A FREE UNCOM MEDIA RESOURCE

UNCOM
MEDIA INC.

AI Implementation Guide

For Organizations Adopting AI Without Losing Control

CLARITY • CONSISTENCY • TRUST

UNCOM MEDIA INC. | WWW.UNCOM.MEDIA

BEFORE YOU BEGIN

A Note Before You Start

Your employees are already using AI. Recent surveys put the number using AI tools their employer never approved somewhere around three out of four, often to draft emails, summarize documents, or write code, frequently without a second thought about what data they just pasted into a chat window.

That gap, between what leadership assumes is happening and what is actually happening, is where most AI risk lives right now. Not in some dramatic, headline-ready failure. In an employee pasting a client contract into a free tool for a quick summary. In a marketing team publishing AI-written copy that quietly drifts off brand. In nobody being quite sure who approved the AI tool that now touches customer data.

AI adoption is not optional anymore, and treating it like a passing trend is its own kind of risk. The organizations getting real value from AI right now are rarely the ones with the most tools. They are the ones with the clearest rules for how those tools get used, by whom, on what, and with what oversight.

> **WHY THIS MATTERS**
>
> Recent industry research found that roughly two out of three organizations use generative AI regularly, while only about one in three say they have policies and controls mature enough to keep pace. This guide exists to help close that gap before it closes on you.

This guide is intentionally general. It is built to apply whether you run a five-person startup, a regional healthcare system, a manufacturing company, a law firm, or a national nonprofit. Adapt it to your structure, your industry, and your risk tolerance. Use what fits, and set aside what doesn't.

We built this at UNCOM Media because AI adoption is, at its core, a communications and trust problem as much as a technology one. Read through it, adapt it to your organization, and put it to work. And if you would like help building the complete version of this, tailored to your team and your risk profile, we would love to talk.

With clarity,
The UNCOM Media Team

WHAT'S INSIDE

Table of Contents

SECTION 01

01 Why You Need an AI Implementation Plan

AI tools are free, instant, and require no IT ticket to start using. That is exactly what makes them valuable, and exactly what makes them risky without a plan. Unlike most technology rollouts, AI adoption inside most organizations did not start with a decision. It started with individual employees quietly finding tools that made their work easier.

That bottom-up adoption is not a problem by itself. The problem is when it happens with no visibility, no shared standards, and no plan for the day an AI tool produces something wrong, biased, or exposed data it should never have touched.

What changes once AI is part of daily work

Once AI touches customer data, published content, hiring decisions, or financial analysis, informal use stops being efficient and starts being a liability. A tool that felt like a personal productivity trick becomes part of how your organization actually operates, whether leadership signed off on that or not.

> **WHY THIS MATTERS**
>
> An implementation plan gives your team a shared, tested framework for everyday AI use and the rare high-stakes moment, so nobody is improvising data handling, disclosure, or damage control in real time.

What a plan actually does for you

- **It protects your data.** By making clear what can and cannot go into an AI tool, and which tools have actually been vetted.
- **It protects your brand and reputation.** By keeping AI-assisted content accurate, on voice, and reviewed before it reaches a customer.
- **It protects you legally.** By addressing bias, disclosure, and intellectual property before a regulator or a customer raises it first.
- **It gives you a real plan for hard days.** Including the ones where an AI tool gets something seriously wrong in public.

This guide walks through all of it, built to scale up or down depending on the size and shape of your organization.

SECTION 02

02 Roles & Responsibilities

AI governance should sit with named owners, not float as everyone's part-time responsibility. At a small organization, one person may fill several of these roles. What matters is that each function has a name attached.

Recommended structure

Role	Who it usually is	What they do
AI Governance Lead	Senior staff member, often in IT, operations, or communications	Owns the AI use policy, approves new tools, coordinates training and reviews
Department Champions	A staff member on each team who uses AI regularly	Surfaces real use cases, flags risks early, trains peers informally
IT / Security Lead	IT or security staff	Vets tools for data handling, access control, and integration risk
Legal / Compliance Contact	In-house or outside counsel	Reviews disclosure obligations, intellectual property questions, and vendor contracts
Executive Sponsor	CEO, COO, or equivalent	Final sign-off on high-risk use cases, budget, and public-facing AI decisions

> **RIGHT-SIZED ADVICE**
> Informal AI adoption is a bigger liability than in most other areas, because generative AI tools require no procurement process to start using. Every role above should exist even at a five-person company, even if one person fills three of them.

