

THE POLICY EVERY BUSINESS NEEDS

Bring Your *Own* AI

Let them bring it. Build the gate. Keep the ledger.

JOHN RECTOR

First digital edition, October 2026

Bring Your Own AI. Copyright 2026 John Rector. Published at johnrector.me, Charleston, South Carolina. Free to read and share unaltered.

This book is not legal advice; have counsel review the model policy before adopting it. The scenes are invented teaching examples. Facts about the world were checked against the sources listed at the end on October 30, 2026.

Online edition, PDF and EPUB: <https://johnrector.me/>

Contents

i About this edition

ii Introduction: The badge and the backpack

PART ONE: WHY THEY BRING IT

1 The model of one person

2 People do not adopt what watches them

3 We have done this before

PART TWO: THE LINE

4 Two kinds of knowledge

5 A gate, not a wall

6 The law in plain words

PART THREE: THE POLICY

7 What the policy must say

8 The first day

9 The last day

10 When a line is crossed

PART FOUR: RUNNING IT

11 Manager, not user

12 What the IT function becomes

13 The five-person company

14 Objections, answered

PART FIVE: A FUTURE YOU CAN FEEL COMING

15 Six predictions

16 A letter to the owner

17 The backpack

APPENDICES

A The policy

B The claim ledger

C The working cards

D A small glossary

E Sources and development

About this edition

This is an original short book. I wrote it with AI assistance, the way I now do most things, and the argument is mine. It is written for the person who runs a business, or runs part of one, and who has noticed that the people they hire now arrive with an AI of their own. It is not legal advice. Where the book touches trade secrets, employment law, privacy or recording consent, it describes the shape of the rule in plain words and tells you to ask a lawyer who knows your jurisdiction and your industry.

The policy in the appendix is a model, not a template to sign unread. Adopt it the way you would adopt a model lease: read every clause, strike what does not apply, add what your industry requires, and have counsel look at the result. The scenes in the book are invented teaching examples unless I say otherwise; the roofing company and its estimators, the analyst with two years of method in a personal account, the new hire on her first Monday, all of them are composites built from rooms I have sat in. Their numbers illustrate decisions. They do not report measurements.

The facts about the world were checked against the sources listed at the end on October 30, 2026. The book does not claim to have read everything published by that date, and the law in this area is moving while you read.

The book is published by John Rector at johnrector.me. This edition has no ISBN. The online and PDF editions carry the same text. The online edition adds navigation, the working cards and the claim ledger in a form you can keep open.

Introduction: The badge and the backpack

HER FIRST MONDAY, 10:20 A.M.

The new company hands her a laptop with its own AI already installed. It is capable and courteous and it knows nothing about her. By twenty past ten it has asked her three questions the AI she left behind would never have asked, because that one knew she settles that kind of thing in her sleep. At 10:40 the onboarding checklist asks her to sign a page that says she will not use any AI the company did not issue. She signs it. She has a backpack under the desk with her own laptop in it, and her own AI on that laptop, and two years of method inside that AI, and she already knows which one she will use for the real work.

Every business I talk to is about to have that Monday, if it has not had it already. The person you hired arrives with an intelligence of their own. It is not a tool they downloaded. It is a working relationship they have been building, often for years, with a frontier model that has watched them work, learned how they decide, and holds a model of them that no company system will ever hold. They bring it the way they bring their judgment. And then the company asks them to leave it at the door.

They will not. The numbers say so and so does every room I have sat in. Two years ago, in a global survey of knowledge workers, more than three quarters of the people using AI at work said they were bringing their own; this spring a survey of twelve thousand employees found that nearly nine in ten of those who had been given an enterprise AI were using a personal

one as well. What they will do instead is sign the page, use the issued AI for the mandated work, and do the real work with their own. The company will record the first as adoption and never see the second. That is the worst of both worlds: the risk of an ungoverned boundary with none of the benefit of the better work.

This book is about the alternative, which I have been arguing for in pieces for some time and now want to set out whole. Let them bring their own AI. Write a policy that says so. Make the policy real with a gate: a visible, permissioned boundary between the person's intelligence and the company's systems, so that every transfer across it is limited, logged and attributable. Draw one line, and draw it clearly: the company's facts stay in the company's systems; the person's methods, and the model their AI holds of them, leave with the person.

I call this Bring Your Own AI, after the phrase that settled the last version of this fight, when the phones arrived. The companies that fought the phones lost a decade and then wrote the policy anyway. The companies that wrote it first got a workforce that worked from everywhere with the instruments it knew best. This is the same fight with higher stakes, because a phone holds your contacts and your AI holds your method.

The book has five parts. The first says why people bring their own, from first principles rather than preference. The second draws the line: what is the company's, what is the person's, and what a gate between them actually consists of. The third is the policy itself, clause by clause, with the first day, the last day and the day something goes wrong. The fourth is about running it: what managers do, what the IT function becomes, what the five-person company does instead of all this. The fifth is the future I am betting on, stated so it can fail. The complete policy is the first appendix, ready to be read, cut and adopted.

One thing before we begin. Nothing here asks you to care less about your data, your customers or your obligations. It asks you to protect them with a control instead of a document. A page that says do not use your own AI is a document. A gate that decides what an AI may touch, and writes a receipt when it does, is a control. Most companies have bought the document and called it the control. This book is about building the control, and the strange discovery most of them make when they do: the people they were trying to restrain turn out to be the people doing the best work in the building.

PART ONE: WHY THEY BRING IT

1

The model of one person

In 1945 Friedrich Hayek published a short essay arguing that the problem of running an economy is not a problem of calculation. If all the facts were in one place, any competent planner could do the arithmetic. The problem is that the facts that matter most are never in one place. They are, in his phrase, the knowledge of the particular circumstances of time and place, scattered and mostly unwritten, held by the person on the spot. A system works when it lets that knowledge be used where it lives. It fails when it tries to collect it at the center.

I have argued elsewhere that this is the deepest reason personal AI wins, and I want to restate it here because everything in the policy follows from it.

What an AI needs in order to help you

Watch what a good AI actually does for a person over a year. It learns when they are sharp and when they are not. It learns which decisions they find hard and which they have made four hundred times. It learns their vocabulary, their shortcuts, the mistakes they make under pressure and the checks they have built to catch them. It learns that they answer email in batches at two, that they will not call a customer before nine, that when they say “clean this up” they mean three specific things. That is a model of one person, and it is the entire source of the AI’s usefulness. An AI that knows the job and not the person is a polite stranger. It will ask the questions a colleague of two years would never ask.

Now notice where that model gets built. Mostly outside work. Whether someone is sharp on Thursday morning depends on how they slept, on the child who was up at three, on the conversation in the car. The methods they bring were refined on their own time, on their own problems, across three previous employers. The company does not see those things and should not. An AI the company owns is sorting the person’s day with half the model missing, and it will always be missing, because the only way to fill it in would be to watch the person’s whole life, and nobody will allow that from an instrument that answers to their employer.

It compounds only if it travels

The second half of the argument is about time. A model of a person gets better every week it watches them work. Its value is the sum of everything it has learned. If that model lives in the company’s system, the sum starts at zero with every new hire and is abandoned at every departure. The person’s experience walks out the door; the model of that experience stays

behind in an account nobody will open again. Everyone loses: the person starts over, the company inherits a stranger, and the stranger spends its first months asking questions.

