

Welcome!

AI in Action:

Practical Secure Chat Workflows
for Business Leaders

Real Workflows. Real Use Cases. Real Business Results.



Agenda and Presenters

01

Introduction to Secure AI
Liam Holmes, CEO & Founder



02

Operations Use Cases
Eric Hammond, Data Center Tech Manager



03

Marketing Use Cases
Gina Kopf, Marketing Manager



Introduction to Secure AI

We have ONE goal today...

Show you how real companies are using AI to get meaningful work done—productively and safely.

Lliam Holmes, CEO & Founder



Why is this topic so important?

Business leaders are asking...

- Where do we start?
- How do we use AI without exposing sensitive data?
- How do we know what employees are putting into AI?
- How do we govern, audit, and control its use?





AI Is Already Being Used in Your Business

You may not have approved it.
You may not have a policy for it.

The reality is:

- Employees are experimenting with public AI tools
- AI is embedded in applications your teams already use
- Vendors are enabling AI faster than policies can keep up
- Sensitive data may be entering AI systems without oversight
- Shadow AI is now a governance and security issue

BOTTOM LINE: The question is no longer whether AI is being used—it is whether it is being used safely and under your control.

Why Business Leaders Feel Stuck

Most organizations know they need AI.
They just don't know how to adopt it responsibly.





Many AI Projects Fail

Organizations are investing heavily in AI, yet many struggle to produce measurable business value.

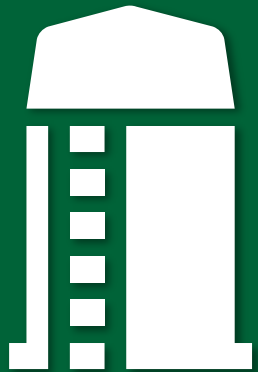
Common reasons:

- Poor data quality
- Disconnected systems
- Limited business context
- Lack of governance
- No clear business objective

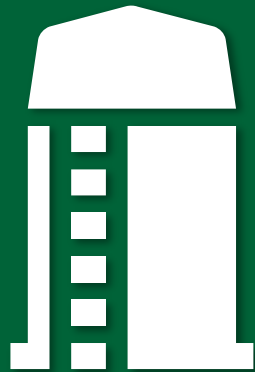
The problem is rarely the AI. It is disconnected data and unclear objectives.

WATCH OUT FOR THE DATA SILO TRAP

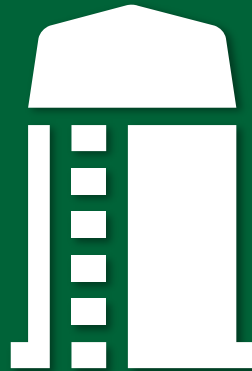
AI has limited value when it is locked inside one system and cannot see across your organization.



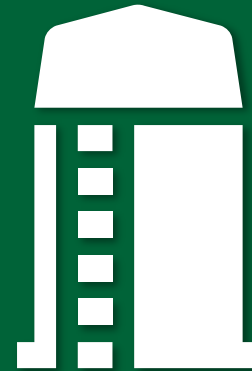
CRM



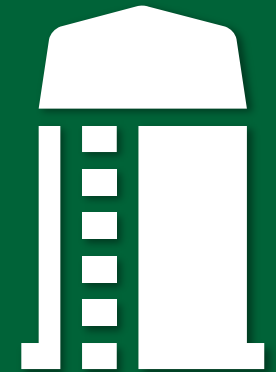
Accounting



ERP



Email



HR Docs

This raises the questions:

- How can we use AI safely?
- How can we avoid the data-silo trap?
- How can AI create measurable efficiency and P&L impact?

At MIS Solutions, these are the same questions we had to solve for our own business—and the questions we now help our customers answer.





What Were Our Choices?

OPTION 1 — BLOCK IT

Block ChatGPT, Claude, Gemini, Grok, and other public AI tools at the firewall.

OPTION 2 — ENABLE IT SAFELY

Evaluate enterprise AI tools and third-party platforms that provide security, visibility, governance, and control.

We needed a platform that provided:

- ✓ Secure AI access
- ✓ Visibility into usage
- ✓ Data protection controls
- ✓ Auditability and governance
- ✓ Integration with business knowledge

It didn't exist for SMBs. So, we built our own.



Why We Built **Secure Chat**

Secure Chat was created to solve a business challenge we faced ourselves.

THE GOAL

Give employees the benefits of AI without exposing sensitive company or customer information.



Now let's show you how MIS uses it to create real business value.

Operations Use Cases

How Secure Chat Works

Innovative ways MIS Solutions is using Secure Chat to complete tasks in minutes or even seconds that once took days or weeks to finish.

Eric Hammond, Data Center Technology Manager





The Problem: Your cyber insurance carriers asked for your IT policy concerning Access Controls to bind coverage.



The Solution: Secure Chat with document branding.



1

Insurance
Demand



2

Secure Chat



3

Creates Policy



4

Applies Branding



5

Coverage
Bound

Search chats...

