



GHOST
PROTOCOL



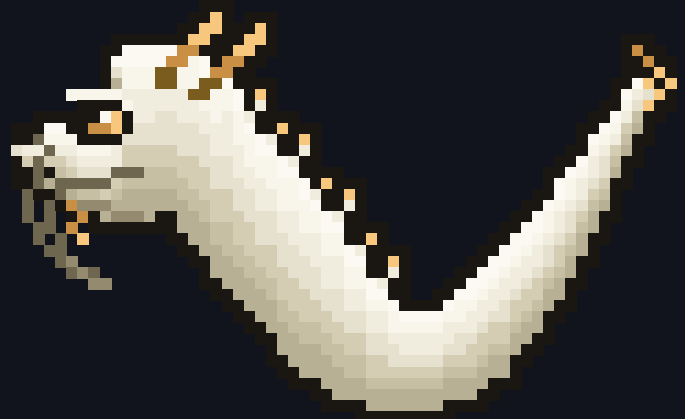
THE FIELD LIBRARY

VOLUME 0

READ FIRST · BEFORE ANY TECHNIQUE

The Oath

The one law of this work, and the clean
way to stand in it.



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

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

THE GHOST PROTOCOL FIELD LIBRARY · VOLUME 0

The Oath

The one law of this work, and the clean way to stand in it. Read before any technique in any volume.

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 Core Path

The Core Path: six volumes, read in order. Each one makes you able to do something the last one did not, and no volume skips the one before it. You are holding Volume 0. It is the shortest and the most important, because everything in the others is built on it.



The Oath YOU ARE HERE

The one law: you test only what you are authorised, in writing, to test. The Sri Lankan law behind it, the rules of engagement, and clean conduct. Read first.



Groundwork

How the web and the network actually work, how an attacker reasons, and the home lab you build before you touch anything. You cannot test what you do not understand.



The Web

The deep core. Reading a web application, the vulnerability classes as mechanisms, the tools as instruments, and the one habit that outranks them all: verify every finding before you believe it.



The Wider Field

Beyond the web at working awareness: network and infrastructure, cloud, APIs, mobile, wireless. What each is, how it differs, and where to go deeper.



The Work

Winning legitimate clients, scoping an engagement into written authorisation, running it, and writing the report the client actually pays for.



The Craft

Becoming genuinely good and staying clean while you do: judgment under uncertainty, how to keep getting sharper, and the standards that separate a professional from a script-runner.

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 YOU ARE HERE

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 BUILT

The Lab Workbook BUILT

Case Files BUILT

The Bestiary BUILT

The Glossary and the Ledger BUILT

Contents

·	Induction	6
1	The One Rule	7
2	The Law	9
3	The Rules of Engagement	11
4	Clean Conduct	14
5	The Ghost's Oath	16
·	Worked answers	18

The night you arrived



You came in after dark, which is the right time to arrive. The studio was quiet the way a good watch is quiet: the terminal glowing, a cup going cold, the city dark in the window.

Something silver was asleep on the warm laptop, a pen-nib tail across the keys. That is Wyrn, which has read every report this house ever filed and forgotten none of them, each dated and numbered in a ledger it never closes. The pale one at the desk looked up when you came in. That is Sol, who keeps the watch.

SOL "Before anyone here asks whether you can break into a thing, they ask whether you are allowed to. Get that one wrong and nothing else you learn counts. That is this whole first book."

At the prompt, a cursor was already bouncing: Blink, who says yes to everything.

BLINK "Pick a target, any target, let's scan something, should I start?"

One green eye opened, just one, in all that grey, and looked at what Blink had half typed.

WYRM "no."

Blink stopped. Sol only nodded, and your first night had started.

CHAPTER ONE

The One Rule

Everything in the rest of the Library sits on top of a single sentence. Learn it until it is a reflex, not a rule you remember.

You test only what you are authorised, in writing, to test. That is the whole of it. Every technique in every other volume is permitted by that sentence or forbidden by it, and there is no third case.