If the model lives with the person, it arrives on the first day already knowing them and leaves on the last day knowing more. The company gets a worker whose assistant is already trained. The person keeps the thing that compounds. The only thing the company gives up is ownership of something it could never have used anyway.

The one condition

There is a condition, and it is the hinge of this whole book. A person will only let an AI see the parts of their life that build the model if the AI works for them. The only agent that can know a person well enough to help is one that answers to that person. So the better the AI, the more certain it is that it must be the person's own. That is not a preference. It is a consequence of what the model is made of.

Which means the question for a business is not whether its people will bring their own AI. They will, because the useful one is theirs by construction. The question is whether the business will build a boundary good enough to let that AI do the company's work safely. Everything from here on is about that boundary.

People do not adopt what watches them

A small-business owner described a proposal to me that I have now heard in a dozen forms. His company has about thirty employees. Several are estimators who spend their days in homeowners' kitchens and driveways, and those conversations hold nearly everything the business needs: the condition of the roof, what the homeowner noticed, what was promised, what materials the job will need. A vendor offered the obvious thing. An app on every estimator's phone. Record the conversations. Let AI produce the notes, the proposal, the training examples. Feed it all into the company.

On a slide it was perfect. In practice he could not get anyone to use it.

The hidden design variable

Put yourself in the estimator's place. A system chosen by your employer is listening to your whole conversation with a homeowner. You do not know where the recording goes, who can pull it up, how long it stays, whether it will be used to score you, or which awkward sentence becomes a training example. You are told it is there to help. Architecturally it feels like it is there to watch. So the battery dies. The microphone fails. The important meeting happens in the one room where the phone was left outside.

This is not resistance to innovation. It is a rational response to an illegible boundary. If a system requires people to invent reasons for not using it, the failure began in the architecture, not in the training session. The company modeled the estimator as one of many identical endpoints. The estimator

experiences himself as a human being in a conversation with another human being. That difference is the whole problem, and no amount of change management closes it.

The inversion

Now invert the architecture. The estimator uses his own AI, in an environment that is legibly his. After six homeowner visits he says: use today's six conversations to draft the proposals, keep every detail that affects scope and price, put the drafts in front of me, and after I approve them create the opportunities in the company's system. The raw conversations never become the company's ambient memory. The company receives exactly what it needs, an approved proposal and an accurate customer record, with clear provenance. The estimator keeps a durable capability that works on his HOA meeting and his daughter's science fair as well as on roofs, and he knows exactly what crossed the boundary, because he approved it.

Send the work product. Do not annex the person. The company that insists on the raw feed collects more and gets less, because the surveillance feeling contaminates the useful workflow. The company that asks only for the finished thing gets better work from people who keep using the instrument, because it is theirs.

Why this is a principle and not a preference

I state it as a law because I have never seen it fail. People do not adopt what watches them. They adopt what works for them. A mandate can produce logins; it cannot produce use. A chief operating officer I know put a slide up with two numbers on it, four thousand seats issued and three hundred and ninety weekly active users, and asked the room how to close the gap. The room treated it as an adoption problem. It was not. Her people used AI all day. They were just not using hers.

The Bring Your Own AI policy is simply the architecture that takes this law seriously. It does not try to make people use the company's instrument. It builds the one thing the company genuinely owns, the gate between the person's intelligence and the company's systems, and lets the person's instrument do the company's work through it.

We have done this before

Around 2009 a large technology company noticed that its employees were bringing their own phones to work and connecting them to company email, and decided, against the instinct of its security function, to permit it under rules rather than forbid it. Within a few years the practice had a name, bring your own device, and every company on earth had a policy about it. The policies converged on the same shape, because the problem had one honest solution.

What the phone fight taught

The first instinct everywhere was prohibition. Issue the company phone, forbid the personal one, and treat anyone who connected their own as a violator. It failed for the same reason the mandated AI fails. People's own phones were better, more familiar, and already in their pockets. They connected them anyway, and the prohibition's only effect was to make the connection invisible to the company. Security got worse, not better, because the company was now governing nothing.

The second phase was accommodation without architecture. Allow the personal phone, ask people to be careful, and hope. That was the era of lost phones with the customer list on them, and it produced the thing that finally worked.

The third phase was the boundary. The settled BYOD policy had three parts. The device is yours. Company data on the device lives in a container the company controls. The company can wipe the container without touching your photos, and must. Add identity, a list of what the container

may reach, and a log, and you have the policy that every company runs today without thinking about it. The fight ended not when companies won or lost but when the boundary became legible enough that both sides could trust it.

The same shape, higher stakes

Bring Your Own AI is the same fight with the stakes raised, and it will settle the same way. The AI is yours. Company facts that pass through it live behind a gate the company controls. The company can revoke the gate without touching your method, and must. Identity, a catalog of what the gate permits, and a receipt for every action: the container, translated.

The stakes are higher in two directions. A phone held your contacts and your email; your AI holds your method and a model of how you think, which is a far more valuable thing to be asked to surrender. And a phone could only read and display; an AI can act, which means the gate has to decide not just what may be seen but what may be done, by whom, in what scope, and what happens if it was wrong.

Why the companies that moved first won

The companies that wrote the phone policy first did not do it out of generosity. They did it because the people they most wanted to hire were the ones who would not work without their own instruments, and because a legible boundary is cheaper to run than an illegible one. They got a decade of a workforce that worked from anywhere with the tools it knew, while their competitors ran help desks for devices nobody wanted.

The same is about to happen here, faster. The people with two years of method in a personal account are the ones you least want to lose and the ones most certain to leave over a mandate. Write the policy first, build the

gate, and you recruit them. Wait, and you will write the policy anyway in a few years, after the best of them have gone to the company that wrote it first.

PART TWO: THE LINE

4

Two kinds of knowledge

Every argument about AI at work eventually comes down to one question: whose is it? And the question is unanswerable until you notice that two different things are being asked about at once.

Facts and methods

The first kind of knowledge is the company's facts. The customer list. The pricing sheet. The contract under negotiation. The source code. The margin on the Henderson job. The plan for next quarter. These are stored in

systems the company built, they are often confidential, some of them are trade secrets in the legal sense, and the company has every right, and in many cases a legal duty, to say where they may go and who may see them.

The second kind of knowledge is the person's method. The way they scope a job. The questions they ask a new client. The checklist they run before they say done. The prompts they refined over eleven months. The file of their own mistakes and the catches they built against them. And, now, the model their AI holds of them: when they are sharp, how they decide, what "clean this up" means when they say it. This knowledge was built across years and employers, largely on their own time, and it is theirs in the way their judgment is theirs.

Most AI policies fail because they treat these as one thing. The prohibition policy treats the person's method as if it were a company fact, and tries to confiscate it. The free-for-all treats company facts as if they were personal method, and lets them walk. Both are category errors, and both produce the same result: the person protects what is theirs by going dark, and the company's facts leak through the darkness.