CHATS

> TODAY (3) 

> YESTERDAY (22) 

> LAST 7 DAYS (16) 

PROJECTS

>  HIPAA Policies

>  Proactive \ Cloud (Tania Lee)

Finally Friday, Eric

Write an IT policy for Access Controls. It should be somewhat of a template for a company called "Healthy Inc" that stores PHI on servers locally



 Auto ▾

 Auto ▾



Research the web
Latest info from live sources



Create an image
Diagrams, art, wireframes



Analyze data
Upload a CSV, get charts



Talk to it
Hands-free voice chat

Secure Chat

Search chats...

CHATS

TODAY (3)

YESTERDAY (22)

LAST 7 DAYS (16)

PROJECTS

HIPAA Policies

Proactive \ Cloud (Tania Lee)

Write an IT policy for Access Controls. It should be somewhat of a template for

Write an IT policy for Access Controls. It should be somewhat of a template for a company called "Healthy Inc." that stores PHI on servers locally.

11:22 AM

11:23 AM

SECURE CHAT ASSISTANT via Claude Sonnet 4.6

Searching knowledge base

Thinking - 1 step - 63.7s

Here is a professional Access Control Policy template for Healthy Inc. You can download it as a Word or PDF document by clicking the Download button on the artifact below.

What's Included

This policy template covers the key areas required for HIPAA compliance and strong access control governance:

Access Authorization — formal request and approval process

Least Privilege / Need-to-Know — minimum necessary access to PHI

Role-Based Access Control (RBAC) — role-aligned permissions

User Account Management — provisioning, modification, and off-boarding

Password & MFA Requirements — complexity rules, logout, and session timeout

Privileged Access — controls for admin accounts

Remote Access — encrypted, MFA-protected channels only

Physical Server Security — on-prem server room access controls (relevant to Healthy Inc.'s local PHI storage)

Third-Party / Vendor Access — BAA requirements and scoped access

Access Reviews — semi-annual reviews with documented results

Audit Logging — 6-year log retention per HIPAA

Violations & Sanctions — disciplinary framework

Next Steps

Fields to customize are marked with brackets [] — fill in specific timeframes, personnel names, and thresholds based on Healthy Inc.'s environment. Consider also aligning this with a Risk Analysis to identify any additional controls needed for your specific server infrastructure.

Healthy Inc. - Access Control Policy

/prompt automate - Disk Space Low

Auto Auto

Search chats...

CHATS

TODAY

Write an IT policy for Acces...

Imagine yourself a security ...

Can you give me a list of co...

YESTERDAY (22)

LAST 7 DAYS (16)

PROJECTS

HIPAA Policies

Proactive \ Cloud (Tania Lee)

Write an IT policy for Access Controls. It should be somewhat of a template for

This policy template covers the key areas required for HIPAA compliance and strong access control governance:

- Access Authorization — formal request and approval process
- Least Privilege / Need-to-Know — minimum necessary access to PHI
- Role-Based Access Control (RBAC) — role-aligned permissions
- User Account Management — provisioning, modification, and off-boarding
- Password & MFA Requirements — complexity rules, logout, and session timeout
- Privileged Access — controls for admin accounts
- Remote Access — encrypted, MFA-protected channels only
- Physical Server Security — on-prem server room access controls (relevant to Healthy Inc.'s local PHI storage)
- Third-Party / Vendor Access — BAA requirements and scoped access
- Access Reviews — semi-annual reviews with documented results
- Audit Logging — 6-year log retention per HIPAA
- Violations & Sanctions — disciplinary framework

Next Steps

Fields to customize are marked with brackets [] — fill in specific timeframes, personnel names, and thresholds based on Healthy Inc.'s environment. Consider also aligning this with a Risk Analysis to identify any additional controls needed for your specific server infrastructure.

Healthy Inc. – Access Control Policy

Copy Download Add to Training Remember

Search the knowledge base for our renewal policy



Auto

Auto



Tab

Healthy Inc. – Access Control Policy

Document

Rendered document

Download

Access Control Policy

Organization: Healthy Inc. Policy Number: POL-SEC-001 Version: 1.0 Effective Date: [Enter Date] Last Reviewed: [Enter Date] Next Review Date: [Enter Date] Policy Owner: [Security Officer Name / Title] Approved By: [Executive Name / Title]

1. Purpose

The purpose of this policy is to establish formal guidelines for controlling access to information systems, networks, and data — including Protected Health Information (PHI) — maintained by Healthy Inc. This policy ensures that access to sensitive systems and data is granted on a least-privilege, need-to-know basis, and that all access is appropriately authorized, monitored, and reviewed.

This policy is designed to comply with applicable regulations, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (45 CFR §§ 164.312).

2. Scope

This policy applies to:

All Healthy Inc. employees, contractors, temporary workers, volunteers, and third-party vendors

All Healthy Inc. information systems, servers, workstations, and network infrastructure

All data stored, processed, or transmitted by Healthy Inc., including

Write an IT policy for Access Controls. It should be somewhat of a template for

This policy template covers the key areas required for HIPAA compliance and strong access control governance:

- Access Authorization** — formal request and approval process
- Least Privilege / Need-to-Know** — minimum necessary access to PHI
- Role-Based Access Control (RBAC)** — role-aligned permissions
- User Account Management** — provisioning, modification, and off-boarding
- Password & MFA Requirements** — complexity rules, lockout, and session timeout
- Privileged Access** — controls for admin accounts
- Remote Access** — encrypted, MFA-protected channels only
- Physical Server Security** — on-prem server room access controls (relevant to Healthy Inc.'s local PHI storage)
- Third-Party / Vendor Access** — BAA requirements and scoped access
- Access Reviews** — semi-annual reviews with documented results
- Audit Logging** — 6-year log retention per HIPAA
- Violations & Sanctions** — disciplinary framework

Next Steps

Fields to customize are marked with brackets [] — fill in specific timeframes, personnel names, and thresholds based on Healthy Inc.'s environment. Consider also aligning this with a Risk Analysis to identify any additional controls needed for your specific server infrastructure.