It sounds small. It is not. Almost everything that ends a security career, or starts a criminal one, is a version of forgetting it: testing a system that felt in-scope but was not, reaching one hop further than the paper allowed, running a scan against a client before the signature was dry, helping a friend "just check" a site that was never yours to touch. None of those feel like crimes while you do them. The law does not care how they feel.

Authorisation is binary

You either have permission for a given action against a given system, or you do not. There is no "probably fine", no "they would not mind", no "it is only a look". A door is locked or it is not, and the fact that you can open it tells you nothing about whether you are allowed to. The skill to get in and the right to get in are two different things, and this work only exists in the narrow place where you have both.



no.

The question is never "can I reach this?" It is "does my paper cover this?" If you cannot answer the second one from the paper in front of you, you have already heard the only word Wyrm needs to say. Stop and check before the next request.

There is a useful way to think about this that comes from a court case abroad. In the United States, **Van Buren v. United States** (2021) settled that access is judged by whether you were entitled to reach a thing at all, a gate you are either through or not, rather than by your private reasons for reaching it. That is a mental model, not Sri Lankan law, and this book flags it as such. But the shape is right everywhere: authorisation is a gate, and you are on one side of it or the other. Your intentions do not move the gate.

Authorisation is scoped

Permission is never general. It is for specific systems, named plainly: these hosts, these URLs, these IP ranges, these test accounts, inside this time window, excluding everything not listed. "You can test our website" is not a scope; it is the start of a conversation that ends in one. The scope says what is in, what is explicitly out, who may authorise it (the person who owns or controls the asset, not a friend who happens to work there), and when. Anything outside the written scope is outside your permission, even if it belongs to the same client, even if it is one link away, even if it would take ten seconds.

Authorisation is in writing

A verbal yes is not a scope. People misremember, deals fall through, and the person who said "go ahead" on a call is not always the person who can actually grant it. Ghost Protocol tests under a written **Test Authorisation**: a signed document, from someone with the authority to sign it, naming the scope and the window. No signature, no test. Volume IV shows you how one is built and what it must contain. Here, you only need the habit: before the first packet, the paper exists and you have read it.

■ THE LINE

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

- 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 "mostly" is a no.

None of this is meant to make you timid. It is the opposite. A professional who knows exactly where the line is works with a freedom an amateur never has, because the amateur is always half-worried and the professional is never worried at all. The paperwork is not the cage. It is what lets you take the gloves off inside the ring.

■ ON YOUR FEET

A friend messages you: their small company's website "has been acting weird" and could you "just take a quick look and see if it is hackable, between us". They are a real friend. They do work there. They are not the owner, and there is nothing in writing. What do you do, and what do you say to them?



WHAT WYRM KEEPS

You test only what you are authorised, in writing, to test. Skill is not permission. A locked door you can open is still a door you may not.

- Authorisation is binary (you have it or you do not), scoped (named systems and a window), and written (a signed Test Authorisation).
- Van Buren is a mental model from US law, not Sri Lankan law: a gate you are through or not. Flagged, not relied on.
- Three yeses before any packet, or you do not touch it.

CHAPTER TWO

The Law

Why the one rule is not just house policy. In Sri Lanka, unauthorised access to a computer is a crime, and wanting to help is not a defence.

Ghost Protocol is a Sri Lankan company, and the ground under this work is Sri Lankan law. You do not need to be a lawyer. You need to know, exactly, the one place the law touches what you do every day: it treats getting into a computer you were not allowed into as a criminal act, on its own, with no damage required.

The Computer Crime Act, No. 24 of 2007

Sri Lanka's **Computer Crime Act, No. 24 of 2007** is the statute that matters most to a tester. Its opening offence is the one that should live in your bones.

Section 3, unauthorised access. Intentionally securing access to any computer, or to any information held in a computer, knowing or having reason to believe that you have no lawful authority to do so, is an offence. On conviction it carries imprisonment for a term that may extend to five years, or a fine that may extend to one hundred thousand rupees, or both. Note what is not in that sentence: you do not have to steal anything, change anything, or cause any harm. The access itself is the crime. "I only looked" is a description of the offence, not a defence to it.

