

Security, Privacy & Who's Responsible for What

Audience: IT Admin, Everyone • Last verified October 21, 2026

IT Admin (security and IT teams) • Everyone (Sections 6–9)

CONTENTS

- | | |
|--|---|
| 1. Who's responsible for what | 7. Risks from documents you give agents |
| 2. How data flows | 8. Review agent output before relying on it |
| 3. Choose a plan that fits your security needs | 9. Protecting Pentaria Materials |
| 4. Recommended Claude security settings | 10. The version-check link |
| 5. Control which agents run in your organization | 11. Reporting a security concern |
| 6. What information to give agents | 12. References |

Pentaria agents run inside an AI system your organization already licenses and controls. That keeps the security picture simple: your data stays within your AI platform, and Pentaria never receives it. This guide explains who is responsible for what, how data flows, which settings to use, and how to use Pentaria agents safely.

1. Who's responsible for what

IT Admin

AREA	YOUR AI PROVIDER (E.G. ANTHROPIC)	PENTARIA	YOUR ORGANIZATION
Hosting, models, uptime and platform security	●		
How the AI platform stores, retains and uses your data	●		Chooses the plan and settings
Agent methods, instructions and release quality		●	
Release notes and notice of new releases		●	
The Pentaria portal and the account data it holds		●	
Installing, updating and removing agents		Provides releases	●

AREA	YOUR AI PROVIDER (E.G. ANTHROPIC)	PENTARIA	YOUR ORGANIZATION
Who can use your AI system and which agents they get			●
Pentaria portal seats (adding and removing users)			●
What information users put into the AI system			●
Reviewing agent output before relying on it			●
Approving and governing official deliverables		Provides guidance	●
Protecting Pentaria Materials from disclosure			●

Your use of your AI platform, and any data you submit to it, is governed by your agreement with that provider, not by Pentaria. (MSA §5.1–5.2; ToS §4.2–4.3, §10)

2. How data flows

IT Admin

DATA	WHERE IT GOES	DOES PENTARIA RECEIVE IT?
Your prompts, uploaded files, conversations and agent outputs	Your AI platform only, under your agreement with that provider	No. Pentaria agents send nothing to Pentaria.
Web research run by Pentaria agents	Searches run through your AI platform's web search feature	No
Pentaria portal account data (name, business email, job title, company)	The Pentaria portal	Yes, to provide your account and licenses
Portal usage (pages visited, downloads, sign-ins, IP address, browser)	The Pentaria portal	Yes, as described in the Pentaria Privacy Policy
Version checks (date and time, agent version, IP address, portal user)	The Pentaria portal, when someone clicks the version link	Yes. The link carries no content from your AI system.

Pentaria does not receive, access or log anything you do inside your AI platform, and therefore never uses it to train or improve its products. (MSA §5.2–5.3; ToS §4.3–4.4; Privacy Policy §1.2, §1.4)

Pentaria's Data Processing Addendum covers the personal data Pentaria processes for your account, such as portal users' names and emails. It doesn't cover data inside your AI platform, because Pentaria never has access to it. (MSA §15; ToS §6.4)

3. Choose a plan that fits your security needs

IT Admin

The plan your organization uses determines which data terms apply. Guide 1, Section 2 covers plans in full.

	CLAUDE FREE, PRO, MAX	CLAUDE TEAM, ENTERPRISE
Terms	Anthropic Consumer Terms	Anthropic Commercial Terms
Model training on your conversations	Each user chooses in their privacy settings	Not used for training by default
Retention	30 days if the user doesn't allow training; 5 years if they do	Per your commercial agreement; Enterprise offers custom retention
Central control	None; each user manages their own settings	Your organization controls settings centrally

Recommendation: use Team or Enterprise for any work involving non-public company information. On individual plans, each user must choose whether their conversations can be used for training, and organization-wide controls aren't available.