Healthy Inc. – Access Control Policy

Copy Download Add to Training Remember

Search the knowledge base for our renewal policy



Auto

Auto



Healthy Inc. – Access Control Policy

Document

Rendered document

Copy

Download

Access Control Policy

PDF (.pdf)

Word (.docx)

Organization: Healthy Inc. Policy Number: POL-SEC-001 Version: 1.0 Effective Date: [Enter Date] Last Reviewed: [Enter Date] Next Review Date: [Enter Date] Policy Owner: [Security Officer Name / Title] Approved By: [Executive Name / Title]

1. Purpose

The purpose of this policy is to establish formal guidelines for controlling access to information systems, networks, and data — including Protected Health Information (PHI) — maintained by Healthy Inc. This policy ensures that access to sensitive systems and data is granted on a least-privilege, need-to-know basis, and that all access is appropriately authorized, monitored, and reviewed.

This policy is designed to comply with applicable regulations, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (45 CFR §§ 164.312).

2. Scope

This policy applies to:

All Healthy Inc. employees, contractors, temporary workers, volunteers, and third-party vendors

All Healthy Inc. information systems, servers, workstations, and network infrastructure

All data stored, processed, or transmitted by Healthy Inc., including

Search chats...

CHATS

TODAY

Write an IT policy for Acces...

Imagine yourself a security ...

Can you give me a list of co...

YESTERDAY (22)

LAST 7 DAYS (16)

PROJECTS

HIPAA Policies

Proactive \ Cloud (Tania Lee)

This policy template covers the key areas required for HIPAA compliance and strong access control governance:

- Access Authorization** — formal request and approval process
- Least Privilege / Need-to-Know** — minimum necessary access to PHI
- Role-Based Access Control (RBAC)** — role-aligned permissions
- User Account Management** — provisioning, modification, and off-boarding
- Password & MFA Requirements** — complexity rules, lockout, and session timeout
- Privileged Access** — controls for admin accounts
- Remote Access** — encrypted, MFA-protected channels only
- Physical Server Security** — on-prem server room access controls (relevant to Healthy Inc.'s local PHI storage)
- Third-Party / Vendor Access** — BAA requirements and scoped access
- Access Reviews** — semi-annual reviews with documented results
- Audit Logging** — 6-year log retention per HIPAA
- Violations & Sanctions** — disciplinary framework

Next Steps

Fields to customize are marked with brackets [] — fill in specific timeframes, personnel names, and thresholds based on Healthy Inc.'s environment. Consider also aligning this with a Risk Analysis to identify any additional controls needed for your specific server infrastructure.

Healthy Inc. - Access Control Policy

Copy Download Add to Training Remember Like Share

Search the knowledge base for our renewal policy

Tab

Download Document

Your organization has brand guidelines configured. Would you like to apply them to this document?

Apply Branding

Download Plain

Download Document



Applying brand guidelines...

This may take a few seconds



Access Control Policy

Organization: Healthy Inc. Policy Number: POL-SEC-001 Version: 1.0 Effective Date: [Enter Date] Last Reviewed: [Enter Date] Next Review Date: [Enter Date] Policy Owner: [Security Officer Name / Title]
Approved By: [Executive Name / Title]

1. Purpose

The purpose of this policy is to establish formal guidelines for controlling access to information systems, networks, and data — including Protected Health Information (PHI) — maintained by Healthy Inc. This policy ensures that access to sensitive systems and data is granted on a least-privilege, need-to-know basis, and that all access is appropriately authorized, monitored, and reviewed.

This policy is designed to comply with applicable regulations, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (45 CFR §§ 164.312).

2. Scope

This policy applies to:

- All Healthy Inc. employees, contractors, temporary workers, volunteers, and third-party vendors
- All Healthy Inc. information systems, servers, workstations, and network infrastructure
- All data stored, processed, or transmitted by Healthy Inc., including Protected Health Information (PHI) stored on local on-premises servers
- All physical locations where Healthy Inc. IT systems or data reside

Make IT possible.

www.mis-solutions.com | 678-745-5109 | 4485 Tench Road, Suite 440, Suwanee, GA 30024



3. Definitions

Term	Definition
PHI	Protected Health Information — individually identifiable health information created, received, maintained, or transmitted by a covered entity
Least Privilege	The principle that users are granted the minimum level of access required to perform their job duties
Need-to-Know	Access is limited to only those individuals who require the information to perform their assigned responsibilities
Role-Based Access Control (RBAC)	Access rights assigned based on defined job roles and responsibilities
Privileged Account	An account with elevated permissions, such as system or network administrators
Security Officer	The designated individual responsible for overseeing information security and HIPAA compliance
Multi-Factor Authentication (MFA)	A security mechanism requiring two or more verification factors to grant access

4. Policy Statements

4.1 Access Authorization

- All access to Healthy Inc. information systems and PHI must be formally authorized before access is granted.