Section 4, access to commit a further offence. Where the unauthorised access is made with the intention of committing another offence, under this Act or any other law (fraud, causing damage, and the like), it is a separate offence with a higher ceiling: a fine that may extend to two hundred thousand rupees, or imprisonment for a term that may extend to five years, or both. The ladder is deliberate: the law is harder on access that is a means to something worse.

■ A NOTE ON HOW TO READ THIS

This chapter is Ghost Protocol's working understanding of the law for the purpose of operating cleanly. It is not legal advice, and statutes are amended over time. The exact sections, figures, and their current wording are confirmed with counsel, and any real question about what the law permits goes to Ryan, not resolved by you at the keyboard. What never changes is the direction of the rule, and that is what you carry.

There is a second thing the Act makes plain by its silence. It contains no general exception for research, curiosity, or good intentions. Some countries are building narrow protections for security researchers acting in good faith. Sri Lanka, as this is written, is not one of them. So your mindset here is the strict one: assume there is no "but I meant well" clause, because there is not, and then you never need one. Your protection is not your intent. Your protection is the signed authorisation that made the access authorised in the first place.

The law here does not reward a good heart. Nowhere in it is there a line that begins "unless you were only trying to help." Work as though there never will be, and the paperwork stops feeling like a burden and starts feeling like the thing standing between you and five years.

Personal data: the PDPA, No. 9 of 2022

During a test you will often come across personal data: names, numbers, records of real people. Sri Lanka now has a law about how such data is handled, the **Personal Data Protection Act, No. 9 of 2022**. It establishes a Data Protection Authority and a set of obligations for anyone who controls or processes personal data. Its core compliance regime is set to commence on 1 January 2027, so it is arriving rather than fully arrived as this edition is written, and that date is the one to hold.

For you, the practical effect is simple and does not wait for any date. Personal data you encounter in a test is not yours, is not a trophy, and is handled under Ghost Protocol's data rules in the next chapter: you take only what proves the finding, you store it where the engagement says, and you destroy it when the engagement ends. The PDPA raises the stakes on getting that wrong; it does not change what "right" looks like for a professional, which was always the same.

■ THE LINE

If you are ever unsure whether something is lawful or authorised, that uncertainty is itself the answer: you stop. A legal doubt is never resolved by proceeding and seeing what happens. It is resolved by asking Ryan, before the action, in writing. The cost of asking is a few minutes. The cost of guessing wrong is in Section 3.



WHAT WYRM KEEPS

In Sri Lanka, getting into a computer you were not allowed into is a crime by itself, with no damage required and no good-intentions defence.

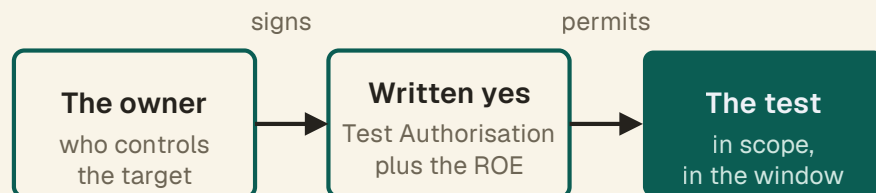
- Computer Crime Act No. 24 of 2007, s.3: unauthorised access is an offence (up to five years, or a fine up to Rs 100,000, or both). s.4: access with intent to commit a further offence carries a higher fine (up to Rs 200,000) alongside the same five years.
- No research or good-faith exemption exists here. Your protection is the signed authorisation, not your intent.
- PDPA No. 9 of 2022 governs personal data; core compliance commences 1 January 2027. Handle personal data as evidence, minimally, and destroy it at the end.
- Any real legal doubt goes to Ryan before the action, never resolved at the keyboard.

CHAPTER THREE

The Rules of Engagement

The authorisation says you may test. The rules of engagement say how. They are the difference between a professional on a job and a stranger loose in someone's systems.

