real consent means a client who understood what they agreed to, not just a client who signed.

Volume O and The Law, Deeper taught the written authorisation as the thing that keeps you out of prison, which it is. This chapter reads the same boundary from the other side. A scope line is not only your legal shield. It is the edge of the harm a test can do, and almost everyone that harm would fall on never sat at the table where the paper was signed.

A boundary is an ethical object, not only a legal one

It is tempting to treat scope as pure self-protection, a fence you stay inside so the law cannot reach you. That reading is true and too small. The fence is also around other people. When you stop at the edge of what was authorised, you are not only saving yourself; you are declining to touch systems and data that belong to people who did not agree and cannot defend themselves against your curiosity. Test the thought by removing the legal risk. Suppose you knew, for certain, that crossing a particular scope line could never be traced to you. Would it then be fine? It would not, and the reason it would not is the ethic under the law: the boundary was protecting someone, and the someone is still there whether or not the law is watching.

Consent has to be informed to be worth anything

A signature is evidence of consent; it is not the same thing as consent. The idea worth borrowing here is **informed consent**, which medicine and research ethics worked out long before this trade existed: agreement only means something when the person agreeing actually understands what they are agreeing to. A client who signs a Rules of Engagement without grasping that your test could, done wrong, take their site down during business hours, or that proving a flaw may put you in front of their customers' real records, has signed something, but they have not truly agreed to it. If it goes wrong, "but you signed" is a legalism, and they will be right to feel it was done to them rather than with them.

So part of the ethic, before the first packet, is making sure the client understands in plain language what the test involves, what could realistically break, what you might see, and what you will do with it. This is the measured, plain-spoken register the house uses with every client: not jargon that lets them nod along without following, and not a sales gloss that hides the risks to get the yes. The clearer the client's picture before they agree, the more their yes is worth, and the better protected everyone is when the test does something unexpected.

Who at the table never signed

Look again at a routine engagement and count the people affected by it who were never asked. The client's own users, whose real names, records, and messages sit inside the system you are about to

probe. Other tenants on the shared infrastructure the client rents, who agreed to nothing and could be hit by a test aimed at your client's slice of it. A payment processor, a mail service, an identity provider one hop away, each a separate company with its own users. A single individual whose record would be the cleanest proof of an access-control flaw. None of them signed your paper. The client consented on behalf of its own assets, and its consent reaches exactly that far and no further.

The ethic that follows is the discipline of minimising harm to the people who never agreed. It is the deep reason behind the handling rules Volume 0 gave you as a list. Take only what proves the finding, because every extra record you touch is a real person's data handled for no reason. Prove the mechanism, not the volume: one redacted record shows an access-control flaw exactly as well as ten thousand, and the mass export only widens the harm you are supposedly reporting. Stop at the trust boundary, because one hop into a provider's shared system is a fresh harm against that provider's other customers, who are now exposed by a test they never heard of. The data-protection law behind this (the PDPA at home, the GDPR where a client's users are in Europe) is the subject of The Law, Deeper, and it is not re-taught here. What this chapter adds is that the law is downstream of the ethic: the rule exists because real people who never consented can be hurt, and your job is to see them even though they were not in the room.



who else?

Before an action, the question is not only "am I in scope" but "whose data, whose system, whose safety does this touch, and did they agree". If the honest answer reaches someone who never consented, that is the edge, and it holds even when the paperwork does not mention them.

Consent before the probe, every time

The rule that nothing happens to anyone's systems without their written yes first holds even for the free scan Ghost Protocol leads with. A free scan is a scoped, agreed, bounded action offered and accepted in advance, never a surprise test sprung on a prospect to impress them with what you found. An unrequested test is an unauthorised one, however good the sales instinct behind it. The wider industry has turned this ethic into a mechanism: a responsible scanning service will not fire an active probe at a domain until the user has proven they control it, by placing a token in DNS or at a known path on the site. That proof is consent made technical, the owner demonstrating in advance that the target is theirs to offer. The shape of the rule is the same whether it is a signature or a DNS record. The agreement exists before the probe, or the probe does not happen.

Consent is a boundary you stay inside, not a gun that Fires once

A signed authorisation is not a starting gun after which everything is permitted until the end date. It is a boundary you stay within for the whole engagement, and it describes a particular test the client pictured when they agreed. If, mid-engagement, the shape of the work changes, you need to reach something not named, a technique the client did not picture, a system a hop further out, then the original consent does not stretch to cover it. You stop at the edge, go back, explain the change in plain terms, and get the agreement extended in writing before you cross. Consent grows by asking again,