AI RULES FOR YOUR BUSINESS

FIELD CHECKLIST

THE AGENT LEASH CARD

REGULATED 150 15 1

Before anyone connects an AI agent

The newest AI agents keep working after the laptop closes, and they ask to connect to email, calendars, and files. Six questions before anyone says yes. If an answer comes back blank, so does the yes.

1 Whose account is it on: the company's or yours?

A personal plan means settings the company can't see and a history it can't open. Chapter 7 of the book has the difference.

2 What will it connect to?

Email, calendar, texts, files, accounts. Every connection is a key. Name each one before it's handed over.

3 What can it do without asking?

Send, book, order, pay, call, change a record. "It asks first" is a setting, not a promise. Read the setting.

4 Who can change that setting?

The company, or the person who set it up? If it's not the company, the leash isn't yours.

5 Does it carry a card, and with what limit?

An agent that can spend gets its own card with a hard cap, never the company card. Size the limit to what a bad week should be allowed to cost.

6 Where's the off switch, and what does it remember after you pull it?

Flip it once before you need it, and write the date. Disconnecting stops the reading. It doesn't erase what was already read.

A PERSON SAYS YES BEFORE ANY AGENT:

- ☐ sends anything outside the company,
- ☐ spends or refunds money,
- ☐ promises a time or a price,
- ☐ touches a safety question, or
- ☐ does anything that can't be undone.

The line for your one page: No AI tool gets connected to company email, calendar, texts, files, or accounts unless _____ says yes first.

Make connections wait for a yes

For whoever runs the office email. Both steps checked November 2026. Menus move, so check the vendor's own page if one has.

Google Workspace. Out of the box, users can connect any third-party app. To change it: Admin console, then Security, then Access and data control, then API controls. Block unconfigured third-party apps, and turn on "Allow users to request access to unconfigured third-party apps" so requests land in Apps pending review, which is your desk. Changes can take up to 24 hours.

Microsoft 365. Microsoft's managed default, rolled out since 2025, makes users ask an admin before an outside app can read mail, calendars, or files. If someone at your company ever changed the setting, it may still let them through. Check it: Microsoft Entra admin center, then Entra ID, then Enterprise apps, then Consent and permissions, then User consent settings. Pick the Microsoft-managed or verified-publisher option, and turn on the admin consent workflow so requests come to you. New in November 2026: under Entra ID, then Users, then User settings, set "Users can create agent blueprints" to No unless you want employees building their own agents.

The ten-minute quarterly check. Open the connected-apps list. For each app, name the job it does and the person who uses it. Remove anything nobody can name a job for. Look for the maker's app (Claude, ChatGPT, Grok), not the agent's name. Blocking it blocks that maker's app for everyone. Write the date on this card.

The day somebody leaves. Open the connected-apps list and remove every app and agent tied to their company email or accounts. Shutting off their seat doesn't do this for you. It's a row on T-8's back for a reason.

The agents in the news, early November 2026. This table ages fast. The current version lives at sykesystem.com.

AGENT	MAKER	SOLD ON	ASKS BEFORE ACTING?
Claude Duet	Anthropic	Paid personal plans (US preview); not Team or Enterprise	Designed to ask before it sends, pays, signs, or deletes
dots	OpenAI	ChatGPT Pro; Business Premium seats; Enterprise, on from Nov 18 unless an admin opts out	User picks one of four rules, including act without asking
Grok Bot	xAI	SuperGrok and Cursor plans; on Cursor Teams it's on by default with no off switch	Allow once, always allow, or deny; the vendor recommends ask-first for sending, buying, and deleting. Can place phone calls (from Nov 4)
Muse	Meta	Free app with paid tiers; a small-business version; no team admin console found	Asks before sensitive actions; "Always allow" skips future asks for that connector. Phone-call beta to US businesses (since September)