Make IT possible.

www.mis-solutions.com | 678-745-5109 | 4485 Tench Road, Suite 440, Suwanee, GA 30024



- Access requests must be submitted to the IT department via an approved ticketing or request process and must be approved by the requestor's department head and the Security Officer (or designated IT authority).

- Access shall be granted based on the individual's role, job function, and demonstrated need-to-know.

- No user shall be granted access to PHI or sensitive systems without documented authorization.

4.2 Least Privilege and Need-to-Know

- Users shall be granted only the minimum necessary access required to perform their job responsibilities.

- Access to PHI stored on local servers shall be restricted to personnel whose job duties directly require interaction with that data.

- Elevated or administrative privileges shall only be issued to IT staff with a documented business need and shall not be used for routine, non-administrative tasks.

4.3 Role-Based Access Control (RBAC)

- Healthy Inc. shall implement Role-Based Access Control across all applicable systems and servers.

- Access roles and permission sets shall be defined, documented, and maintained by the IT department in coordination with department heads.

- When an employee's role changes (e.g., promotion, transfer, role modification), access rights shall be reviewed and updated within [X business days] of the change.

Make IT possible.

www.mis-solutions.com | 678-745-5109 | 4485 Tench Road, Suite 440, Suwanee, GA 30024

POTENTIAL USE CASES

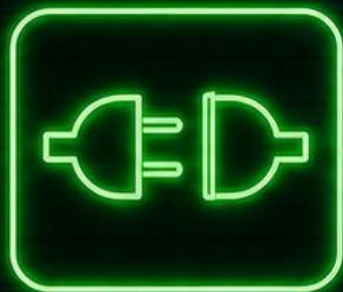


• YOUR DATA.



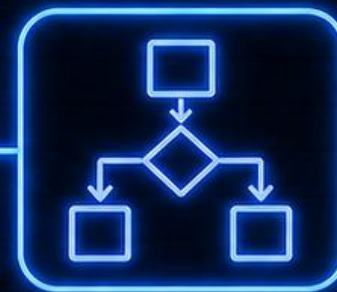
ALWAYS PROTECTED. •

Getting a black belt in Secure Chat



Connectors

Connect securely.
Integrate seamlessly.



Workflows

Automate conversations.
Drive outcomes.



Recipes

Pre-built. Proven.
Powerful.



Packages

Deploy. Share.
Scale.





SECURE CHAT

SALESFORCE

Secure Chat Recipes



ADD A STEP

Trigger

Connector

Secure Chat Tasks

Recipe

AI Prompt

MCP AI Step

Condition

For Each

Notify

Microsoft 365

Task

Stop

Click a step to add it, then drag the dots between steps to connect them.

Weekly trigger

Weekly · Mon at 09:00

Review inbox emails

inbox

Identify replies needed

Today's date is {{today}}. Review the inbox emai...

