FELLOW

AI Meeting Assistant Security Checklist

AI meeting assistants are a must-have in 2025, but not all are created equal when it comes to security. Here’s what to consider.

For Organizational Leaders

1 Check for SOC 2 or ISO 27001 compliance

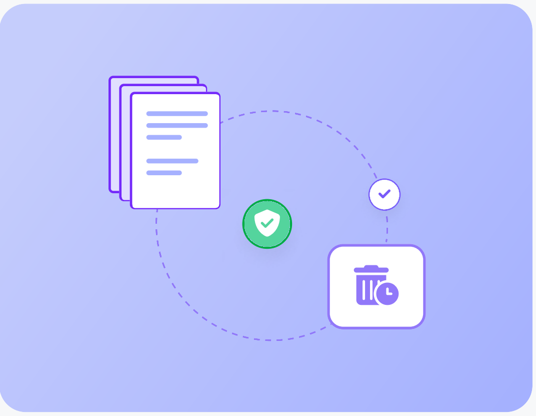
Ensure the AI meeting assistant has undergone a SOC 2 audit or ISO 27001 certification. In either case, it confirms that data protection standards are in place and is a good indicator of an AI meeting assistant's overall commitment to security and privacy.

2 Check for industry-specific certifications

Make sure that if your particular industry or region requires additional certifications or protocols they are followed. For example, if your organization is in health care, ensure HIPAA compliance.

3 Ask how long data is stored

Find out the default data retention period and whether you can adjust it. Shorter retention periods reduce risk and the ability to delete old data ensures better control over sensitive information.



4 Can you download and delete data?

Verify that you can access and delete your meeting data at any time. This is crucial for legal compliance, particularly with regulations like GDPR, and for maintaining control over proprietary information.

5 Ask about third-party vendor security

Ask which third-party AI vendors the AI meeting assistant relies on and whether those vendors maintain the same security standards. Ensure they're transparent about data processing practices and compliance certifications.

6 Is it clear when the recording is happening?

Look for a tool that clearly indicates when recording begins, such as joining as a visible attendee or displaying a recording icon. This transparency reduces the risk of legal issues around consent.

7 Set up recording rules

Establish organizational guidelines for when recordings are allowed. For example, restrict AI meeting assistants from recording legal meetings or performance management discussions.

8 Set up recording access permissions

Implement access controls for recorded meetings. Permissions should ensure that only authorized employees or third parties can view or share recordings.

9 Limit access to admin settings

Restrict access to the AI meeting assistant's administrative settings to a select group. This ensures that only authorized personnel can make changes to recording rules and permissions.

10 Implement a single AI meeting assistant organization-wide

Finally, once you've assessed and approved an AI meeting assistant, share with all employees that it's the only AI meeting assistant that has been approved for use and assure compliance.

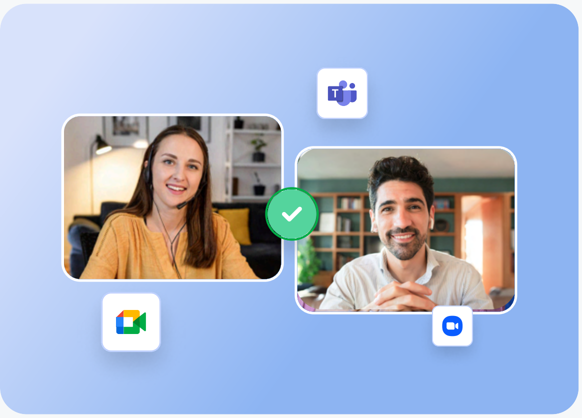
For Employees

1 Use strong passwords and enable 2FA

Employees should protect their accounts with a strong, unique password and enable two-factor authentication for an additional layer of security.