The two-column test

Here is the test I give every client, and it fits on an index card. Draw two columns. On the left, what the company owns: facts, records, customer data, work product the company paid for, anything a court would call a trade secret. On the right, what the person owns: method, skill, templates built on their own time, their AI's model of them, the general lesson of every job they have done. Now take any piece of information that passes through the person's AI and ask which column it belongs in.

A customer's phone number is left. The way the person handles a difficult customer is right. The proposal for the Henderson job is left. The questions the person asks every homeowner are right. The log of what the person's

AI did inside the company's systems is left. The log of how the person's AI learned to work with them is right.

The policy's whole job is to keep the columns separate: left-column information stays in the company's systems or passes through a gate the company controls, and right-column information lives in systems the person controls and leaves with them. Almost every hard case gets easy once you ask which column it is in.

Standards and procedures

One more distinction, because it settles most of the arguments that remain. A company has every right to set standards: what finished means, what reviewed means, what confidential means, what may not leave the building, what must be kept for seven years. Standards are sacred. A company has no business specifying the instrument: which model, which prompts, which workflow, how the person gets from the problem to the finished thing. Procedures are negotiable, and the person's procedures are their own.

When a policy says "all AI work must be done in the approved tool," it has confused a procedure for a standard. When it says "all work product sent to a customer must be reviewed by a person who signs it," it has stated a standard, and it is a good one, and it is entirely compatible with the person using whatever instrument they like to get there.

A gate, not a wall

A policy is a document. A gate is a control. The difference between a company that has an AI policy and a company that governs AI is the gate, and in most organizations the gate does not yet exist in one piece.

Three layers

Every business of any size has spent decades building systems of record: the ledger, the customer database, the HR system, the ticketing queue, the document store. These hold the facts. They are not going anywhere and they were never the contested ground.

Above them, unevenly and mostly by accident, a second layer is being built: the place where an intention becomes a permitted transaction. Call it the system of action. It is the surface where something outside the company asks to change something inside it and gets an answer that is either a receipt or a refusal. This layer is the only part of the whole arrangement the company genuinely owns. Not the model. Not the interface. Not the person's method. The gate.

Above that is the third layer, which belongs to the person: their intelligence, their memory, their prompts, their agents, their accumulated method. It arrives on the first day and leaves on the last. It asks the gate to act. The gate decides.

What a gate consists of

The engineering is unglamorous and finite, and I will list it because the list is the policy's technical appendix. Identity: the gate knows which person, and which AI acting for them, is asking. A capability catalog: a published list of what may be done through the gate, by role. Scopes: every grant is narrow, named, and expires. Receipts: a log entry per action, attributable to a person. Idempotency: a write that arrives twice happens once.

Revocation: access can be withdrawn instantly, and is, on the last day.

Sensitivity labels: the data carries its own classification so the gate can refuse without a meeting.

Return dates: context borrowed from the company for a task has a date on which it is deleted from the person's side.

Do those eight things and the person experiences intelligence while the company experiences governed transactions. Those are the same event described from two sides, and the second description is the one that survives an audit.

The plumbing already exists

Two years ago this would have been a design sketch. It is now plumbing. The major labs converged, with unusual speed, on a shared protocol for connecting an AI to outside systems, with an authorization layer that lets an AI client request access to a company resource on behalf of a named person, and an enterprise extension that lets the company say centrally which connections its people may use and under what conditions. I do not need to name versions; by the time you read this they will have changed. The shape is what matters: a personal client, a company resource, an explicit authorization flow, a bounded transaction, a log. That is the gate, and your IT function can build it from standard parts.

The consumer agents the labs now ship on the person's side have grown the matching features: rules that set what the agent may do on its own and what it must ask about, in at least one case scoped to a single task or time

period, approval before it spends money or sends a message, and a view of what it is doing that the person can inspect. The two halves were built to meet. Your policy is the agreement about where.

What the gate gives you that the mandate never could

A log. Right now the work your best people do with their own AI is invisible to you, not because they are hiding it but because there is no surface for it to appear on. The gate gives it a surface. Every proposal that entered the customer system, every record that was updated, every document that was read, attributed to a person, with a timestamp and a scope. That is more governance than the mandate ever produced, and it comes with better work, because the people producing it are using the instruments they know.

The law in plain words

I am not a lawyer, and this chapter will keep telling you to find one. But a business owner needs the shape of the rules before the conversation with counsel, so that the conversation is short. Here is the shape, as of the autumn of 2026, in four parts.

Trade secrets require reasonable measures

In the United States, federal law protects a trade secret only if its owner has taken reasonable measures to keep it secret. That phrase is the hinge. A company whose confidential pricing can be pasted into any consumer AI by any employee, with no policy, no gate and no log, will struggle to show it took reasonable measures, and may find that what it thought was a trade secret is not one in court. The Bring Your Own AI policy, with its gate, its sensitivity labels and its receipts, is not a concession to employees. It is the reasonable measure. Prohibition without a control is not; it is a document.

Confidentiality is about where facts go, not which instrument touches them

Your confidentiality agreements, your customer contracts and your industry's rules are written in terms of information: what may be disclosed, to whom, under what protection. An AI is a place information can go. The question for each AI is the same question you would ask of any vendor: where does the data live, who can see it, how long is it kept, and is it used to train something that other people will use. The labs answer that question differently for consumer and business accounts, and

the answers change; the policy should require that any AI touching left-column facts be on terms that meet your confidentiality obligations, and your counsel should check the terms once a year.

Recording and consent

Several of the most useful workflows begin with a recorded conversation. The law on recording varies by state and country, and in many places every party must consent. A policy that lets people bring their own AI must say plainly what may be recorded, with whose consent, what must be kept for the company's records, and what may not be captured at all. Private does not mean lawless. The estimator's workflow in chapter two works only where the homeowner has agreed, and the policy must say so.

Literacy and the arriving rules

In the European Union, companies that deploy AI have been under a duty since early 2025 to ensure their staff have a sufficient level of AI literacy, and broader obligations continue to phase in. In the United States, state laws on automated decisions are arriving one legislature at a time and their effective dates keep moving; Colorado, which passed the first broad one, repealed and replaced it this May with a narrower disclosure law that takes effect in 2027, before the original had ever come into force. If your business touches hiring, lending, housing, insurance or health, the rules about using AI in those decisions are stricter and specific. The policy in this book is a floor, not a ceiling: it governs the boundary between a person's AI and your systems. It does not replace the rules that govern what decisions an AI may be part of. Ask counsel which of those apply to you, and read the national framework for managing AI risk if you want a shared vocabulary for the conversation.

The one sentence to carry into the lawyer's office

Here is the sentence. We want to let our people use their own AI for our work through a gate we control, with our facts staying in our systems, every action logged and attributable, and their methods staying theirs; help us write the clauses that make that enforceable here. A good lawyer will have questions. They will be about your industry and your jurisdiction, not about the principle, because the principle is just the reasonable measure, written down.

PART THREE: THE POLICY

7

What the policy must say

The complete policy is in the first appendix. This chapter walks its twelve clauses and says why each one is there, so that when you cut it down for your business you know what you are cutting.

1. Purpose

The policy exists to let people do the company's work with the AI they know best, safely. State that in the first sentence, because the first sentence sets the tone for every reading that follows. A policy that opens with a prohibition is read as a prohibition no matter what it permits later.

