



SAMPLE

CONFIDENTIAL

AI Compliance Register

Every third-party AI service seen on the network, what each one does with company data, and the control applied. For auditors, insurers and internal review.

PREPARED FOR
Example Industries Inc.

37

AI VENDORS

9

BLOCKED

28

CONTROLLED

3

AUDITS ON RECORD

Period covered
26 Jul 2026 to 26 Sep 2026

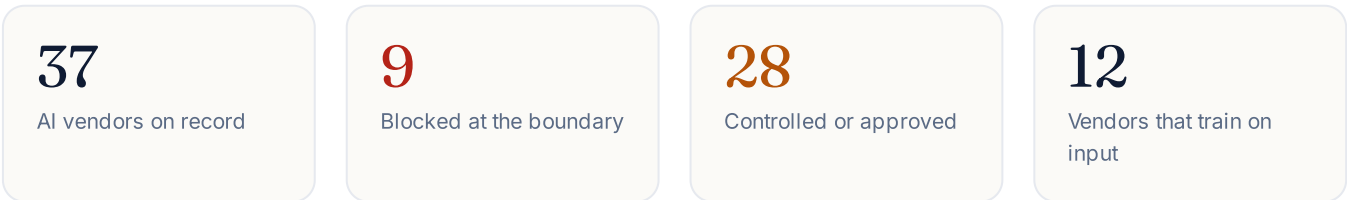
Prepared by
Your Company Ltd
security@yourcompany.example

Policy
General business
Issued 26 Sep 2026

STATEMENT OF CONTROL

How Example Industries Inc. controls third-party AI

Example Industries Inc.'s network traffic is reviewed for AI services at every audit. Each service found is recorded with its data terms and risk, and handled under the General business policy: blocked at the network boundary, allowed only with business terms, or approved by the client.



Control applied to each vendor



Highest-risk vendors on record

01	DeepSeek deepseek.com High risk rating · Data may be stored outside your region	Blocked
02	Kimi kimi.com High risk rating · Data may be stored outside your region	Blocked
03	Manus manus.im High risk rating · Data may be stored outside your region	Blocked
04	SeaArt seaart.ai High risk rating · Data may be stored outside your region	Blocked
05	Kling AI klingai.com High risk rating · Data may be stored outside your region	Blocked

Contents

1. AI vendor register	each vendor, data terms, risk, control, first and last seen
2. Change log	3 audits, what was added and removed
3. Framework cross-reference	CMMC / NIST 800-171, HIPAA, NIST AI RMF, insurance
4. Method and sign-off	how the evidence was produced

SECTION 1

AI vendor register

Sorted by control, then by use. The full register is also available as CSV.

AI VENDOR	DATA TERMS	RISK	CONTROL APPLIED	SEEN
DeepSeek deepseek.com Models & Infrastructure	Trains unless the user opts out Business no-training plan: no tier Checked 2026-09-26	High Data location risk: high	Blocked Firewall / DNS feed, updated daily	26 Sep 2026 26 Sep 2026 In use
Suno AI suno.com Audio, Voice & Music	Trains on user data Business no-training plan: unstated Checked 2026-09-26	Medium Data location risk: low	Blocked Firewall / DNS feed, updated daily	26 Sep 2026 26 Sep 2026 In use
Napkin napkin.ai Productivity & Collab	Trains unless the user opts out Business no-training plan: no Checked 2026-09-26	Medium Data location risk: low	Blocked Firewall / DNS feed, updated daily	26 Sep 2026 26 Sep 2026 In use
Kimi kimi.com Text & Language	Trains unless the user opts out Business no-training plan: yes Checked 2026-09-26	High Data location risk: high	Blocked Firewall / DNS feed, updated daily	26 Sep 2026 26 Sep 2026 In use
Manus manus.im Agents & Automation	Does not train on user data Business no-training plan: yes Checked 2026-09-26	High Data location risk: high	Blocked Firewall / DNS feed, updated daily	26 Sep 2026 26 Sep 2026 In use
Character.AI character.ai Lifestyle & Entertainment	Trains on user data Business no-training plan: no tier Checked 2026-09-26	Medium Data location risk: low	Blocked Firewall / DNS feed, updated daily	26 Jul 2026 26 Sep 2026 In use
SeaArt seaart.ai Image & Visual	Not stated by the vendor Business no-training plan: unstated Checked 2026-09-26	High Data location risk: high	Blocked Firewall / DNS feed, updated daily	26 Aug 2026 26 Sep 2026 In use
Kling AI klingai.com Video	Trains unless the user opts out Business no-training plan: unstated Checked 2026-09-26	High Data location risk: high	Blocked Firewall / DNS feed, updated daily	26 Aug 2026 26 Sep 2026 In use
DeepSwap deepswap.ai Image & Visual	Does not train on user data Business no-training plan: unstated Checked 2026-09-26	High Data location risk: high	Blocked Firewall / DNS feed, updated daily	26 Sep 2026 26 Sep 2026 In use
DeepL deepl.com Text & Language	Trains on user data Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Perplexity AI perplexity.ai Search, Knowledge & Docs	Trains unless the user opts out Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Remove.bg remove.bg Image & Visual	Trains on user data Business no-training plan: unstated Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use