Setting expectations up front

- Formalize every role in writing, and revisit it at least annually as tools and risks evolve
- Give every team the same governed standards for tool approval and data handling
- Hold a regular check-in, at least monthly, between the governance lead, department champions, and leadership

SECTION 03

03 Finding the Right Use Cases

Not every task belongs in an AI tool, and not every AI use case needs the same level of oversight. Sort potential use cases by risk and value before you roll anything out broadly.

Category	Examples	Oversight Needed
Good starting points	Drafting internal documents, meeting summaries, brainstorming, first drafts of content, internal research	Light human review
Use with oversight	Customer-facing content, code before it reaches production, data analysis feeding real decisions	Mandatory human review before use
Avoid or tightly restrict	Final hiring or termination decisions, medical, legal, or financial advice given to customers, anything involving sensitive personal data without real safeguards	Executive and legal sign-off, or avoid entirely

A WORD OF CAUTION

If an AI mistake in a given use case could end up in a headline, a lawsuit, or a termination hearing, it belongs in the top tier of oversight, not the bottom. When in doubt, treat the use case as higher risk than it feels.

Start small, on purpose

Pick one or two low-risk, high-value use cases to pilot before rolling AI out broadly across the organization. A successful, well-governed pilot builds the trust and the playbook you need before tackling anything higher stakes.

Revisit this list regularly

What counts as low risk today may not stay that way as a tool's capabilities, your data exposure, or the regulatory landscape changes. Review your use case list at the same cadence you review the rest of this plan.

SECTION 04

04 Choosing & Vetting AI Tools

Nearly every organization already has employees using AI tools that were never formally approved. Instead of banning tools outright, which research shows employees will often ignore anyway, give people a fast, low-friction way to request a new tool and get a real answer.

Before approving any AI tool

- Does the vendor clearly explain how your data is used, stored, and whether it trains future models on your inputs?
- Is there an enterprise or business tier with a contractual guarantee against training on your data?
- Does it support single sign-on and role-based access control?
- Has your IT or security lead reviewed it before it rolls out broadly?
- Is there a documented process to revoke access the moment someone leaves the organization?

> **THE SHADOW AI PROBLEM**
>
> Recent surveys have found that close to half of employees say they would keep using an unauthorized AI tool even after their company explicitly banned it. A workable, fast approval process beats a strict policy nobody actually follows. Consider a no-fault reporting channel so employees can surface the tools they are already using without fear of punishment.

Keep an approved tools list

Maintain one current, visible list of approved AI tools by use case, owned by your AI governance lead. Review it on the same schedule as your account and access reviews, and remove tools that go unused or fail a security review.

SECTION 05

05 Data Privacy & Security Basics

This is the section most likely to prevent a genuinely bad day. Data pasted into the wrong AI tool does not stay private just because you meant it to.

The core rule

Never enter anything into an unvetted or public AI tool that you would not be comfortable seeing published. That includes customer data, employee records, financial details, unreleased plans, credentials, health information, and anything involving minors.

Practical safeguards

- Use enterprise or business-tier tools with a written data protection agreement wherever real work data is involved
- Turn off model training on your inputs wherever the tool allows it
- Treat AI chat logs like email: retained, potentially discoverable, and subject to the same records policies
- Require multi-factor authentication and single sign-on on every approved AI tool
- Review vendor security certifications, such as SOC 2, before broad rollout

NEVER PASTE THIS INTO AN UNVETTED TOOL

Passwords or API keys, health records, another company's confidential information, anything under a signed NDA, or personal data belonging to minors. If you would hesitate to email it to a stranger, do not paste it into an AI chat window.

Build on your existing security foundation

AI data governance is not a separate system. It should plug directly into the access reviews, offboarding workflow, and password management you already use for every other tool in your organization.

SECTION 06

06 Using AI in Your Voice

AI can produce a fast first draft. It cannot know your brand voice, your customers, or the details only your team knows to be true. Treat every AI draft as a draft, never a finished product.

Content quality standards

- A human always edits AI-generated content for accuracy and voice before it goes out under your name
- Fact-check every claim, statistic, quote, and citation an AI tool produces. AI tools can state false information with complete confidence
- Measure every AI draft against your documented brand voice guide, not just against whether it sounds fluent
- Never let AI publish anything under a named person's byline without that person reviewing it first

A HELPFUL RULE

If you would not let a brand-new, uncredentialed intern publish something without a review, do not let AI do it either. The tool is a capable assistant, not an accountable one.