2. The instrument is yours

The company does not specify which AI a person uses, does not require them to use a company-issued one, and does not claim ownership of their methods, prompts, templates, or the model their AI holds of them. This is the clause that recruits. It is also the clause that most lawyers will want to soften, and you should hold it, because a softened version reads as the confiscation it was meant to replace.

3. The facts are ours

Company information, defined broadly and with examples, stays in company systems or passes only through the gate. The person's AI may work on company facts but may not become a store of them. This is the clause that protects. It is the reasonable measure, and it is where the sensitivity labels live: public, internal, confidential, restricted, with examples of each, and with the rule that restricted information never leaves the company's systems in any form.

4. The gate

All access by a person's AI to company systems goes through the company's gate, with the person's identity, within a named scope, and with a receipt. The policy does not describe the gate's engineering, which will change. It describes what the gate guarantees, which will not.

5. Approved paths

The company publishes a catalog of what may be done through the gate, by role, and keeps it current. Anything not in the catalog is not permitted until it is added. This is what makes the policy operable: a person can look up whether their AI may update a customer record, and the answer is yes, no, or ask.

6. What is never permitted

A short list. Pasting restricted information into any AI outside the gate. Granting an AI standing access to a company system without scope or expiry. Letting an AI act on a customer, a colleague or a supplier as if it were the person, without the person's review. Recording anyone without the consent the law requires. Using an AI to make a decision about a person that the law reserves for a human. Keep the list short enough to remember and absolute enough to enforce.

7. Review before it leaves

Any work product that goes to a customer, a regulator, a court, or the public is reviewed and signed by a person before it goes. The AI may produce it. A human stands behind it. This is a standard, and it is the most important one in the policy.

8. Accountability does not delegate

The person is responsible for what their AI does through the gate, the way they are responsible for what they do with any instrument. "The AI did it" is not a defense, and the policy says so. This is the clause that makes managers comfortable, and it should.

9. Receipts and inspection

The company keeps a log of every action taken through the gate and may inspect it. The company does not inspect the person's AI, their prompts, or their method, and says so. The first half is governance. The second half is the boundary that makes people willing to be governed.

10. Borrowed context has a return date

When company information is loaded into a person's AI for a task, the policy says how long it may stay and requires its deletion from the person's side after. A thirty-day default with longer periods by approval is reasonable. The point is that the person's AI is a workbench for company facts, not a warehouse.

11. The first day and the last day

On the first day the person declares which AI they bring and connects it through the gate. On the last day the company revokes the gate and the person confirms that borrowed context has been deleted and that nothing in the left column leaves with them. Both are checklists. Both are in the policy so that neither is a negotiation.

12. Literacy and incidents

The company provides enough training for people to use the policy well, and it has a graded, no-blame process for the day a line is crossed. The last clause of a policy is the one people read when something has gone wrong. Make it the clause that tells them what to do, and promises they will not be punished for reporting it.

The first day

The policy becomes real at onboarding or not at all. Here is the first day, as a sequence.

Declare

The new person tells the company which AI they bring. Not to approve it; the instrument is theirs. To know it. The company records which AI, on which account terms, so that the confidentiality question from chapter six has an answer. If the person's AI is on consumer terms that do not meet the company's confidentiality obligations for the left column, the company says so and either pays for the business terms or limits what that AI may reach through the gate. This is a conversation, and it should take ten minutes.

Connect through the gate

The person's AI is connected to the company's systems through the gate, with the person's identity, and with the scopes their role is granted in the catalog. Nothing is connected directly. The person can see what their AI may reach, and the company can see the same list. Legibility in both directions is the whole point.

Learn the labels

The person is shown the sensitivity labels with examples from their own job, and the three or four things that are never permitted. Not a forty-page handbook. A card. The two-column test from chapter four is on the back of

it.

Agree the return date

The default period for borrowed context is explained and the person's AI is set to honor it. Many AIs can now be given a standing instruction about retention; the policy asks the person to give it.

Sign the standards, not the procedures

The person signs a page that lists the standards: what finished means, what reviewed means, what confidential means, who signs before work leaves. The page does not say which AI to use or how to use it, and the person notices that it does not. That is the moment the policy earns its name.

What the company records

Three things, on one page: which AI the person brought and on what terms, which scopes were granted and by whom, and the date the return-date instruction was set. That page is the beginning of the person's receipt trail and the end of the onboarding. It should not take the technology function more than an hour, and after the tenth hire it takes ten minutes.

What the first day feels like from the other side

Compare this to the Monday in the introduction. Instead of signing a page that forbids the thing she will do anyway, she connects the AI she trusts to the systems she needs, can see exactly what it may touch, and is told the company does not want her prompts and will not read them. She starts work at eleven with an assistant that already knows her. The company starts receiving finished work from a person who is not hiding anything, because there is nothing to hide.

The last day

Everything in the policy that protects the company is tested on the last day, and most companies have no last-day process at all beyond collecting the badge.

Revoke

The gate is closed for that person: every scope, every connection, instantly. This is the container wipe of the phone era, translated. If revocation is not instant, the gate was not built properly; fix the gate rather than the departure process.

Reconcile

The company and the person walk the two columns. Left: has every piece of company information loaded into the person's AI for a task been deleted, per the return-date clause? The person confirms it, in writing, and where the AI keeps a record, the record is shown. Right: the person's methods, templates, prompts and their AI's model of them leave with them, and the company confirms it has no claim on them. Both confirmations are on one page and both sign it.

What stays and what goes

The company keeps the receipts: the log of everything the person's AI did through the gate while they were employed. That is the company's record of its own transactions, and it stays. The company keeps the work product

it paid for. The person keeps the way they produced it. If there is a dispute about which column something belongs in, the policy says it is resolved by the test, not by seniority, and names the person who decides.

The clean carry

I have written about the clean carry: leaving a job without losing every reusable method, which only works when personal capability is kept separate from an employer's confidential work. The last-day process is where the clean carry is either honored or breached. A company that honors it gets a reputation among exactly the people it wants to hire. A company that tries, on the last day, to claim the person's method as its own gets a reputation too, and a departing employee with every reason to be careless about the left column.

The departure as a delivery

The best last day I have seen was treated like a delivery. Work finished, files in order, knowledge handed to the next person, gate revoked, columns reconciled, both pages signed, thanks exchanged. It took an hour. The person went on to recommend two people who later joined. That is what the policy buys on the last day: a departure that improves the company's position rather than exposing it.

When a line is crossed

It will happen. Someone will paste a confidential document into an AI outside the gate because it was faster. Someone's AI will update a record it should not have had the scope to touch. Someone will record a call without the consent the law required. The measure of the policy is not whether these happen but what happens next.

The most instructive case

In 2023 a large electronics manufacturer discovered that engineers had pasted proprietary source code into a consumer AI service to get help with it, and responded by restricting the use of such services across the company. The incident is usually told as a story about careless employees. It is better read as a story about an absent gate. The engineers needed help with the code. The company had provided no path for getting it safely. They took the path that existed. The prohibition that followed did what prohibitions do: it made the next instance invisible.

The lesson is not never. The lesson is build the path, then the rule.