Email report

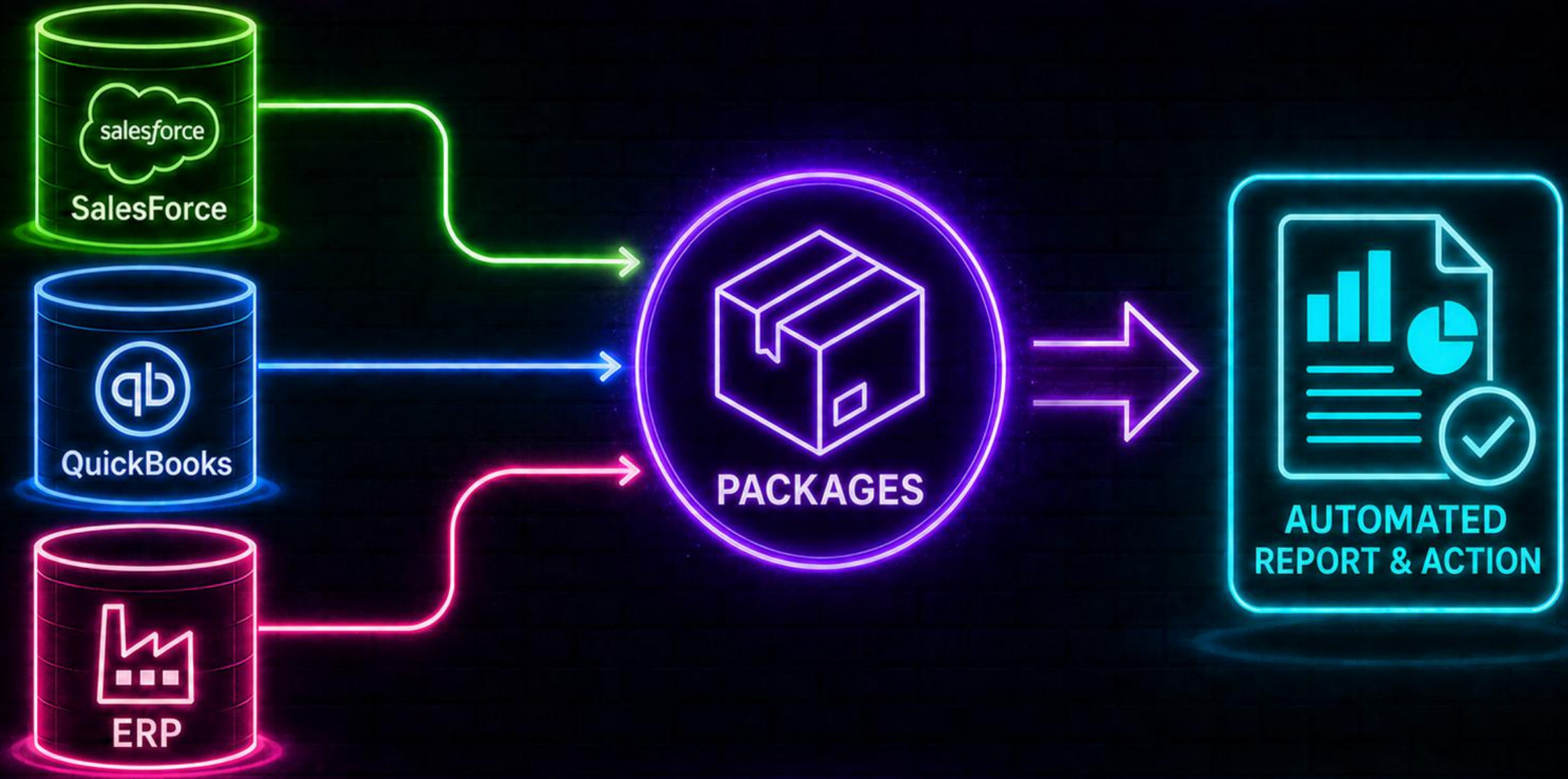
email notification

End

end

Select a step to configure it, or click a step in the palette to add one.

Packages - A Silo Smashing Symphony



Secure Chat Mastery



Marketing Use Cases

From Idea to Execution

How we used Secure Chat to plan and build this event.

Gina Kopf, Marketing Manager



AI Is Changing the Way We Work



Move Faster



Stay Organized

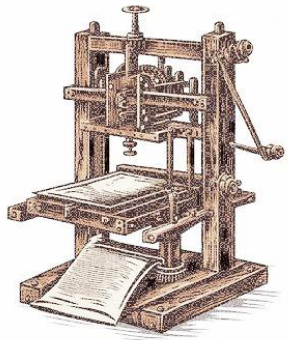


Better Decisions



Meet Demands

Evolution of How We Access Information



1400's

Printing Press

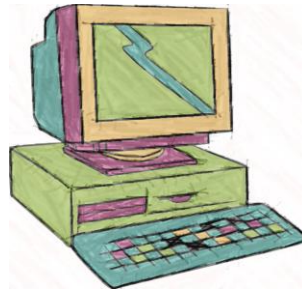
Knowledge
becomes available
to the masses



1800's

Typewriter

Creating text
becomes available
to the masses



1990's

Internet

Info accessible
if you know where
to search for it



2000's

Search Engines

Digital library to
sort billions of pages
of info instantly



2023+

AI Revolution

Technology as
companion to solve
complex problems

To-Do's for Creating this Event

01 Create a plan for the event

02 Create email campaign & calendar

03 Create social content & graphics

04 Create a landing page for registrations

05 Design handouts + Presentation

06 Create a new website for new product

07 Develop training materials for team

08 Be sure all channels tell the same story

It Started With a Prompt

Help me draft a brief for an upcoming executive AI event. We want to position it as a business leadership workshop focused on how AI creates value for small and midsize organizations. Secure Chat should be introduced as a practical example of how MIS Solutions is implementing these ideas.



SECURE CHAT ASSISTANT via Gemini 2.5 Flash

Searching knowledge base, analyzing your files

Thinking · 2 steps · 11s

Here is a draft for your executive AI event brief, Gina Kopf, incorporating all the strategic positioning we've discussed. This brief positions the event as a valuable business leadership workshop, w

Event Brief: AI in Action Executive Workshop

Driving Business Value and Secure AI Adoption for SMB Leaders

Event Name: AI in Action: Practical AI Workflows for Business Leaders (Secondary / Tagline: Featuring Real-World Examples from MIS Solutions)

Date: Thursday, July 30, 2026 **Location:** The Water Tower, Buford, GA

1. Overall Event Goal

To educate and empower small and midsize business (SMB) leaders on how Artificial Intelligence (AI) can create tangible business value, improve productivity, and enhance strategic decision-ma

2. Target Audience

Primary: Executive-level leaders of small and midsize businesses (20-250 employees).

Event Planning Workflow

To start, I gave the app more than just my question or prompt.

Over the last months, the team uploaded relevant context to the Knowledge Base.

- Uploaded all feedback gathered from our last event so we can always be improving
- Uploaded brand guidelines for MIS Solutions
- Uploaded the product documents explaining Secure Chat
- Shared our event goals and target audience
- Shared the channels we plan to use for promotional outreach
- Uploaded results/analytics from past campaigns – Email and LinkedIn engagement

Content Development Used Prompts

Great! Now that we have a plan taking shape, can you help me create an invitation email and social content to promote this event? The social post will be via MIS LinkedIn page and emails will target our client and prospect database.