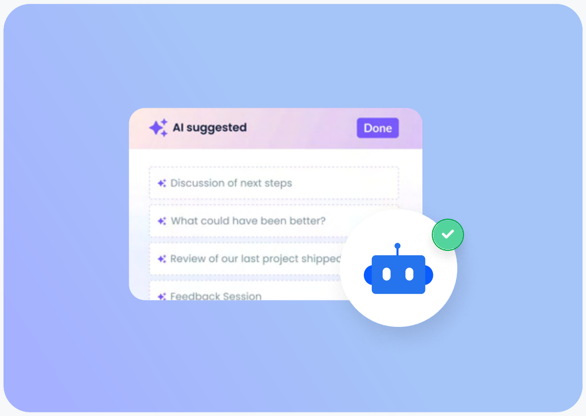
2 Ask for recording consent

Before recording a meeting, ensure all attendees are aware and have provided their consent.



3 Confirm organizational approval

Check that the AI meeting assistant you're using has been vetted and approved by your organization. Avoid using unapproved tools that could compromise security.


AI suggested
Done
Discussion of next steps
What could have been better?
Review of our last project shipped
Feedback Session

4 Regularly update software

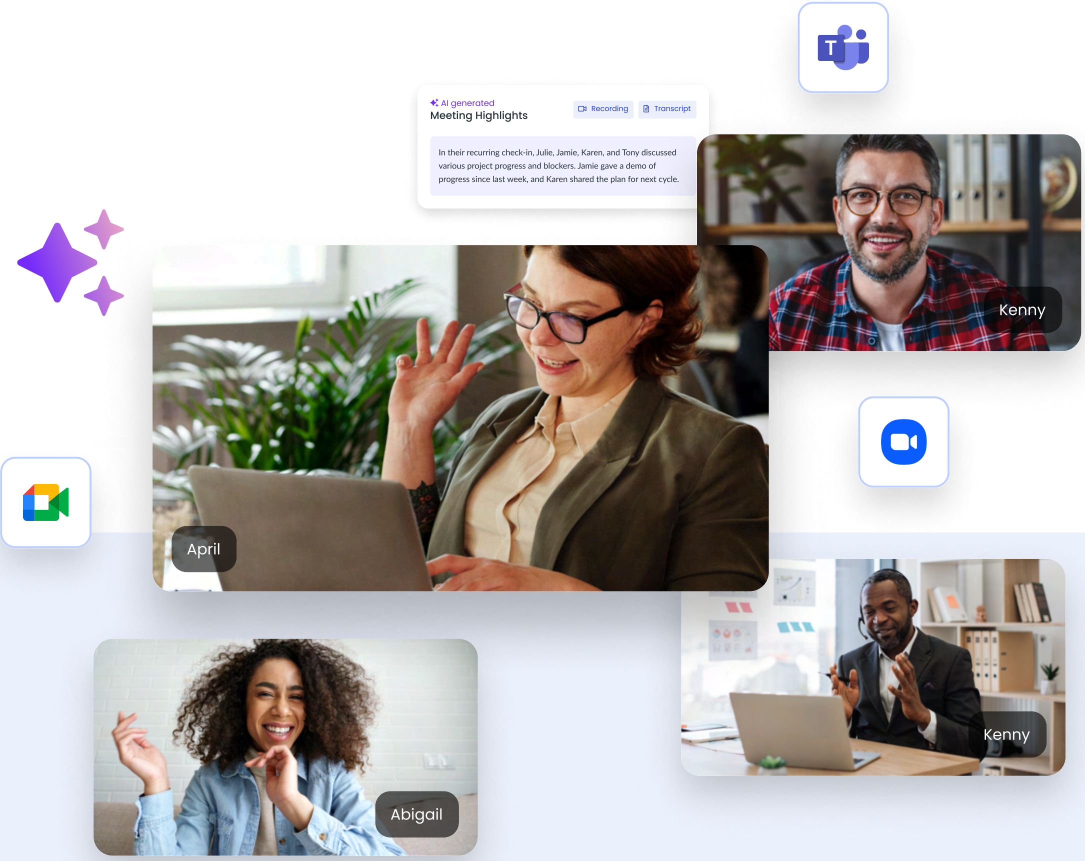
Keep the AI meeting assistant software updated to benefit from the latest security patches and feature improvements. Outdated software is more vulnerable to breaches.