Protecting a consistent voice at scale

If your organization has a documented brand voice guide, share it directly with your team as a reference when editing AI output. Consistency in tone matters more as AI makes it easier to produce a much larger volume of content, much faster than before.

07

SECTION 07

Disclosure & Transparency

The rules around when you must disclose AI use are changing quickly and unevenly. Regulation now reaches businesses through multiple channels at once: international law, state law, and existing consumer protection enforcement.

What the landscape looks like right now

- International transparency rules increasingly require disclosure when a person is interacting with an AI system, and require AI-generated images, audio, and video to be identifiable as such
- A growing number of U.S. states have their own AI transparency and disclosure laws, with more taking effect on a rolling basis
- There is no single federal AI disclosure law in the United States yet, but consumer protection regulators have been active in enforcing against deceptive AI-related claims under their existing authority

Practical guidance in the meantime

- Disclose clearly when a customer is talking to a chatbot rather than a person
- Label AI-generated or AI-manipulated images, audio, and video, especially in advertising
- Be transparent internally whenever AI meaningfully informed a decision affecting an employee or a customer
- Never claim content is entirely human-written if a customer or regulator asks directly and it isn't

NOTE

This section covers general best practice, not legal advice. AI disclosure law is a genuinely fast-moving area, with new state and international rules taking effect on a rolling basis over the next several years. Loop in counsel before finalizing your disclosure language.

SECTION 08

08 Approval & Review Workflow

A clearly tiered, documented approval process keeps everyday AI use moving quickly while giving higher-risk use cases a fast, well-understood path to real oversight.

Use directly, with light review

- Internal drafts, meeting notes, and brainstorming
- Research and summarization for internal use
- Personal productivity tasks that never touch customer or sensitive data

Get manager or department champion sign-off

- Any customer-facing content before it publishes
- Code generated by AI before it merges into production
- External communications, including social posts and email campaigns

Get executive and legal sign-off

- Anything informing a hiring, promotion, discipline, or termination decision
- Anything in a regulated area, such as health, finance, or legal advice
- Any new AI tool that will touch customer or financial data before broad rollout

KEEP THE PATH FAST

Even with a formal tiered process, higher-risk use cases should never wait on more than a small, defined group of decision-makers. Document who those people are and their backup contacts.

SECTION 09

09 Employee Training & Acceptable Use

A policy nobody understands is not a policy. Training is what turns a written document into something your team actually follows.

- **Give every employee baseline AI literacy training** before any organization-wide rollout, covering what AI tools can and cannot be trusted to do
- **Provide role-specific training** for teams using AI heavily, such as marketing, customer service, or engineering
- **Put your acceptable use policy in writing** and have every employee with AI access acknowledge it, using the sample in Section 13
- **Refresh training regularly** as tools, risks, and rules change, not just once at onboarding
- **Create a no-fault reporting channel** so employees can disclose AI tools they are already using without fear of punishment, so you can vet and either approve or replace them

> **RIGHT-SIZED ADVICE**
>
> You cannot train your way around a policy that is harder to follow than the shadow alternative. If your approved workflow is slower or more restrictive than free public tools with no real reason, expect people to route around it.

Make training stick

Use real examples from your own organization's actual use cases rather than generic hypotheticals. Training that feels abstract gets ignored the first time a real deadline hits.

SECTION 10

10 Risk Areas: Bias, Hallucination & IP

Three risks show up in nearly every AI use case, regardless of industry. Understanding them is the difference between catching a problem before it publishes and explaining it after.

Hallucination

AI tools can state false information with complete confidence, including fabricated statistics, quotes, case citations, and sources that do not exist. Verify every factual claim before it reaches a customer, a court, or the public.

Bias

AI models can reflect and amplify biases present in their training data. Use extra caution with AI in hiring, lending, pricing, or any decision that affects real people, and periodically test outputs for disparate impact across groups.

Intellectual property

Ownership of AI-generated content remains legally unsettled in many jurisdictions. Do not assume AI output is automatically yours to use commercially without review, and do not feed copyrighted material into a tool without the rights to do so.

> **A SIMPLE STANDARD**
>
> Treat every AI output as a claim made by someone you have never met and cannot fully vouch for, until a human on your team has actually checked it.

SECTION 11

11 Measuring Impact

Adoption is not the same thing as success. A tool everyone uses but that quietly erodes quality or trust is not a win, no matter how the usage numbers look.

