Demo Corporation: AI trust summary

Published 10 Nov 2026, version 3. Facts as of 10 Nov 2026. Live page: https://ghostaudit.ai/trust/demo-corporation

AI policy	Approved AI tools	Customer data used to train AI	AI usage monitoring
In place	**7**	**No**	**Metadata only**
Approved 7 Oct 2026	Listed by name below	Confirmed 3 Oct 2026	No prompts or content

Demo Corporation uses AI tools to write, summarise, code and answer customer questions faster. We know customers want to understand what that means for their data, so this page states it plainly. Our people may use only the AI tools listed here, each under a business agreement. We monitor which AI tools are used on company devices, never what is typed into them. The facts below are read from our governance records each time this page is published. Demo Corporation is a fictional company. This page is an example of a GhostAudit AI trust center.

How we govern AI

- AI acceptable use policy in place, approved 7 Oct 2026. Reviewed once a year; next review due 10 Nov 2027.
- Accountable for AI governance: Head of IT and Security.
- An inventory of AI systems is maintained, with an owner and a risk level for each.

Approved AI tools

Adobe Firefly (Adobe), ChatGPT (OpenAI), Claude (Anthropic), GitHub Copilot (GitHub (Microsoft)), Grammarly (Grammarly), Jasper (Jasper AI), Microsoft Copilot (Microsoft). Tools that have not been approved are not permitted for company work.

Customer data and AI

Is customer data entered into AI tools?	**Only into the approved AI tools named below, for defined business purposes. Support and success teams may use customer account context to draft replies. Bulk exports of customer data are not permitted in any AI tool.**	Confirmed by owner 3 Oct 2026
Which AI tools may process customer data?	**Only these approved tools: ChatGPT, Claude, Microsoft Copilot.**	Confirmed by owner 3 Oct 2026
Under what contractual terms?	**Business or enterprise agreements that include a data processing agreement.**	Confirmed by owner 3 Oct 2026
Is customer data used to train AI models?	**No. Our agreements with these vendors exclude training on our data. This is also switched off in each workspace's admin settings.**	Confirmed by owner 3 Oct 2026
Is AI output reviewed by a person before it reaches customers?	**Yes. A person reviews AI output before it is used in anything sent to a customer.**	Confirmed by owner 3 Oct 2026

Monitoring and controls

- Use of AI tools on company devices and browsers is monitored.
- Monitoring records metadata only: which tool, when and for how long. Prompts, page content, keystrokes and screenshots are never collected.
- A tool policy defines which AI tools are approved, under review or prohibited.
- Employees are warned before they use an AI tool that has not been approved.
- Prohibited AI tools are blocked on managed devices.
- On-device checks warn before sensitive data is submitted to an AI tool. The check runs on the device; the content never leaves it.
- Usage records are removed after 1 year.
- A process is in place to record, contain and review AI incidents and near misses.

Employee training and policy acknowledgement

- Employees are asked to read and acknowledge the AI acceptable use policy.

Frameworks and assessments

Self-assessed against: EU AI Act (last assessed 31 Oct 2026); ISO/IEC 42001 (last assessed 21 Oct 2026); NIST AI Risk Management Framework (last assessed 11 Oct 2026); SOC 2 (AI-relevant criteria) (last assessed 11 Sep 2026). Self-assessments are not certifications.

Documents available on request

On request through the trust center: AI acceptable use policy.

Contact

Questions about how we use AI, or a security questionnaire to complete? Write to our security team. security@democorp.example