4. Recommended Claude security settings

IT Admin

SETTING	PLAN	WHERE	RECOMMENDATION
Single sign-on (SSO)	Team, Enterprise	See Anthropic's documentation	Turn on, so access follows your identity provider and leavers lose access automatically.
SCIM provisioning	Enterprise	See Anthropic's documentation	Turn on, so users and groups sync from your identity provider. Groups are also how you restrict which agents people get.
Audit logs	Enterprise	See Anthropic's documentation	Use them for security review and compliance.
Custom data retention	Enterprise	See Anthropic's documentation	Set retention to match your data policies.
Skills and plugins scanning	Team, Enterprise	Organization settings → Plugins & skills → Policy	Turn on. Claude scans skills and plugins and shows the result in your inventory.
Publishing	Team, Enterprise	Organization settings → Plugins & skills → Policy	Set to Requires review, so nothing users build reaches the whole organization without approval. (Team plans default to Open.)
User-created skills	Team, Enterprise	Organization settings → Plugins & skills → Policy	Decide deliberately. On lets teams build their own tools; off gives the tightest control (Guide 1, Section 2.3).

SETTING	PLAN	WHERE	RECOMMENDATION
Skill sharing	Team, Enterprise	Organization settings → Plugins & skills → Policy	On if you share restricted agents with named people (Guide 3, Section 3.2); otherwise your choice.
Connectors	Team, Enterprise	Organization settings → Connectors	Allow only the connectors your organization has approved. Pentaria agents don't currently use connectors.
Claude in Chrome (browser extension)	All	Your browser-extension policy	Optional. Only the Market and Product Definition agent's URL route uses it, to read a public product page.

5. Control which agents run in your organization

IT Admin

- **Download Pentaria agents only from the Pentaria portal** (agentexplorer.pentaria.com). Don't install agent files received by email, chat or from colleagues, and don't upload ZIP files that have been unzipped or repackaged.
- **Install centrally where you can.** Agents an admin installs appear in one inventory with version history and rollback (Guide 3). Personal copies are harder to track and keep current.
- **Deploy company-wide only what everyone should have**, and give restricted agents to the people who need them (Guide 3, Section 3).
- **Limit the Pentaria Knowledge Builder** to Content Owners and their named delegates (Guide 4, Section 3.1).
- **Keep Pentaria agents in approved AI systems.** Users must not load Pentaria agents into personal AI accounts or AI systems your organization hasn't authorized. (*MSA §4.1; ToS §8.1; AUA §2.1–2.2*)
- **Review the inventory regularly.** In **Organization settings → Plugins & skills → Inventory**, check for duplicate or member-added copies of Pentaria agents, and use the **Users (30d)** column to see what's in use.
- **Keep agents current.** New releases include fixes. Watch for Pentaria's release emails and the release notes at pentaria.com/releasesnotes (Guide 3, Section 4.1).
- **Protect portal accounts.** Each user keeps their own portal login and doesn't share it. Remove leavers promptly (Guide 3, Section 7.2). (*MSA §4.2(f); ToS §3.3, §7(f); AUA §2.7*)

6. What information to give agents

Everyone

Pentaria agents are built for company work and often need non-public information, such as product plans, win/loss data and interview transcripts. Your AI platform processes that information under your organization's agreement with the provider. Always follow your organization's AI usage policy.

GENERALLY APPROPRIATE (ON A TEAM OR ENTERPRISE PLAN)	USE WITH CARE	AVOID UNLESS YOUR POLICY EXPLICITLY ALLOWS IT
Product and market information, public competitor information, your approved deliverables, internal strategy documents your role allows you to see	Win/loss data and interview transcripts: these often contain names and contact details of real people. Remove personal details you don't need. Customer data: use only what the task requires. Restricted documents (roadmaps, pricing): share only with agents and bundles limited to authorized people (Guide 4, Section 4.1).	Regulated data (health, payment card, government ID numbers), credentials and passwords, information you aren't authorized to share with your AI platform

Research agents search the web. Several agents run web searches through your AI platform, based on what you've provided. If your product or plans are confidential, keep that in mind when deciding what to give an agent that does deep research.