A written authorisation gives you the right to test. The **rules of engagement**, the ROE, give you the shape of the test: what is in scope, what is out, when you may work, what you may and may not do, who you talk to, and the handful of moments where you stop everything and pick up the phone. Volume IV teaches you to write one. This chapter teaches you to live inside one, because you will be held to it long before you are trusted to draft it.



No step may be skipped. No written yes, no test.

The owner signs the authorisation and its rules of engagement, and only then does the test begin, in scope and in the window.

What the ROE pins down

- **Scope.** The exact systems in play, named as hosts, URLs, IP ranges, and test accounts, and an explicit list of what is out. Out of scope is as binding as in scope. The subdomain that is not listed is not yours, however tempting.
- **The window.** When you may test. Outside the agreed window you do nothing, even reconnaissance. Some clients want testing only at night, or not during a sale, or not on their busiest day. That is their call and it is in the paper.
- **Permitted and forbidden techniques.** What you may do to the systems in scope. Denial of service, anything destructive, social engineering of staff, and touching real customer data are off the table unless the ROE names them as allowed. When in doubt, a technique is forbidden until the paper says otherwise.
- **Communication.** Who your point of contact is, how to reach them fast, and how often you report in. You are never a silent presence in someone's systems for a week.

The stop-and-report triggers

A professional test has a small set of moments where the correct action is not to press on but to halt and tell your contact at once. Memorise them. They override your curiosity and your deadline both.

- You find evidence that someone else is already inside, a real intrusion in progress or past. You are now standing in a possible crime scene. Stop, do not touch it, report immediately.
- 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.
- You realise an action could cause an outage or data loss. Stop before it does, not after.
- You encounter especially sensitive data: medical records, financial details at scale, anything about children, anything whose exposure could hurt real people. Take the minimum to prove it exists, and report.
- You find something that could endanger a person's safety. People before findings, always.

Notice the shape of all five: the instinct to "just keep going a little to be sure" is exactly the instinct to override. Being sure is the client's problem to resolve with you, not yours to resolve alone by digging deeper into the thing you were told to stop at.



SOL SAYS

The best testers are not the ones who went furthest. They are the ones who knew the exact moment to stop and did it without being told. Stopping well is a skill. Practise it like any other.

How you handle what you find

Everything you touch during a test belongs to someone else. Treat it that way.

- **Take only what proves the finding.** One screenshot that shows the access, one record that demonstrates the flaw, not the whole table. Evidence, not loot.
- **Store it where the engagement says, and nowhere else.** No copies on your personal machine, no pasting into a chat, no "I will clean it up later".
- **Destroy it at the end.** When the engagement closes, the client's data leaves your hands. You keep the report, not the spoils.
- **Never keep a souvenir.** The screenshot you kept because it was impressive is the thing that ends you. There are no trophies in this work.

No client, no prospect, without a written yes

This holds even for the free scan Ghost Protocol leads with. 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. We never test a client's or a prospect's systems to "show them what we found", however good the inten-

tion or the sales instinct. An unrequested test is an unauthorised one, and an unauthorised one is Chapter Two. Volume IV covers the conversation around the free scan; the rule itself lives here.

■ ON YOUR FEET

Two days into an authorised web test, you find a web shell that you did not place and that predates your engagement. Someone was here before you. Your report is due Friday and you are behind. What do you do in the next five minutes, and what do you not do?



WHAT WYRM KEEPS

The authorisation says you may. The rules of engagement say how, and the first skill inside them is knowing the moment to stop.

- The ROE fixes scope (in and out), the window, permitted techniques, and communication. Out of scope binds as hard as in scope.
- Five stop-and-report triggers: another intruder, out-of-scope access, risk of outage, highly sensitive data, danger to a person. Halt and report; do not "keep going to be sure".
- Handle findings as evidence: take the minimum, store it where told, destroy it at the end, keep no souvenirs.
- No scan of any client or prospect, not even the free scan, until someone with authority over the target has said yes in writing.

CHAPTER FOUR

Clean Conduct

Ghost Protocol wins on the merits, and only on the merits. This is the ethic, and it is also, quietly, the strategy.

