



# Securely Deploying Copilot for Microsoft 365

## 5 Copilot Security Best Practices



harmonic

# 1. Create a Policy (1/2)



- Start Early.** Don't wait until you have an "AI initiative" to create an AI policy.
- Involve the Right Stakeholders.** Are security, engineering, legal, compliance, product, IT, and identity involved to help create the policy?
- Set Strategy for Copilot.** Be explicit about what you want to achieve with Copilot, what's included, and what's not included.



# 1. Create a Policy (2/2)



**Craft a Specific, Well-Written Policy.** Create a policy that is well-worded and written for humans. It should outline real use cases and give specific examples.



**Review Regularly.** Do you have enough feedback from the business? Do you meet at a regular cadence? Is the policy reviewed and refined at a set cadence?

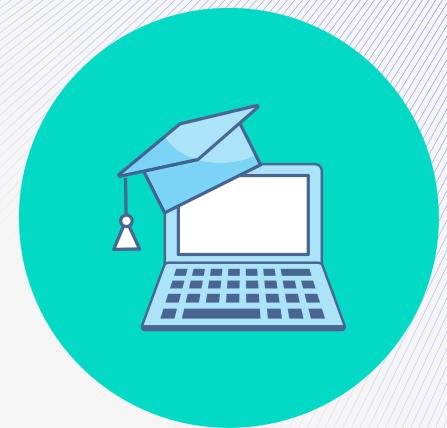


**Decide Scope.** Based on the defined use cases, stakeholders, and desired outcomes, define the scope of the initial rollout. Start small and prove out.



**Benchmark.** Create benchmarks that help to understand how you are performing against the defined AI policy.

## 2. User Training



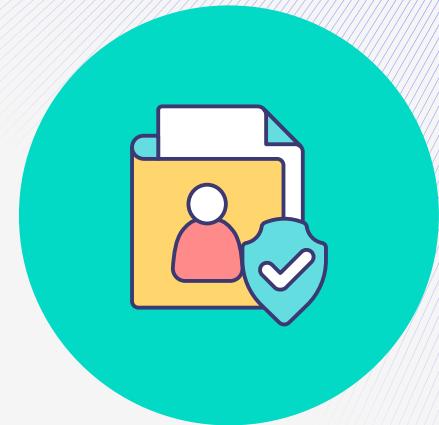
- Focused and Use Case Specific.** Training should focus on developing specific practical skills and behaviors tied to business use cases.
- Coach on Reviewing AI Output.** Ensure employees know the importance of reviewing AI output for accuracy and ask Copilot to cite sources.
- Vary Training Types.** A one-off online training may not be enough to engage the user.
- Have a Plan to Revisit Regularly.** Training should be continuous, tailored, and refreshed often!

### 3. Limit Permissions



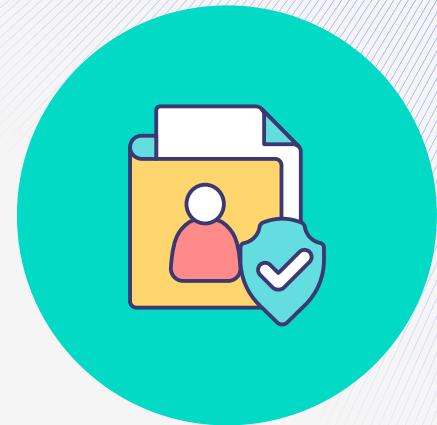
- Be Selective.** Select trial uses with limited permission sets to reduce the risk of accidental data leakage.
- Perform Regular Access Reviews.** You likely already have a set cadence for access reviews but consider a one-off effort before rolling out.
- Get Close to Identity Teams.** Ensure identity teams part of the process
- Protect Privileged Accounts.** These accounts will provide most access and should be the focus going forward.

# 4. Understand Your Data, Inputs and Outputs (1/2)



- Understand your Data.** Better organization of data will help to restrict unauthorized access, but it will also help to improve the quality of the Copilot responses.
- Data Retention.** Create and enforce a data retention policy that will remove outdated data that hinders the quality of Copilot responses.
- Labeling.** Data labeling can be a painful exercise, but Microsoft is pushing this hard to reduce the risk of sensitive data leakage. Automated labeling is available to E5 licenses.
- Consume Logs.** Don't blindly trust – get visibility into what is going on!

## 4. Understand Your Data, Inputs and Outputs (2/2)



**Ensure Output Quality.** Users should consider taking an extra step and always ask Copilot to cite its work.



**Detect Risky Users.** Use existing signals to identify risky users and reduce account takeover risks. Entra ID's risky user detections will provide some visibility.

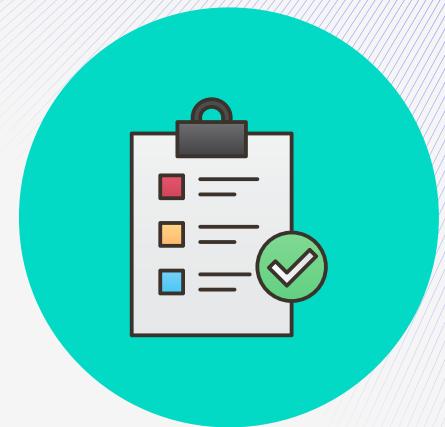


**Sensitive Data Detection.** Remember, sensitive data that is an output from Copilot may still be shared externally.



**Third Party Guardrails.** Investigate innovative security vendors (like Harmonic!) that can detect sensitive data and mitigate the risk.

## 5. Reading the Smallprint



- Copilot Feedback.** Is end-user feedback opt-in enabled? Consider what you are sending back to Microsoft and what that means for data leaving your tenant.
- Bing Search Queries.** Are Bing search queries enabled? Beware that this data will go outside of the boundary.
- Transcription for Teams.** To benefit from post-meeting summaries, admins will need to enable transcription in the [Teams Admin Center](#).
- Change Channel.** Copilot cannot be enabled on a Semi-Annual Enterprise Channel, and requires that you set your channel to “Current” or “Monthly”.



# Secure AI's Future with Harmonic

Harmonic is at the forefront of secure AI adoption, providing solutions that safeguard your data while empowering innovation.

## Why Harmonic?

- Precise risk control and AI visibility.
- Automated solutions to lighten your security team's load.
- Proactive data protection for AI innovation.

**Book a meeting to learn more about Harmonic's data security platform.**

**Book Now**

