

# Questions for IT or your admin

Organisation version. Send it in week 1; ask for written answers by week 4. Where an answer is “we don't know”, the pilot stays at levels 1 and 2 until it is known.

## 01 WHO OWNS AGENTS

- Who may create an agent, a scheduled task or a task started by an event, and who approves a new one?  
\_\_\_\_\_
- Who is the named owner of each agent, and who takes over when that person leaves?  
\_\_\_\_\_
- Where is the list of every agent and scheduled task running for us today?  
\_\_\_\_\_

## 03 WHICH CONNECTORS ARE ALLOWED, AND WHETHER THEY WRITE

- Which apps may our AI tools connect to, for whom, and on which plans?  
\_\_\_\_\_
- For each connection: may it only read, or also write, send or delete?  
\_\_\_\_\_
- Who approves a new connection, and can “ask first” be set as an approval in the tool?  
\_\_\_\_\_

## 05 DATA LOCATION AND RETENTION

- Where is our data processed and stored when staff use these tools, including files opened from a laptop?  
\_\_\_\_\_
- How long are chats, files, task results and logs kept, and can we set that?  
\_\_\_\_\_
- On our plans, is our data used to train the vendor's models, and where is that written?  
\_\_\_\_\_
- When a connection is removed, what happens to what the tool already took from it?  
\_\_\_\_\_

## 02 AGENT IDENTITIES AND THE AUDIT TRAIL

- Does each agent act under the account of the person who set it up, or under an identity of its own?  
\_\_\_\_\_
- Where is the record of what each agent read, sent and changed, and who reads it?  
\_\_\_\_\_
- How long is that record kept, and can it be changed after the fact?  
\_\_\_\_\_

## 04 THE PLATFORM AND ITS MEMORY DEFAULTS

- Which of Claude, ChatGPT and Gemini do we license, on which plans, and for whom?  
\_\_\_\_\_
- Is memory on or off by default for our accounts, and can staff change it?  
\_\_\_\_\_
- Can a person see and clear what their assistant remembers, and can we clear it for them?  
\_\_\_\_\_

## 06 HOW TO PULL THE PLUG

- How do we stop one agent now, and how do we stop all of them at once?  
\_\_\_\_\_
- Who can do it outside office hours, and how long does it take?  
\_\_\_\_\_
- Can we cut every connection to one app in one step?  
\_\_\_\_\_
- When did we last try it?  
\_\_\_\_\_

Microsoft's 2026 Work Trend Index tells IT leaders to treat agents “as managed entities with identities, permissions, policy enforcement, and lifecycle management”. Microsoft, 5 May 2026

As of Oct 2026, on Claude Team and Enterprise an owner adds connectors first; on a Google work account the admin decides which apps are allowed. Anthropic says custom connectors “aren't verified”. Anthropic and Google help pages, read 16 Oct 2026

The UK's National Cyber Security Centre: “you should always be able to ‘pull the plug’ and halt autonomous AI agent activity immediately.” UK NCSC, 20 Aug 2026

Each tool's own settings and their defaults, as of Oct 2026, are in The Agent Playbook's dated insert. These products change monthly. Check the settings in your own tool. Neosaipien is not affiliated with Anthropic, OpenAI or Google.