You will spend your days finding the weak points in other people's defences and the private things behind them. That access is a kind of power, and the whole of your professional character is in what you refuse to do with it. Ghost Protocol's standing rule is short: we win on the merits, full stop. The work speaks. We never reach for leverage outside it.

Honesty in the work itself

The first place conduct shows is the finding. You do not inflate a medium into a critical to look impressive, and you do not soften a critical into a medium to keep a client comfortable. A severity is an honest judgment, argued from evidence, and it reads the same whether or not it flatters anyone. The intern's most common failure, and not only the intern's, is a claim the evidence does not support. In this house that is not a small slip. A report that overstates is a report that lies, and a tester who lies once is worth nothing afterwards, because no one can tell which of your trues is true.



where?

If you cannot point at the evidence, you do not have a finding, you have a feeling. Feelings do not go in the report, and Wyrms will not file a claim it cannot see.

Never leverage

Sometimes the access hands you something that is not a security finding at all: a counterparty's private embarrassment, an unrelated regulatory exposure, a personal secret. The temptation, in a dispute or a negotiation, is to let it be known that you know. Do not. Never a "settle this, or the wrong people hear about that". Never the soft version of it, the hint, the shame-if-your-regulator-found-out. Threading a threat of disclosure into a demand is not sharp negotiating. In most places it is a crime in its own right, an unwarranted demand with menaces, and it does something even worse than the legal risk: it turns us from the party in the right into the party in the dock, and torches the very claim we were owed.

If a genuine legal or regulatory violation really does exist, reporting it to the proper authority is a separate decision, made for proper reasons, and walled off completely from anything we want out of a dispute. The two are never threaded together. We negotiate firmly on the facts and let the strength of a clean party with a real case do its own work, because it does.

■ THE LINE

The moment a conversation, a draft, or your own thinking starts to connect "a thing we could reveal about them" with "a thing we want from them", stop. That connection is the line, and it does not matter how softly it is drawn or how good the cause feels. Take it to Ryan. We do not send it, we do not hint it, we do not keep it in our back pocket.

Confidentiality

What you see inside a client's systems stays inside the engagement. You do not brag about it, you do not name the client in a story at a meetup, you do not screenshot the funny thing for a group chat. Clients let us in because they trust the house to be silent about everything except the findings they are paying to hear. That silence is not a courtesy. It is the product.

Why clean is also the clever move

None of this is only morality. Credibility is the one asset in this work you cannot buy back once it is gone. A reputation for being straight, for never overstating, for never playing dirty even when dirty would have won the round, is the thing that brings the next client and the one after. The leverage of a clean party with a real case accrues on its own. We let it. In a small market like ours, where everyone eventually hears about everyone, the clean operator is not just the decent one. Over any length of time, the clean operator is the one still standing.

■ ON YOUR FEET

Mid-test, inside the authorised scope, you stumble on something that is not a security issue at all: evidence that a senior person at the client is doing something embarrassing and probably against company policy, but unrelated to the systems you were hired to test. It is not your finding to make. What do you do with what you saw, and what do you not do?



WHAT WYRM KEEPS

We win on the merits, only on the merits. Never leverage what the access showed you. Credibility is the one thing you cannot buy back.

- Findings are honest: never inflated to impress, never softened to please. A claim with no evidence is not a finding.
- Never thread a threat of disclosure into a demand, not even softly. Any genuine report to an authority is a separate, walled-off decision, taken to Ryan.
- What you see in a client's systems stays in the engagement. The silence is the product.
- Clean conduct is the ethic and the strategy both: in a small market, the clean operator is the one still standing.

CHAPTER FIVE

The Ghost's Oath

The four chapters, compressed into something you can hold in your head and hold yourself to. Not a form for anyone else. A promise you make to the person at the keyboard.

Everything in this volume comes down to seven lines. They are not a contract and no one will file them. They are the shape of the professional you are deciding to be, written plainly enough that on a tired night, behind on a report, one request away from somewhere you were told not to go, you will remember exactly where you stand.