5 Be cautious about sharing notes

Only share meeting notes with those who need access. Over-sharing could expose sensitive information to unintended recipients.

6 Review recaps for compliance

After a meeting, check the AI-generated summaries and transcripts for accuracy and compliance with organizational standards. Redact any sensitive information that shouldn't have been recorded.

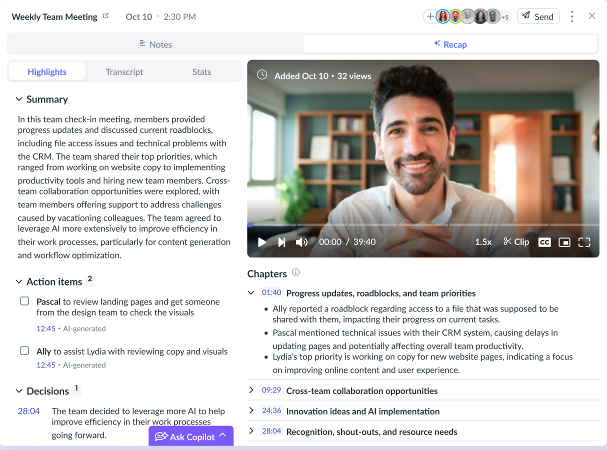


AI generated
Meeting Highlights

In their recurring check-in, Julie, Jamie, Karen, and Tony discussed various project progress and blockers. Jamie gave a demo of progress since last week, and Karen shared the plan for next cycle.

The only AI meeting assistant built from the ground up with privacy and security in mind.

Fellow's comprehensive and customizable privacy controls allow leaders to govern AI recording across the organization. Built to support every team and meeting type, Fellow offers a centralized approach to AI recording and note taking making it a scalable and secure solution for the entire organization.



Summary

In this team check-in meeting, members provided progress updates and discussed current roadblocks, including file access issues and technical problems with the CRM. The team shared their top priorities, which ranged from working on website copy to implementing productivity tools and hiring new team members. Cross-team collaboration opportunities were explored, with team members offering support to address challenges caused by vacationing colleagues. The team agreed to leverage AI more extensively to improve efficiency in their work processes, particularly for content generation and workflow optimization.

Action items 2

- ☐ **Pascal** to review landing pages and get someone from the design team to check the visuals
  12:45 • AI-generated
- ☐ **Ally** to assist Lydia with reviewing copy and visuals
  12:45 • AI-generated

Decisions 1

28:04 The team decided to leverage more AI to help improve efficiency in their work processes going forward.

Chapters

01:40 **Progress updates, roadblocks, and team priorities**

- Ally reported a roadblock regarding access to a file that was supposed to be shared with them, impacting their progress on current tasks.
- Pascal mentioned technical issues with their CRM system, causing delays in updating pages and potentially affecting overall team productivity.
- Lydia's top priority is working on copy for new website pages, indicating a focus on improving online content and user experience.

09:29 **Cross-team collaboration opportunities**

24:36 **Innovation ideas and AI implementation**

28:04 **Recognition, shout-outs, and resource needs**

AI meeting recording, transcription and recaps with privacy, control and security at its core

Access permissioning

Fellow's recap library provides customizable channels with their own access permissions and rules. This allows the organization to centralize all their meeting recording while providing the privacy and control over who can access which meeting recaps, recordings and transcripts.

Pause and Resume recording

Maintain privacy of sensitive information without missing out on documenting the rest of the meeting. With Fellow, any meeting attendee can pause the recording of the meeting in one click and resume the recording when they're ready.

Any information shared during the pause will also be removed from the transcript and meeting notes.

Redaction

Attendees can redact any part of the meeting from the transcript, recording, summary, and action items that may be sensitive and regenerate the meeting recap

Review recaps for compliance

After a meeting, check the AI-generated summaries and transcripts for accuracy and compliance with organizational standards. Redact any sensitive information that shouldn't have been recorded.

shopify Uber UNIVERSITY OF MICHIGAN Stanford University Webflow motorola Fanatics