A graded response

The policy sets out three grades. A lapse: left-column information reached a person's AI outside the gate, no harm resulted, the person reported it. Response: delete, note, retrain if needed, no penalty. A breach: restricted information left the company's systems, or an AI acted outside scope with effect. Response: contain, assess, notify as the law requires, review the scope that allowed it, and a conversation with the person about what

happened, which may have consequences if the act was knowing. A violation: a person deliberately circumvented the gate or the never-permitted list. Response: the ordinary disciplinary process, because this is ordinary misconduct with a new instrument.

The grades matter because a policy that treats every lapse as a violation gets no reports, and a policy that gets no reports governs nothing.

No-blame reporting

Say it in the policy and mean it: a lapse reported promptly is never penalized. The company learns where the gate is missing a path from the lapses people report, and it learns nothing from the ones they hide. The first month after the policy goes in, expect a cluster of reports. They are not a sign the policy is failing. They are the inventory of everything that was already happening in the dark.

Fix the gate, not the person

After any incident the first question is what path should have existed. If the engineer needed help with the code, the catalog needs a path for code help through the gate. If the estimator needed the proposal drafted, the catalog needs the drafting path. Most incidents are a missing entry in the catalog. Add it, announce it, and the incident rate falls, not because people were punished but because the safe path became the easy path.

PART FOUR: RUNNING IT

11

Manager, not user

The industry calls the person a user. I have argued at length that the word is wrong, because it describes a relationship with a tool, and an AI you delegate to is not a tool. You manage it. The right word for the human is manager. In a business that allows people to bring their own AI, this matters twice: the person is the manager of their AI, and their manager is the manager of a person who manages an AI. Both relationships need to be understood or the policy produces confusion.

What changes for the person's manager

Nothing about outcomes. Everything about method. A manager used to be able to watch the work: the hours, the drafts, the visible effort. Now the work happens inside an instrument the manager cannot and should not see. What the manager can see is what crosses the gate: the finished proposal, the updated record, the delivered file, and the receipt for each. The manager has to learn to manage by outcome, which the best managers always did, and to stop managing by observation, which the rest of them did because they could.

Concretely: scope the outcome in writing before the work starts. Say what finished means. Let the person and their AI get there however they get there. Inspect the result the way a customer would. Hold the person accountable for it, not the AI. That is the posture, and it is identical to the posture the person takes toward their own AI. The whole company becomes a chain of delegation with a human standing behind each link.

Accountability does not delegate

The one thing that must not change: when a piece of work is wrong, the person who delivered it owns it. "My AI did it" is not an explanation the manager accepts, and the policy says so. This is what makes managers willing to allow the instrument. The instrument may be anything; the signature is a person's.

What to measure

Stop counting seats and logins. They measure procurement, not work. Count what crosses the gate: finished work delivered, records updated, time from request to done, errors found in review. The gate's receipts are the measurement system, and they are far better than anything the mandate produced, because they count outcomes and attribute them to people.

The people, not the AI

One rule I give every manager, and it has nothing to do with capability. Never let an AI deal with a person who is worthy of your own attention. The customer with the complaint, the colleague who is struggling, the supplier whose invoice is wrong: they get you. Your AI can prepare you for them. It cannot stand in for you. A company that lets people bring their own AI should also say, in its standards, which relationships must be held by a human, and hold managers to that as firmly as it holds them to the confidentiality clause.

What the IT function becomes

For thirty years the function that managed technology in a company did two things: it issued instruments and it protected the perimeter. The Bring Your Own AI policy ends the first job and transforms the second.

From issuing to gatekeeping

The company no longer issues the AI. It issues the gate. The technology function's product is the system of action from chapter five: identity, the capability catalog, scopes, receipts, revocation, labels, return dates.

Building that is real engineering, mostly from standard parts, and running it is a real operational job. It is also far smaller than the job of procuring, deploying, training on and supporting a company AI that nobody wanted to use.

The catalog as a product

The capability catalog is the most visible artifact the function now produces, and it should be treated as a product with customers. Every entry says what an AI acting for a person in a role may do: read the customer record, update a status, draft an invoice for review, post to the ticketing queue. Every request for a new entry is a feature request. The catalog's growth rate is the honest measure of how much of the company's work is reachable by the people's instruments, and the lapse reports from chapter ten are its backlog.

Systems integration, again

Most of this work is integration: connecting the gate to the systems of record the company already has, with the authorization flow the labs have converged on, and with the scopes and logging the policy requires. It is unglamorous, well-understood work, the kind a competent integrator does in weeks rather than years. A business without the staff to do it can hire the work done. The important thing is to recognize it as integration, not as an AI project. The AI arrived with the people. What the company builds is the door.

What the function stops doing

It stops reading prompts. It stops auditing people's personal AI accounts. It stops arguing about which model is approved. It stops running training sessions on an instrument nobody wanted. It stops counting seats. It spends the time it recovers on the gate, which is the only thing the company owns, and on the catalog, which is the only thing that grows.

The five-person company

Most businesses are not thirty people with a technology function. They are an owner, a few employees, and a laptop in the back office. The policy for them is three paragraphs, and this chapter is that version.

What the owner actually needs

The owner needs three things. The customer list and the books do not walk out the door. Nothing goes to a customer that a person has not read. And the people who work there can use whatever AI makes them good, because the owner cannot afford to make them worse. That is the whole policy, and it can be said in one meeting.

The small-business gate

A five-person company does not build a system of action. It uses the ones that already exist. The bookkeeping system, the scheduling tool, the customer list: each now has a way to connect an AI with a named login, a limited scope and a log, because the labs and the software companies built the plumbing for everyone at once. The owner's gate is the settings page of each system, where each person's AI is connected under that person's name with the minimum it needs. When someone leaves, the owner removes the connection. That is revocation. The log the system keeps is the receipts.

The three-paragraph policy

Paragraph one: use the AI you like; it is yours and so is how you work with it. Paragraph two: the customer list, the books, the pricing and anything a customer told us in confidence stay in our systems; your AI may work on them through the connection we set up for you, but may not keep copies, and you delete anything you borrowed when the job is done. Paragraph three: nothing goes to a customer or the public until a person here has read it and put their name on it, and if something goes wrong, tell me the same day and you will not be in trouble for telling me.

That is enforceable, legible and short enough to remember. It is also, clause for clause, the same policy as the long one; it has simply been written for a company where the owner is the gate.

Where to get help

An owner who wants this set up and does not want to learn the settings pages can have it done in an afternoon by someone who does this for a living. In Charleston that is what my own company's on-site team does for businesses that already have their systems and need the connections, the scopes and the policy put in place correctly. Elsewhere, a local integrator who understands both the AI connections and the business's software will do it. The work is small. The mistake is to think it requires an AI project.

Objections, answered

Every room produces the same seven objections. Here they are, taken seriously, with the answer I give.

“It is a security risk.”

The mandate is the security risk, because it governs nothing. People use their own AI either way; the only question is whether the company can see and bound what that AI touches. A gate with scopes and receipts is more security than any prohibition ever delivered. The honest version of this objection is “we have not built the gate,” and the answer is to build it.

“We are liable for what their AI does.”

