

Some staff were in Copilot. Others had signed up for Claude on their own, some with personal emails. **Nobody could say who had access or where the work lived.**

The Challenge

This Midwest missions organization, which also runs a higher-education arm, came to AI piecemeal. Individual accounts can't be tied to single sign-on, so there was no central control over access or where the organization's work was stored.

The timing was hard. The organization was in the middle of major change, including staff turnover, and the senior vice president driving the AI work had little bandwidth to spare.

In IBM's 2025 research, only **37%** of breached organizations had policies to manage AI or detect shadow AI.¹

The Solution

MSI recommended one Claude Team organization the institution owns, with single sign-on through its Microsoft tenant. When leadership asked for the case, MSI gave a straight answer instead of a pitch: the real gains next to the real costs.

MSI wrote a plain-language migration guide with two paths (work-email signups keep their chats, projects, and files; everyone else exports first), fact-checked against Anthropic's current documentation.

On September 30, MSI delivered an onsite Claude 101 workshop with the organization's own policy built in. The policy revision adds risk tiers and explicit exclusions for SSNs, biometric data, payment cards, and dates of birth.

Engagement Snapshot

CLIENT	Midwest Missions Organization
INDUSTRY	Faith-Based Nonprofit
RELATIONSHIP	Monthly AI Strategy Program
DELIVERED IN	June to October 2026

By the Numbers

37% of breached organizations had policies in place to manage AI or detect shadow AI.¹

1 AI platform the organization owns, replacing a mix of Copilot and personal accounts.

The Results

The organization now runs one AI platform it owns, and staff who signed up with a work email kept their history and projects through the move. Training and the policy revision are moving in parallel.

"Mixed tools and personal accounts are where most organizations start. MSI gets them onto one platform they control, with training and a policy that match how people work."

¹ IBM, Cost of a Data Breach Report 2025, research conducted by Ponemon Institute; IBM press release, July 30, 2025.