7. Risks from documents you give agents

Everyone

Pentaria agents read the files you upload and the web pages they research. A document can contain hidden or misleading text designed to redirect an AI, sometimes called **prompt injection**. To reduce the risk:

- **Use files from trusted sources.** Be cautious with documents from outside your organization, such as files sent by vendors or downloaded from unfamiliar sites.
- **Use your official deliverables.** Feed agents your approved deliverables from Pentaria Knowledge or your system of record, not copies from email or old chats (Guide 4).
- **Watch for unexpected behavior.** If an agent suddenly ignores its normal steps, asks for information unrelated to the task, or produces content that doesn't fit the request, stop and start a new conversation. Report it to your IT Admin.
- **Keep connectors to what's approved.** The fewer systems an AI can reach, the less a misleading document can do (Section 4).

8. Review agent output before relying on it

Everyone

Pentaria agents label their evidence (for example, marking content as cited, inferred or self-reported), but AI output can still be incomplete or wrong. Your organization is responsible for reviewing and validating any output before relying on it, and a deliverable becomes official only when its Content Owner approves it (Guide 5). (*MSA §5.4; ToS §10; AUA §8*)

9. Protecting Pentaria Materials

Everyone

Agent instructions are confidential. Pentaria agents' instructions, prompts and methods are Pentaria's Confidential Information, even though your organization has downloaded the files. That applies however the instructions are viewed: by opening the agent's files, or by asking an agent to display, restate or summarize its instructions. Content produced that way is not an Output. It remains Pentaria's Materials, and:

- **it must stay inside your organization.** Don't paste it into public forums, personal accounts or AI systems your organization hasn't approved;
- **anything built from it is a Modified Material.** You're permitted to adapt Pentaria Materials for internal use, but a tool that copies or adapts them belongs to Pentaria, isn't supported or updated, and must be deleted if your subscription ends (Guide 7); and
- **it must be deleted if your subscription ends.**

Everything else your agents produce for you, such as ICPs, Market and Product Definitions and battle cards, is your Output and isn't subject to these restrictions.

(MSA §4.2(a)–(c), §8.1, §9.4, §9.6; ToS §7(a)–(c), §8.4, §8.6, §9; AUA §2.2–2.4, §4)

10. The version-check link

Everyone

Each agent's introduction includes a link to the Pentaria portal that checks whether the agent is current. You must be signed in to the portal to use it. When you click it, the portal records the date and time, the agent version, your IP address and your portal user account. The link sends no content from your AI system. Pentaria uses this information to deliver updates and improve its library, as described in the Pentaria Privacy Policy.

Corporate link-scanning tools may open links automatically to check them; this doesn't send any of your content to Pentaria.

11. Reporting a security concern

Everyone

SITUATION	WHAT TO DO
You think a Pentaria agent is behaving unsafely or has been tampered with	Stop using it, tell your IT Admin, and email support@pentaria.com . Your IT Admin can withdraw it immediately by setting it to Not available (Guide 3, Section 6).
Pentaria Materials may have been shared outside your organization	Tell your IT Admin and email support@pentaria.com .
A portal account may be compromised	Your administrator should remove or reset the user in the User administration panel of the Pentaria portal, then promptly email support@pentaria.com . (ToS §3.3)
A security issue with your AI platform itself	Follow your AI provider's reporting process.

12. References

- Pentaria Privacy Policy: pentaria.com/privacy
- Your agreement with Pentaria: Master Services Agreement or Terms of Service, and the Authorized User Agreement
- Claude: [Manage plugins for your organization](#)
- [Claude plans and pricing](#)
- Anthropic: [Updates to Consumer Terms](#)