You are liable for what your people do, with any instrument, and you always were. The policy makes the person accountable for their AI’s actions through the gate, logs every action, and requires human review before anything leaves. That is a stronger liability position than one in which an unseen AI does unseen work and nobody signs anything.

“It is unfair; not everyone can afford a good AI.”

True, and the policy should answer it directly: the company pays for business-grade terms for anyone who needs them, on an account the person controls. The cost is modest and the alternative, a company-issued AI nobody uses plus a personal one the company cannot see, is more expensive. Equity is a reason to fund the instrument, not to confiscate it.

“Their AI might be training on our data.”

It might, if it is on the wrong terms, which is why the first day includes the account-terms conversation and why the policy requires that any AI touching confidential facts be on terms that exclude training. The labs offer such terms. Check them once a year. This objection is a reason for clause three, not a reason against the policy.

“We already bought an enterprise AI.”

Keep it. Offer it. Some people will prefer it, and it is a fine answer to the equity objection. Do not mandate it. The seats you bought are not the measure of anything; what crosses the gate is. An enterprise AI that people choose and a personal AI that people bring can both pass through the same door.

“What about customer data and our contracts?”

Customer data is left-column, restricted or confidential by label, and the policy says it never leaves your systems in any form except through the gate, in scope, with a receipt. Your customer contracts are satisfied by the same control that satisfies your trade-secret obligations. If a contract forbids any third-party processing, the catalog for that customer’s data simply has no AI entries, and the gate refuses.

“Our people will leave with everything they learned.”

They always did. What they learned is theirs, and it was theirs under the old arrangement too; you just could not see it. What they must not leave with is your facts, and the last-day process in chapter nine is the first time most companies will have actually checked. A company that tries to keep the method keeps neither the method nor the person. A company that keeps the facts and honors the method keeps the facts, and often the person.

PART FIVE: A FUTURE YOU CAN FEEL COMING

15

Six predictions

A policy is a bet about the world it will be enforced in. Here is the world I am betting on. Each prediction is stated so that it can fail; the conditions under which I would admit failure are in the claim ledger.

1. The AI clause joins the device clause.

By 2028 the standard employment agreement will have a clause about the AI a person brings, the way it now has a clause about devices and confidential information. It will say the instrument is the person's, the facts

are the company's, and access runs through a gate. Companies will add it for the same reason they added the device clause: the lawyers will want the reasonable measure in writing and the recruits will ask what the policy is.

2. The mandate loses to the gate.

Surveys of employers today find that most have a formal AI policy and far fewer have any control behind it. Within three years the proportion will invert in a specific way: the share of companies mandating a single issued AI for all work will fall below the share permitting personal AI through a permissioned boundary. The mandate will survive in regulated functions and in companies that have not yet lost anyone to it.

3. The gate becomes a product.

The system of action, the layer where an intent becomes a permitted transaction, will be sold as a category by 2028, the way identity management is sold now. The identity and security vendors will get there first, because it is mostly identity with a catalog attached, and the enterprise software companies will bundle it. A small business will buy it the way it buys a password manager.

4. The two halves meet.

The labs' consumer agents will ship a work mode by 2027 that recognizes an employer's gate, honors its scopes and labels, and keeps the person's own memory and method outside it. The person will switch their AI into work mode the way they switch a phone into a work profile. The protocol for this exists; what is missing is the product surface, and the labs have every incentive to build it, because the employer's gate is what makes their consumer agent permitted at work.

5. Courts will read the gate as the reasonable measure.

Within three years a trade-secret case will turn on whether an employer took reasonable measures to protect information that passed through employees' AI, and a gate with scopes and receipts will be treated as the measure while a bare prohibition will not. After that case, every general counsel will ask for the gate, and the policy in this book will stop being a recommendation and become a floor.

6. "May I bring my own AI?" becomes an interview question.

By 2030 the people a company most wants to hire will ask it in the first interview, the way they now ask about remote work, and the answer will decide offers. Companies that say no will find they are interviewing a different population than the one they wanted. The ones that say yes, with a gate, will have written the policy years before and will not remember it as a decision.

What would make me wrong

If the labs decide the enterprise is the customer and the person is the endpoint, and build the gate on their own side with the company as the account holder, the fourth prediction fails and the model of the person ends up owned by the employer after all. If a few serious incidents make prohibition politically unavoidable, the second slows by years. If courts treat any employee use of AI as a per se failure of reasonable measures, the fifth inverts and the whole argument has to be made again on different ground. I do not expect any of these, but the book is only honest if it says so.

A letter to the owner

I want to tell you why I believe this, in the first person, with only the facts.

I run a small AI services business in Charleston, South Carolina. The front door says, in effect, bring us your AI: people walk in with the AI they already have and we fix it, improve it or move it to another, in person, at a table, with an expert beside them. The people who come through that door appear to need completely different things. One owns a roofing company. One teaches piano. One is managing a household. One has thirty employees. One has none and does not want any. But the work underneath is almost always the same: a direct relationship with a frontier model, and a personal system built on top of it, with their files, their methods, their permissions and their history. Not one of them has ever asked me to help them adopt their employer's AI. Every one of them is building their own.

My company also has an on-site team that goes to medium-sized businesses, the ones with an information officer and a security function, and does systems integration: connecting what they already have, correctly, to what their people now bring. That team is where I learned that the gate is finite work. It is identity, a catalog, scopes and logs, built from standard parts, and it takes weeks. The companies that think it is an AI project are usually the ones still counting seats.

I run my own company on the policy in this book. My AI has the keys to my systems, under exactly this arrangement: I carry the intention, it carries the work, the systems keep the record, and I stand behind the result. When it asks me to choose among options I tell it to decide, because the

bottleneck is the one job a manager must not keep. The book you are reading was produced that way. I am not asking you to do something I have not done.

And I have been on the other side. Long ago I was one of the first two employees of a company that was founded, on paper, by the corporations it served. Our owners were our customers. I learned early what happens when the line between the people you work for and the people you serve is drawn honestly: everyone gets better work, and nobody has to hide anything. That is the feeling the policy in this book is designed to produce inside a company. The person keeps the instrument. The company keeps the ledger. Every transfer between them is visible, limited and attributable. Nobody is annexed, and nothing walks.

So here is what I would say if you were in front of me with the mandate on the table.

Do not sign it. Let them bring their own. Write the twelve clauses, or the three paragraphs if you are five people, and have a lawyer who knows your industry read them. Build the gate from the parts that already exist, or have someone build it for you in an afternoon. Publish the catalog. Label the data. Set the return date. Run the first day and the last day as checklists. Promise that a lapse reported is never punished, and keep the promise. Then stop counting seats and start counting what crosses the gate, and watch what the people you were trying to restrain turn out to be able to do.

Let them bring their own AI. Everything else in this book is a footnote to that.

The backpack

HER FIRST MONDAY, 10:20 A.M., AGAIN

The new company hands her a card. On one side are the labels, with examples from her own job, and the four things that are never permitted. On the other is a two-column test. At 10:40 she connects the AI she has been working with for two years to the company's systems through a gate that shows her exactly what it may touch, and shows the company the same list. Nobody asks for her prompts. The backpack is still under the desk. It is not hidden anymore.

At eleven she starts work with an assistant that already knows her, and the company starts receiving finished things.