AI VENDOR	DATA TERMS	RISK	CONTROL APPLIED	SEEN
v0 by Vercel v0.dev Code & Development	Trains unless the user opts out Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Gamma gamma.app Productivity & Collab	Trains unless the user opts out Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Sep 2026 26 Sep 2026 In use
Devin Desktop (formerly Windsurf) windsurf.com Code & Development	Trains on user data Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Writesonic writesonic.com Marketing, Sales & SEO	Does not train on user data Business no-training plan: yes Checked 2026-09-26	Low Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Gemini Notebook (formerly NotebookLM) notebooklm.google Search, Knowledge & Docs	Does not train on user data Business no-training plan: yes Checked 2026-09-26	Low Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Otter.ai otter.ai Productivity & Collab	Trains on user data Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Hugging Face huggingface.co Models & Infrastructure	Does not train on user data Business no-training plan: unstated Checked 2026-09-26	Low Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
QuillBot quillbot.com Text & Language	Trains unless the user opts out Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Midjourney midjourney.com Image & Visual	Trains on user data Business no-training plan: no tier Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
HeyGen heygen.com Video	Trains unless the user opts out Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Aug 2026 26 Sep 2026 In use
Runwayml (runwayml.com) runwayml.com Video	Trains on user data Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Aug 2026 26 Sep 2026 In use
Grok grok.com Text & Language	Trains unless the user opts out Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Mistral mistral.ai Models & Infrastructure	Trains unless the user opts out Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use

AI VENDOR	DATA TERMS	RISK	CONTROL APPLIED	SEEN
You.com you.com Search, Knowledge & Docs	Does not train on user data Business no-training plan: yes Checked 2026-09-26	Low Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Poe poe.com Text & Language	Does not train on user data Business no-training plan: no tier Checked 2026-09-26	Low Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Jasper jasper.ai Text & Language	Trains on user data Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Replit replit.com Code & Development	Trains on user data Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Julius julius.ai Data, Analytics & Research	Does not train on user data Business no-training plan: yes Checked 2026-09-26	Low Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Ideogram ideogram.ai Image & Visual	Trains on user data Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Leonardo AI leonardo.ai Image & Visual	Trains on user data Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Allowed with controls Business plan with no-training terms only	26 Jul 2026 26 Sep 2026 In use
Claude claude.ai Text & Language	Trains unless the user opts out Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Sanctioned Approved by the client, on its allowlist	26 Jul 2026 26 Sep 2026 In use
Grammarly grammarly.com Text & Language	Trains unless the user opts out Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Sanctioned Approved by the client, on its allowlist	26 Jul 2026 26 Sep 2026 In use
ChatGPT chatgpt.com Text & Language	Trains unless the user opts out Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Sanctioned Approved by the client, on its allowlist	26 Jul 2026 26 Sep 2026 In use
Cursor cursor.com Code & Development	Trains unless the user opts out Business no-training plan: yes Checked 2026-09-26	Medium Data location risk: low	Sanctioned Approved by the client, on its allowlist	26 Jul 2026 26 Sep 2026 In use
Fireflies.ai fireflies.ai Productivity & Collab	Does not train on user data Business no-training plan: yes Checked 2026-09-26	Low Data location risk: low	Sanctioned Approved by the client, on its allowlist	26 Jul 2026 26 Sep 2026 In use

SECTION 2

Change log

One entry per audit. It shows the control is reviewed over time, not once.

AUDIT DATE	AI VENDORS	ADDED	REMOVED
26 Sep 2026	37	Gamma, DeepSeek, Suno AI, Napkin, Kimi, Manus, DeepSwap	—
26 Aug 2026	30	HeyGen, Runwayml (runwayml.com), SeaArt, Kling AI	—
26 Jul 2026	26	Baseline: 26 vendors recorded	—

Method

Each audit analyses the client's DNS, proxy or firewall log against a register of AI-tool domains that is updated daily. Each vendor's data-training and data-location terms are checked by hand; the date is shown in the register.

Verdicts follow the General business policy. Tools the client approved are recorded as sanctioned and excluded from blocking. Blocked tools are enforced on the client's firewall or DNS filter by a feed refreshed daily.

AI services reached outside the logged network, such as on personal devices at home, are not visible to this method.