SECURE CHAT ASSISTANT Gemini 2.5 Flash

Absolutely, Gina Kopf! With the clear event brief and

Here's a draft for an invitation email and two LinkedIn

1. Invitation Email Draft

This email is designed to be the primary invitation, bu

Subject Line: AI in Action: Practical Strategies for Bu

Dear [Recipient Name],

AI is fundamentally reshaping the business landscape

Many organizations are asking: **How do we harness A**

At MIS Solutions, we've been helping Georgia busines

Why Attend This Workshop?

This isn't a product pitch; it's a leadership session for

Boost Productivity: Discover real-world AI workflc

Make Smarter Decisions: Learn how AI can enhar

Protect Your Business: Understand how to confid

Avoid "Shadow AI": Replace uncontrolled AI use v

Who You'll Hear From

2. LinkedIn Social Content (2 Posts)

These posts adopt the "business leadership workshop" positioning, focus on the value, and incorporate the new landing page strategy's messaging.

LinkedIn Post 1: Problem-Led & Value-Focused

Post Copy: Is your business truly leveraging AI, or just experimenting? For SMB leaders, moving beyond experimentation to measurable value can be a challenge

Join MIS Solutions for "AI in Action: Practical AI Workflows for Business Leaders" on July 30th. This isn't about AI hype; it's a workshop for CEOs, Operations, a

We'll share real-world examples from MIS Solutions on how we implement AI securely and effectively, featuring our private AI platform, Secure Chat.

Date: Thursday, July 30 **Location:** The Water Tower, Buford, GA

Reserve your seat and transform AI potential into business results. *(Link to new high-converting landing page)* #AlinAction #BusinessLeaders #SMB #AIGoverna

Visual Recommendation:

Type: Branded Graphic / Infographic-style

Content: A graphic with the event title "AI in Action: Practical AI Workflows for Business Leaders." Visually represent the three key benefits (Productivity, Decis

Why it works: Directly addresses a pain point, promises clear outcomes, and uses a visual to quickly convey the workshop's value.

LinkedIn Post 2: Speaker Spotlight & Urgency

Post Copy: Meet your guides to practical AI: On July 30th, join Lliam Holmes, Founder of Secure Chat & Chief Security Strategist, and myself, **Gina Kopf**, Marketi

One Conversation, Multiple Outputs



AI in ACTION for business leaders

Practical Secure Chat Workflows for Business Leaders

Real Workflows. Real Use Cases. Real Business Results.

Join us Thursday, July 30
8:30 AM – 11:00 AM
The Water Tower | Buford, GA

Last month, we introduced the conversation around AI usage and governance and received only business leaders' strategies for adopting AI responsibly.

Now we're taking the next step to address how to use AI effectively while maintaining security, visibility, and control.

Join MIS Solutions for our first AI in Action workshop, where we will explore the conversation and demonstrate how AI is being used across leadership, operations, and marketing to improve productivity, streamline workflows, and support better business decisions.

After this morning on AI theory in business leaders, this session will introduce practical scenarios and real-world use cases covered by Secure Chat, a private AI environment designed to help businesses embrace AI while maintaining governance and control.

This is a private session with demonstration:

- How AI is changing the way business operates
- Real-world examples of AI in leadership, operations, and marketing
- Practical use cases for improving productivity and efficiency
- Key considerations for secure and governed AI adoption
- How Secure Chat helps balance innovation with security and visibility

Save Your Seat Today

Your Journey to Secure AI Adoption Starts Here

Secure Chat

First Name Last Name

Phone Email

Company Name

Yes No

Register Now

Coffee and a light breakfast will be served. Seating is limited.

Why Attend an MIS Workshop?

Serving Georgia Businesses Since 1995

For more than 30 years, MIS Solutions has helped Georgia businesses use technology to become more innovative, productive, and prepared for what's next.

Today, with leading organizations recognizing one of the biggest technology skills in demand – Artificial Intelligence, this workshop is an opportunity to share what you've learned. Learn more about our [AI Adoption](#) event.



Featured Presenters



Liam Holmes, CEO

Join Liam as the Chief Security Strategist, Co-Founder, and CEO of MIS Solutions, Inc. to see how more than 30 years' experience in strategy, technology, and cybersecurity shaped MIS Solutions and the company's vision for the future of AI in business.

Join all speakers for an AI in Action workshop where we will explore the conversation and demonstrate how AI is being used across leadership, operations, and marketing to improve productivity, streamline workflows, and support better business decisions.



Eric Hammond, Data Center Tech Manager

Eric Hammond brings more than 20 years of experience in business operations, technology, hardware, and cloud computing. He is responsible for managing and maintaining the company's data center infrastructure, ensuring high availability and security of the company's data.

Join all speakers for an AI in Action workshop where we will explore the conversation and demonstrate how AI is being used across leadership, operations, and marketing to improve productivity, streamline workflows, and support better business decisions.



Gina Kopf, Marketing Manager

Gina Kopf brings over a decade of experience in business operations, technology, hardware, and cloud computing. She is responsible for managing and maintaining the company's data center infrastructure, ensuring high availability and security of the company's data.