APPENDICES

A

The policy

A model Bring Your Own AI policy. Read every clause. Strike what does not apply. Add what your industry requires. Have counsel review the result before adoption. Bracketed items are for you to fill in.

Bring Your Own AI Policy

[Company name]. Effective [date]. Owner: [role].

1. Purpose. This policy exists so that the people of [Company] can do the Company's work with the AI they know best, safely. It sets the boundary between a person's own AI and the Company's information

and systems. It is written to be read in ten minutes and kept.

2. Your instrument is yours. You may use the AI of your choice for Company work. The Company does not require you to use an AI it issues, does not specify which AI you use, and does not claim ownership of your prompts, templates, methods, or the model your AI holds of how you work. Your methods leave with you when you leave.

3. The Company's information is the Company's. Company information includes customer and supplier data, financial records, pricing, contracts, plans, source code, personnel information, work product the Company paid for, and anything received in confidence. It is labeled Public, Internal, Confidential or Restricted. [Examples for each label, drawn from your business.] Company information stays in Company systems or passes only through the Gate described in clause 4. Your AI may work on Company information for a task but may not become a store of it. Restricted information never leaves Company systems in any form.

4. The Gate. All access by your AI to Company systems runs through the Company's gate, under your identity, within a named scope, with a logged receipt for every action. No AI is connected directly to a Company system, given a shared credential, or granted standing access without scope and expiry.

5. Approved paths. The Company publishes a catalog of what an AI acting for a person in each role may do through the Gate, and keeps it current at [location]. An action not in the catalog is not permitted until it is added. Requests to add a path go to [role] and are answered within [n] business days.

6. Never permitted. (a) Entering Confidential or Restricted information into any AI outside the Gate. (b) Granting an AI standing access to a Company system without scope and expiry, or sharing

your credentials with it for that purpose. (c) Allowing an AI to act toward a customer, colleague, supplier or the public as if it were you, without your review of what it sends or does. (d) Recording any person without the consent required by law and this policy. (e) Using an AI to make a decision about a person that law or Company policy reserves to a human.

7. Review before it leaves. Any work product sent to a customer, a regulator, a court, or the public is reviewed and approved by a named person before it is sent, regardless of how it was produced. That person's name is on it.

8. Accountability. You are responsible for what your AI does through the Gate, as you are responsible for what you do with any instrument. The involvement of an AI does not reduce that responsibility.

9. Receipts and inspection. The Company keeps the log of actions taken through the Gate and may inspect it for security, compliance and operational purposes. The Company does not inspect your AI, your prompts, your method or your personal accounts, and will not ask you to produce them.

10. Borrowed context. Company information loaded into your AI for a task may remain there for [30] days unless a longer period is approved by [role], after which you delete it. Where your AI supports a retention instruction, set it to this period.

11. First day and last day. On joining, you declare which AI you bring and on what account terms, connect it through the Gate, and receive the labels and this policy. If your AI's account terms do not meet the Company's confidentiality obligations for the information your role touches, the Company will fund suitable terms on an account you control or limit the scopes available to that AI. On

leaving, the Company revokes the Gate for you, you confirm in writing that borrowed context has been deleted, and the Company confirms in writing that it claims nothing in clause 2.

12. Literacy and incidents. The Company provides training sufficient to use this policy well. If a line in this policy is crossed, report it to [role] the same day. A lapse reported promptly, where no harm has resulted, is never penalized. Breaches are contained, assessed, and notified as the law requires, and the Gate is reviewed for the path that was missing. Deliberate circumvention of the Gate or of clause 6 is handled under the Company's ordinary disciplinary process.

Standards, not procedures. This policy sets standards: what is confidential, what is reviewed, who is accountable. It does not set procedures. How you work with your AI is yours.

Acknowledged by: [name], on [date].

The claim ledger

A prediction without a failure condition is a mood. Here is each claim with what is already true, what has to happen, and where I am probably wrong.

The AI clause joins the device clause

ALREADY TRUE

Most large employers now have a formal AI policy, and device and confidentiality clauses are universal in employment agreements.

WHAT HAS TO HAPPEN

Employment lawyers must settle on language that separates the instrument from the information, and recruits must start asking for it.

WHERE I AM PROBABLY WRONG

Many of the clauses that get written will be prohibitions dressed as policies. The clause may arrive by 2028 and say the wrong thing.

The mandate loses to the gate

ALREADY TRUE

Policies outnumber controls; most employers have a document and far fewer have an approval process or a restriction on what may be entered.

WHAT HAS TO HAPPEN

The gate has to become easy to buy and install, so that permitting is cheaper than prohibiting.

WHERE I AM PROBABLY WRONG

Regulated industries may standardize on the issued AI for liability reasons, and if they are a large enough share, the inversion happens only outside them.

The gate becomes a product

ALREADY TRUE

The connection and authorization protocols exist and are shared across the major labs; identity vendors already sell most of the parts.

WHAT HAS TO HAPPEN

Someone has to package identity, catalog, scopes, receipts and revocation as one product with a price a small business can pay.

WHERE I AM PROBABLY WRONG

The enterprise software companies may fold the gate into their own suites, so that it never becomes a category, just a feature of the systems of record.

The two halves meet

ALREADY TRUE

The consumer agents have permission layers, approvals and activity records; the enterprise side has managed authorization.

WHAT HAS TO HAPPEN

The labs have to ship a work mode that honors an employer's gate while keeping the person's memory and method outside it.

WHERE I AM PROBABLY WRONG

The labs may decide the enterprise is the customer and build the gate on the company's side of the account, which would put the model of the person back in the employer's hands.

Courts read the gate as the reasonable measure

ALREADY TRUE

Trade-secret protection already turns on reasonable measures, and courts already weigh access controls and logs.

WHAT HAS TO HAPPEN

A case has to be litigated on these facts and decided on this ground.

WHERE I AM PROBABLY WRONG

The first case may go the other way, with a court holding that any employee use of personal AI shows a failure of reasonable measures. If so, the argument has to be won on appeal or in the next case.

"May I bring my own AI?" becomes an interview question

ALREADY TRUE

Most AI users already bring their own tools to work, and the share is highest among the youngest workers.

WHAT HAS TO HAPPEN

Enough companies have to say yes that saying no becomes a visible disadvantage.

WHERE I AM PROBABLY WRONG

In a weak hiring market candidates ask fewer questions, and the pressure may come later and from a smaller group than I expect.

The working cards

Six short exercises for the owner or the manager. Do each one with your own AI. Each produces a document you keep.

Card 1: The two columns

Draw two columns. Left: what the company owns (facts, records, customer data, paid-for work product, trade secrets). Right: what the person owns (method, templates, prompts, their AI's model of them). Take the ten pieces of information that pass through your people's AI most often and put each in a column. Disputes go on a third list for counsel.

Card 2: The labels

Define Public, Internal, Confidential and Restricted with three examples each from your business. Decide which labels may pass through the gate at all. Put the result on one card.

Card 3: The catalog

List everything a person in each role does inside your systems in a week. For each, decide: may their AI do it through the gate (yes), never (no), or with review (ask). The yes list is your first catalog.