What to actually track

- Time saved on specific, well-defined tasks, not vague productivity impressions
- Error or correction rate on AI-assisted work compared to the same work done without it
- Approved tool adoption versus ongoing shadow AI usage, to see whether your process is actually being followed
- Customer satisfaction and complaint trends after AI-assisted content or support rolls out
- Total cost of tools against measurable, attributable output

> **A HELPFUL HABIT**
>
> Review these measures on the same cadence as your other operational metrics, not as a one-time pilot report. AI tools, and the risks around them, change fast enough that a snapshot from six months ago may already be out of date.

Ask your team directly

Numbers alone will not tell you whether your team trusts the tools they have or is quietly working around them. A short, regular check-in with department champions surfaces problems dashboards miss.

SECTION 12

12 When AI Goes Wrong: A Basic Incident Protocol

An AI incident can move from an internal mistake to a public story faster than almost any other kind of error, because the mistake is often already published, sent, or acted on before anyone reviews it.

Your basic first steps

1. **Pause the specific workflow or tool immediately.** Stop the bleeding before you diagnose the cause.
2. **Notify your AI governance lead and legal.** They should know within minutes, not at the next scheduled meeting.
3. **Assess what data or content was affected, and who saw it.** This shapes everything that follows.
4. **Correct or retract any public-facing content immediately.** Do not wait for a perfect statement to stop something inaccurate from spreading further.
5. **Notify affected customers or employees if required.** Coordinate the message with legal and communications before it goes out.
6. **Document what happened and update your policy.** An incident that repeats because nothing changed is a second, avoidable failure.

> **THIS IS A STARTING POINT, NOT A FULL PLAN**
>
> A true AI incident response plan includes pre-approved statement templates, a documented notification chain, and a tested communications protocol for the day something goes wrong in public. UNCOM Media specializes in building that complete plan alongside your leadership team, so an AI mistake never becomes a crisis you are managing for the first time in real time.

SECTION 13

13 Sample AI Use Policy & Staff Agreement

Below is a short, adaptable statement your organization can copy, adjust to fit your context, and have every employee with AI access sign.

[Company Name] AI Use Policy & Agreement

_____ agrees to use AI tools on behalf of [Company Name] in line with this policy, and in doing so agrees to:

- Use only AI tools that have been reviewed and approved through the process outlined in Section 04
- Never enter customer data, employee data, financial details, credentials, or other sensitive information into an unapproved or unvetted AI tool
- Review all AI-generated output for accuracy, bias, and voice before publishing, sending, or acting on it
- Disclose AI use to customers or the public wherever required by company guidelines or applicable law
- Report any AI tool currently in use that is not on the approved list, through the no-fault reporting channel, without fear of punishment
- Complete required AI training and any scheduled refreshers
- Escalate anything uncertain to a manager, department champion, or the AI governance lead before proceeding
- Follow the organization's AI incident protocol and pause use immediately if instructed by leadership

Signature _____ Date _____

SECTION 14

14 Quick-Start Checklist

Use this checklist to put the basics of this guide into practice this quarter.

- [ ] Name an AI governance lead, department champions, an IT/security lead, and a legal contact in writing
- [ ] Run a no-fault survey to find out what AI tools employees are already using, approved or not
- [ ] Sort likely use cases into good starting points, use with oversight, and avoid or restrict
- [ ] Build and publish an approved AI tools list, reviewed on a set schedule
- [ ] Document what data can never go into an unvetted AI tool, and train every employee on it
- [ ] Require single sign-on and multi-factor authentication on every approved AI tool
- [ ] Define your tiered approval process, including legal and executive escalation for higher-risk use cases
- [ ] Confirm your AI disclosure language with legal counsel given the fast-changing regulatory landscape
- [ ] Roll out baseline AI training to every employee, with role-specific training for heavy-use teams
- [ ] Review the basic incident protocol in Section 12 with leadership and legal counsel
- [ ] Have every employee with AI access sign the policy agreement in Section 13
- [ ] Schedule a quarterly review of tools, use cases, and measured impact

UNCOM
MEDIA INC.

You've Got the Basics. Let's Build the Rest.

This guide covers the fundamentals every organization needs to adopt AI without losing control of its data, its voice, or its reputation. But AI adoption without a real plan is a reputational risk waiting to happen, and every organization eventually faces the moment it did not fully plan for.

UNCOM Media helps organizations of every size and industry build AI use policies, training, and communication plans that let you move fast without losing what makes you trustworthy. If you would like help turning this guide into a complete, board-ready plan built specifically for your team, we would love to talk.

WWW.UNCOM.MEDIA

rich@uncom.media

(469) 513-1040

CLARITY • CONSISTENCY • TRUST