Join all speakers for an AI in Action workshop where we will explore the conversation and demonstrate how AI is being used across leadership, operations, and marketing to improve productivity, streamline workflows, and support better business decisions.



AI in ACTION for business leaders

Hi there,

Your employees are using AI to draft emails, summarize documents, and analyze data. In many organizations, this is happening with little to no visibility or guidance.

The question: How to embrace AI so it creates value while maintaining security, governance, and control?

That's what we'll be discussing at AI in Action! Experience real workflows, real use cases, and real business results.

Join our first AI in Action Workshop: Practical Secure Chat Workflows for Business Leaders

- Learn how Secure Chat helps business leaders use AI to improve productivity
- See real-world examples from leadership, operations, and marketing teams
- Discover how to streamline workflows and reduce manual effort
- Embrace AI while maintaining security, visibility, and control

In-Person Event Details

Thursday, July 30
8:30 AM – 11:00 AM EDT
The Water Tower | Buford, GA

Save Your Seat

Presenters and Use Cases

Explore how Secure Chat helps businesses balance innovation with data governance.



Liam Holmes
CEO and Founder

Understand how business leaders are balancing innovation, productivity, and governance in the age of AI.



Eric Hammond
Data Center Tech Manager

Learn how Secure Chat improves operational efficiency, reporting, and decision-making.



Gina Kopf
Marketing Manager

See how Secure Chat accelerates content creation and campaign execution in line with brand standards.



MIS Solutions, Inc.

How do you give employees access to the benefits of AI without introducing unnecessary business risk?

That's the challenge many organizations are trying to solve right now.

Join us for AI in Action: Practical Secure Chat Workflows for Business Leaders. We'll discuss how SMBs can improve productivity and efficiency while maintaining governance, security, and visibility.

You'll hear practical examples from leadership, operations, and marketing teams that are already putting AI to work every day.

July 30
The Water Tower | Buford, GA

>> Reserve your seat today. <https://hubs.li/Q04nF8N0>

#AIAAdoption #CyberSecurity #BusinessTechnology #SecureChat #MISolutions



AI in Action for Business Leaders

Practical Secure Chat Workflows for Business Leaders

Join us to learn from our own use cases and real business results.



LIAM HOLMES
CEO & FOUNDER



ERIC HAMMOND
DATA CENTER TECH MANAGER



GINA KOPF
MARKETING MANAGER

Thursday 8:30 AM EDT

July 30 2026

The Water Tower | Buford, GA

2500 Clean Water Court

AI Your Team Can Use Control Your Business Can Trust

Secure Chat

AI is already inside your business. Is usage happening in a secure environment?

Employees are using commercial AI platforms in everyday work tasks. Risk happens without visibility, governance, or controlled protection.

THE PROBLEM

Uncontrolled AI usage creates real business risk.

- Shadow AI Usage**
Employees use public AI tools without oversight.
- No Audit Visibility**
You do not know what tools are being used or how.
- No Policy Control**
Proper AI Governance is currently nonexistent.
- Disconnected Data**
Generic answers instead of insights from your data.
- Data Exposure Risk**
Sensitive info may be shared on public platforms.

THE SOLUTION

Support for a private, governed AI environment.

- Private and Secure**
Encrypted environment with DLP protection.
- Visibility and Control**
See how AI is used with audit logs and admin controls.
- Governed AI Usage**
Enforce policies, control access, and protect data.
- Connected Intelligence**
Answers from company docs, knowledge, and live data.
- Ready for Business**
Easy for employees to use and easy for IT to trust!

Use AI Confidently While Staying In Control

Secure Chat helps businesses embrace AI securely through a centralized, private AI environment where employees can work faster, and leadership maintains visibility, control, and protection over sensitive company data. Built with enterprise-grade security, audit visibility, DLP protection, and intelligent business system connectivity, this was designed to support secure AI adoption at scale.

The Only AI Built for Business. mysecurechat.ai

Planning vs Execution

The real challenge came over the next several weeks, aligning the team on goals, timelines, and deliverables.

- Exchanged dozens of emails and Teams messages.
- Planning meetings every Monday.
- Brainstorming sessions on Thursday.
- Discussions with our account management team.
- Branding conversations.
- Executive feedback.
- Content revisions.



The Conversation Continued

Can you please search @M365 Teams, @M365 Email, @M365 Calendar, and gather all notes about next steps for the team to be ready for this event?



✉ 18 emails found · 5 best

Searching: Gather

Best matches

> Secure Ch
Gina Kopf ·
Direct Match
We are aski

> FW: Secur
Gina Kopf ·
Direct Match
I'd like to ha

> FW: Secur
Gina Kopf ·
Direct Match
The goal is t

> AI in Actio
Gina Kopf ·
Direct Match

🗒 14 Teams messages found

> # Gina Kopf Channel
Tue, Jun 30, 2026, 4:22 PM
I shared this updated event playbook with Lance and Debbie this morning as they were planning to review event planning today. wanted to make sure you have
[Open in Teams](#)

> 👤 Gina Kopf Chat
Thu, Jul 9, 2026, 3:01 PM
Hi there. sharing the Event Playbook for AI in Action. I added the info to this doc that we discussed this morning and entered into Coda. Please add any items I
[Open in Teams](#)

> 👤 Gina Kopf Chat
Mon, Jun 29, 2026, 6:17 PM
For tomorrow morning, attached is the updated in-person event planning document to review as part of the event training. right now it is saved in the following
[Open in Teams](#)

> # Gina Kopf Channel

Bringing Data Together Across Systems

Now, can you please put this information into a To-Do list that I can share with my team?