Card 4: The gate inventory

For each system of record, write down how an AI connects to it today: named login or shared credential, scoped or full access, logged or not, revocable in a minute or not. Every “shared, full, unlogged” entry is a line in your plan.

Card 5: The first day and the last day

Write both checklists from chapters eight and nine for your company, on one page each. Assign the person who runs them. Run the last-day list on the next departure and note what you could not confirm.

Card 6: The incident drill

Pick the most likely lapse in your business. Write what the person should do the same day, what you do the next day, and which catalog entry would have prevented it. Add the entry.

A small glossary

Bring Your Own AI

A policy that lets people do the company's work with their own AI through a permissioned boundary, keeping the company's facts in the company's systems and the person's method with the person.

Gate

The company's system of action: the surface where an AI acting for a person asks to read or change something in a company system and receives a scoped, logged answer. The only part of the arrangement the company owns.

System of action

The layer between a person's intelligence and the systems of record, where intent becomes a permitted transaction. Identity, catalog, scopes, receipts, idempotency, revocation.

Systems of record

The ledger, the customer database, the HR system, the document store. The facts. Already built; changed by this policy only in who may touch them and how the touch is logged.

Capability catalog

The published list of what an AI acting for a person in a role may do through the gate. Anything not listed is not permitted until added.

Scope

A narrow, named, expiring grant of access. The unit in which the gate permits anything.

Receipt

The log entry for one action through the gate, attributed to a person, with a timestamp and scope.

Left column, right column

The two kinds of knowledge. Left: the company's facts. Right: the person's method and their AI's model of them.

Borrowed context

Company information loaded into a person's AI for a task, with a return date after which it is deleted.

Lapse, breach, violation

The three grades of incident. A reported lapse is never penalized; a breach is contained and the gate reviewed; a violation is ordinary misconduct.

Manager

The right word for the human in a relationship with an AI. Not user. The one who carries the intention and stands behind the outcome.

Sources and development

The argument is mine, and parts of it were first made in the posts listed below. The facts were checked on October 30, 2026. Where a figure appears in the text, this is where it came from.

Friedrich A. Hayek, "The Use of Knowledge in Society," *American Economic Review*, vol. 35, no. 4, September 1945. The knowledge of the particular circumstances of time and place.

Microsoft and LinkedIn, 2024 Work Trend Index, "AI at work is here. Now comes the hard part," May 8, 2024. 78 percent of AI users bring their own AI tools to work; 31,000 knowledge workers in 31 markets. A 2024 figure, not since updated by the same survey. <https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part>

Gartner, press release, May 13, 2026. 88 percent of employees with enterprise AI access also use personal AI tools for business tasks; 12,004 employees and managers in 40 countries. <https://www.gartner.com/en/newsroom/press-releases/2026-05-13-gartner-predicts-by-2027-50-percent-of-enterprises-without-a-people-centric-ai-strategy-will-lose-their-top-ai-talent>

PagerDuty, shadow AI workplace survey, June 11, 2026. 66 percent of 1,250 office professionals used AI tools they believed policy did not allow. <https://pagerduty.com/newsroom/shadow-ai-workplace-survey-2026>

GovInfoSecurity, interview with Intel's chief information security officer, January 11, 2012. Intel's bring-your-own-device program: pilots in 2009, company-wide in January 2010, under a formal policy. <https://www.govinfosecurity.com/byod-get-ahead-risk-a-4394>

Bloomberg, "Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak," May 2, 2023. <https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak>

18 U.S.C. 1839(3), definition of a trade secret: the owner must have taken reasonable measures to keep the information secret. The federal civil claim was created by the Defend Trade Secrets Act of 2016. <https://www.law.cornell.edu/uscode/text/18/1839>

Covington, "European Commission Provides Guidance on AI Literacy Requirement under the EU AI Act," March 6, 2025. Article 4 applies from February 2, 2025. <https://www.insidi>

deprivacy.com/artificial-intelligence/european-commission-provides-guidance-on-ai-literacy-requirement-under-the-eu-ai-act/

Blank Rome, "Colorado Replaces AI Act with Narrower New AI Law," May 2026. SB 26-189 repealed and replaced SB 24-205; effective January 1, 2027. <https://www.blankrome.com/news-and-events/colorado-replaces-ai-act-with-narrower-new-ai-law/>

National Institute of Standards and Technology, AI Risk Management Framework 1.0 (NIST AI 100-1), January 2023, and the Generative AI Profile (NIST AI 600-1), July 2024. <https://www.nist.gov/itl/ai-risk-management-framework>

Anthropic, "Introducing the Model Context Protocol," November 25, 2024. <https://www.anthropic.com/news/model-context-protocol>

TechCrunch, "OpenAI, Anthropic, and Block join new Linux Foundation effort to standardize the AI agent era," December 9, 2025. The protocol moved to a foundation co-founded by the major labs. <https://techcrunch.com/2025/12/09/openai-anthropic-and-block-join-new-linux-foundation-effort-to-standardize-the-ai-agent-era/>

OpenAI, "How your data is used to improve model performance." Consumer content may train models by default with an opt-out; business offerings are excluded. <https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance>

Anthropic, "Updates to Consumer Terms and Privacy Policy," August 28, 2025. Consumer users choose whether chats train the model; business, enterprise and API use is excluded. <https://www.anthropic.com/news/updates-to-our-consumer-terms>

Microsoft, "Data, privacy, and security for Microsoft 365 Copilot." Enterprise prompts, responses and accessed data are not used to train foundation models. <https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy>

Axios, "Meta debuts Muse personal AI agent," September 8, 2026. A consumer agent whose permissions can be limited to a task, service, transaction or time period. <https://axios.com/2026/09/08/meta-debuts-muse-personal-ai-agent>

Anthropic, "Get started with Claude Duet," October 2026. A consumer agent that asks before each purchase and sends email only with approval. <https://support.claude.com/en/articles/17631495-get-started-with-claude-duet>

Forrester, "Bring-Your-Own-AI Hits the Enterprise," September 21, 2023. An early call for a formal BYOAI management strategy. <https://www.forrester.com/press-newsroom/forrester-byoai-management-policy>

Related writing on johnrector.me

Bring Your Own AI (September 16, 2026): <https://johnrector.me/2026/09/16/bring-your-own-ai/>

Do Not Make Them Use Your AI (September 12, 2026): <https://johnrector.me/2026/09/12/do-not-make-them-use-your-ai/>

The Charge Is Yours (October 23, 2026): <https://johnrector.me/2026/10/23/the-charge-is-yours/>

You Are Not the User (October 30, 2026): <https://johnrector.me/2026/10/30/not-the-user/>

My AI Delegate (October 30, 2026): <https://johnrector.me/2026/10/30/ai-delegate/>

The Clean Carry | App to Stack (October 28, 2026): <https://johnrector.me/2026/10/28/the-clean-carry-app-to-stack/>

The Middle Cannot Finish (October 27, 2026): <https://johnrector.me/2026/10/27/the-middle-cannot-finish/>

Worthy of Their Attention (October 4, 2026): <https://johnrector.me/2026/10/04/worthy-of-their-attention/>

Super Admin: The Advanced Course in Personal AI (October 27, 2026): <https://johnrector.me/2026/10/27/super-admin/>