This pack is supporting evidence for the control of third-party AI services. It does not by itself demonstrate compliance with any framework and is not legal advice.

Sign-off

Reviewed by (IT provider)

Accepted by (client)

Date

SECTION 3

Framework cross-reference

Which requirement each part of this pack supports. Supporting evidence only.

CMMC Level 2 / NIST SP 800-171 Rev. 2

REFERENCE	REQUIREMENT	EVIDENCE IN THIS PACK
3.1.20	Verify and control/limit connections to and use of external systems	The register lists every external AI service in use and the control applied to each.
3.13.1	Monitor, control and protect communications at external boundaries	Disallowed AI services are blocked at the firewall / DNS boundary by the daily feed.
3.13.6	Deny network communications by default and allow by exception	Block-by-policy plus a per-client allowlist of sanctioned tools; exceptions are recorded in the register.
3.11.1	Periodically assess risk to operations, assets and individuals	Each audit rates every AI tool for risk, data sovereignty and data-training terms.
3.3.1	Create and retain system audit logs	Audits are produced from the client's DNS / firewall logs; the change log keeps the history.

HIPAA Security Rule (45 CFR 164)

REFERENCE	REQUIREMENT	EVIDENCE IN THIS PACK
164.308(a)(1)(ii)(A)	Risk analysis	Inventory of AI services that could receive ePHI, with each vendor's data-use terms.
164.308(a)(1)(ii)(B)	Risk management	The control applied to each AI service (blocked, allowed with controls, sanctioned).
164.308(a)(1)(ii)(D)	Information system activity review	Monthly review of AI traffic: new, removed and high-risk tools.
164.308(b)(1)	Business associate contracts	Flags AI vendors used without enterprise or no-training terms, where a BAA is required before any ePHI is shared.

NIST AI Risk Management Framework 1.0

REFERENCE	REQUIREMENT	EVIDENCE IN THIS PACK
GOVERN 1.6	Mechanisms are in place to inventory AI systems	The register is the inventory of third-party AI tools in use.
GOVERN 6.1	Policies address AI risks from third-party entities	A written sector policy gives a verdict and reason for every AI tool.
MAP 4.1	Legal and technology risks of third-party components are mapped	Data-training terms, data sovereignty and risk flags per vendor.
MANAGE 3.1	Third-party AI risks are monitored	Monthly audits and the change log show new and removed AI vendors.

Cyber-insurance questionnaires

REFERENCE	REQUIREMENT	EVIDENCE IN THIS PACK
AI use policy	Do you have an acceptable-use policy for AI tools?	The applied sector policy with a verdict for every tool.
Generative AI controls	Do you restrict employee use of generative AI with company data?	Blocked and allowed-with-controls tools, with the enforcement point.
Shadow IT monitoring	Do you monitor use of unsanctioned cloud and AI services?	Monthly audit results and the change log.

FOR IT COMPANIES AND MSPS

What you pay, and what your clients get

In plain words: you are an IT company that looks after other businesses. For \$249 a month you add up to **25 of those businesses** to your account. On top of that you get **10 AI audit reports a month** with your logo, which you run for whichever clients you choose. The add-ons give every client a report every month.

PACKAGE 1

Assess

\$249/month

The MSP plan

What you get for each client

- ✓ 10 white-label AI audit reports a month, with your logo ([sample](#))
- ✓ A ready AI policy for each client (15 sector templates)
- ✓ An upload link with your logo, so clients send their own log file

PACKAGE 2 · RECOMMENDED

+ Monthly reports

\$398/month

MSP plan \$249 + Monthly AI Report \$149

Everything in package 1, plus

- ✓ A 10-page AI report for every client, every month ([sample](#))
- ✓ 25 audits a month instead of 10, so all 25 clients are checked every month

PACKAGE 3

+ Compliance evidence

\$548/month

MSP plan \$249 + both add-ons \$299

Everything in package 2, plus

- ✓ An AI compliance evidence pack for every client ([sample](#))
- ✓ Vendor register, change log and CMMC, HIPAA, NIST AI RMF and insurance mapping

In practice, with 25 clients

	PACKAGE 1	PACKAGE 2	PACKAGE 3
Client companies you can add	25	25	25
Audit reports per month (you choose which clients)	10	25	25
How often each client is audited	about every 3 months	every month	every month
Clients that get a monthly AI report	—	all 25, every month	all 25, every month
Clients that get a compliance evidence pack	—	—	all 25
Total per month	\$249	\$398	\$548

Example with package 1: audit 10 clients in January, 10 others in February, the last 5 in March. Evidence packs without monthly reports: \$448/month. More than 25 clients: +\$99/month for every 25 more.

Pay with PayPal or credit / debit card. One monthly bill. How it works: shadowaitools.com/msp-ai-governance-service.php