Next Steps for AI in Action July 2026 Event Readiness

I. Core Marketing Deliverables (from Secure Chat Marketing Brief July 2026)

Marketing Positioning Document

Next Step: Obtain approval from the team.

Owner: Gina Kopf

2-page Handout

Next Step: Obtain approval from the team.

Owner: Gina Kopf

Logo and Brand Guidelines

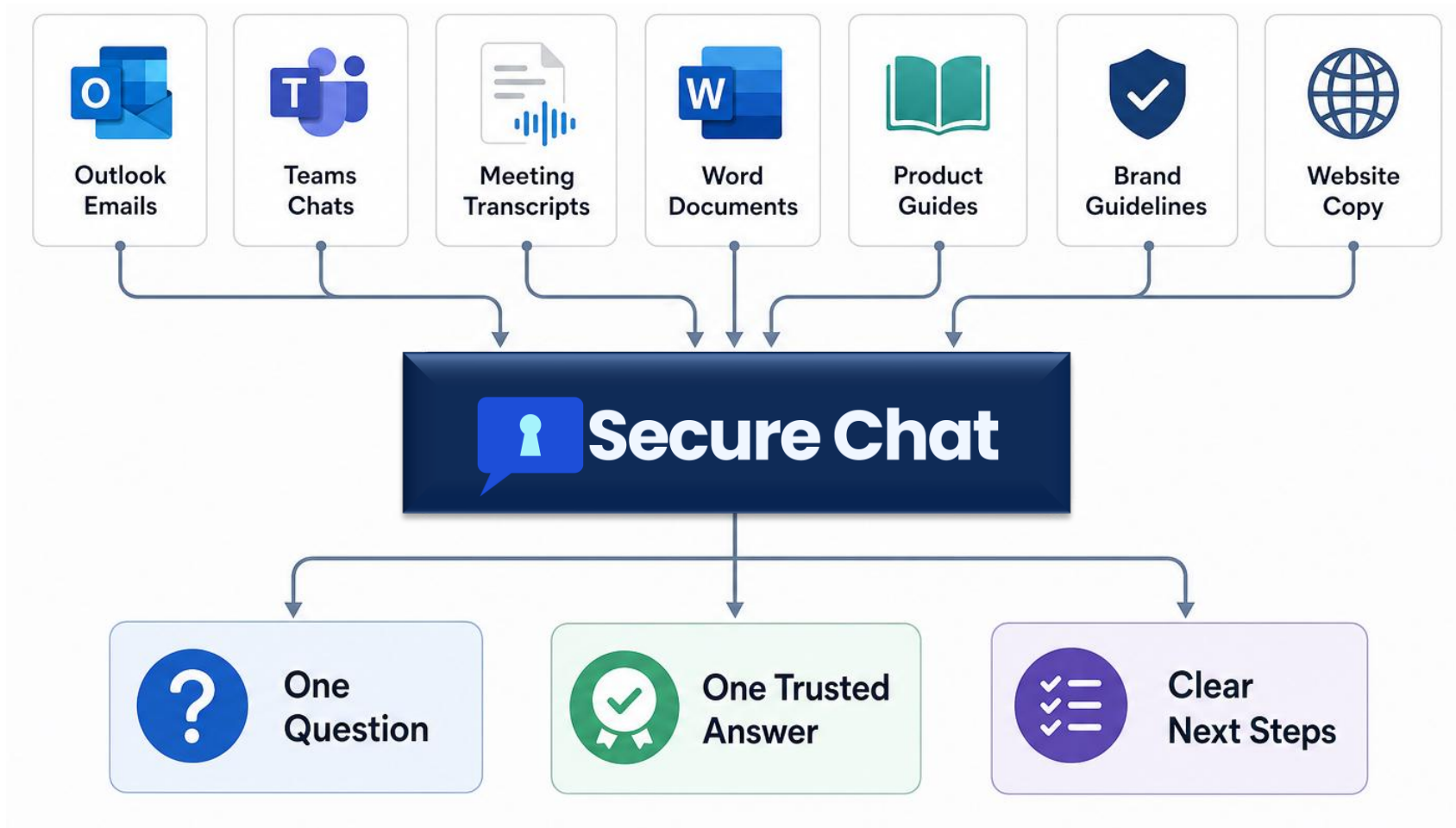
Next Step: Finalize the guidelines.

Owner: Carol

Product Overview (Internal)



Getting & Staying on the Same Page



Next Steps



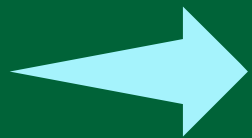
Get Secure Chat



Resource Page



Event Feedback



Get your 14-day free trial with code AllA-73026

Code expires Sept. 1, 2026

Thank You for Joining Us!