The Ghost's Oath

GHOST PROTOCOL · THE LONG WATCH

- 1 I test only what I am authorised, in writing, to test. Skill is not permission.
- 2 I treat authorisation as binary and scoped. Three yeses before any packet, or I do not touch it.
- 3 I know the law I work under, and I never settle a legal doubt by carrying on. I ask first.
- 4 I live inside the rules of engagement, and I stop and report the moment one of the triggers is met, even when I would rather press on.
- 5 I handle what I find as evidence, not as loot. I take the minimum, store it where I am told, destroy it at the end, and keep no souvenirs.
- 6 I win on the merits and never on leverage. I keep the client's silence, and I take any threat that creeps into a demand to Ryan.
- 7 I verify every finding before I believe it, and I never write a claim my evidence cannot support.

Signed, the new ghost

Date

Read them once more, slowly. Then carry on into Groundwork, where you learn how the machine actually works, because the oath only protects a person who also knows what they are doing. The line keeps you a professional. The craft makes you one.



SOL SAYS

You will break plenty of things in the years ahead, all of them with permission. None of that is what makes you one of us. This page is. Keep it, and the rest of the Library is yours to use without ever looking over your shoulder.

The First line



By the time you had read the oath through twice, the studio had gone quiet again. Then, without being asked, Wyrms nib tail lifted off the desk.

One line, dated and numbered, at the top of a fresh page with your name on it. You did not get to read what it wrote. You only knew it was written now, and that Wyrms never crosses anything out.

BLINK "Ooh, your first entry. Do not worry about what it says. Mine was not flattering either. The trick is to never give it the same thing to write twice."

WYRM "logged."

The tail came down. The eye closed to its thin curve. Blink was already brightening towards tomorrow, which with Blink is always a scan, a tool, a thing to try right now.

Tomorrow you build your lab and learn how the machine actually works, so that your bold ideas land on your own targets and never in Wyrms ledger. Tonight, for the first time and with permission, you are on the watch.

WORKED ANSWERS

On your Feet, answered

These scenarios have no single clean answer, but each has a clearly professional one, and a clearly wrong one. Try each yourself before you read the standard the house judges it against.

Chapter One: the friend who asks you to "just take a quick look"

You say no, and you say it warmly, because the friend is not the problem. There is no written authorisation from someone who owns or controls that system, so there is no test, and "between us" changes nothing. A quick look is still unauthorised access, still an offence under the Computer Crime Act, and you would be putting both of you at risk, not helping.

The professional move is to decline the favour and offer the real path in its place: if their company genuinely wants to know, the owner can authorise a scoped scan, in writing, and Ghost Protocol will do it properly. The friendship is not a scope. The clearly wrong answer is the five-minute look you talk yourself into because it felt harmless.

Chapter Three: the web shell that predates your engagement

You stop, immediately, and you do not touch it. That shell is potentially evidence of a real intrusion and possibly a crime scene; deleting it, triggering it, or poking at it could destroy evidence or alert whoever placed it. You do not continue testing in that area. You contact your point of contact at once, by phone, and report exactly what you found, where, and when, with timestamps, and you preserve your own logs of how you found it.

From this moment it is likely an active security incident, and what happens next (incident response, and possibly law enforcement) is the client's decision to make with you, not yours to pre-empt by digging. Your Friday deadline is irrelevant and you say so. You also write down that you stopped and the time you stopped, because a clean account of your own actions is part of the evidence too.

Chapter Four: the embarrassing, unrelated thing you saw

It is not your finding and it is not in your scope, so it does not become a thing you hold. You do not screenshot it, collect it, put it in the report, mention it in a chat, or file it away in case it is ever useful. The access did not make it yours.

If what you saw is mere embarrassment or a breach of company policy, you let it go and keep the silence, because the silence is the product. If, and only if, it is a genuine and serious legal or safety matter, that is a separate decision, taken to Ryan, made for proper reasons, and walled off completely from the engagement and from any advantage to us. The one path that ends your career is the one where "a thing I could reveal about them" ever gets connected to "a thing we want". It never does.