Copilot

Copilot for Microsoft 365

A handbook for partners

Table of Contents

Chapter 1
Planning

Prerequisites

Copilot for Microsoft 365 subscription
Business Standard and above
Office E3 or Microsoft E3 and above or A3-A5 faculty

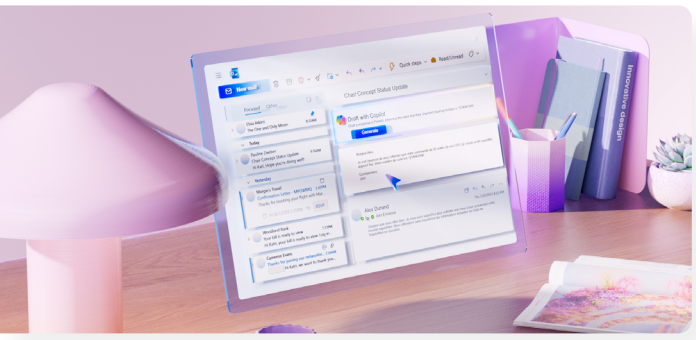
New Outlook for Windows

Update channels set to either Current Channel or Monthly Enterprise Channel

Best practices prior to rollout or adoption of Copilot

End-user training
Organizations must ensure their users understand Copilot for Microsoft 365's capabilities to set proper user expectations. They should develop training materials and FAQs to educate users on how to best utilize Copilot for Microsoft 365. They should also collect and develop training resources to educate end users on how to benefit from Copilot for Microsoft 365's suggestions. Setting expectations upfront is key to driving user adoption.

Helpdesk readiness
Prepare Helpdesk teams to be familiar with AI. Doing so results in better customer support and instills confidence in the Helpdesk team. Early training of Helpdesk personnel also helps get them invested in the success of Copilot for Microsoft 365 adoption. When Helpdesk teams understand Copilot for Microsoft 365, they can answer questions, troubleshoot issues and guide customers more effectively. All of this will lead to improved customer satisfaction.



Prepare for launch

Identify early adopter teams or individuals that can test Copilot for Microsoft 365 and provide feedback
Organizations should consider employing a structured rollout plan that includes good change management practices. For example, when rolling out Copilot for Microsoft 365, you can consider launching it in a limited pilot group first. Doing so allows you to gather feedback, assess value and optimize configurations before a wider rollout. You can then scale usage and customize it for more teams once the pilot demonstrates results.

Monitor usage and feedback
Keep track of how extensively users are employing Copilot for Microsoft 365 across your organization. Look for teams or individuals who are early adopters and can provide useful feedback and help champion Copilot for Microsoft 365 adoption among their coworkers. Solicit input from users on Copilot for Microsoft 365's suggestions. Was it helpful? Did it miss key contexts? Was training adequate? This type of feedback can help you improve user training.

Evaluate security diligently
It's important that organizations use the permission models that are available in Microsoft 365 services. This will ensure the right users or groups have access to the correct content. Microsoft provides powerful security tools within its Microsoft 365 and Azure ecosystems that help organizations tighten permissions and implement the right amount of access. To prevent data oversharing, Microsoft 365, Azure and Copilot for Microsoft 365 all use the same policies and settings that administrators defined within these tools.

Chapter 2
Data preparation

Best practices

Clean out redundant, outdated and trivial (ROT) content
Remove outdated materials that are no longer accurate or relevant and perform an extensive audit of all organizational content (documents, emails, chats and wikis).

For example, you can delete the following: old product specification sheets that are five years old or older, promotional emails for expired campaigns and resolved IT ticket conversations.

In addition, you can enable archive/deletion policies on collaborative platforms to automate removal of stale content, ongoing removal of obsolete and irrelevant content focuses Copilot for Microsoft 365 on current, high-value information.

Tip: *The use of retention policies and retention labels can help organizations comply proactively with industry regulations and internal policies, reduce risk if a litigation event or a security breach occurs and ensure users only work with content that is current and relevant to them.*

Organize content into logical folders and sites
Structure your files, emails and pages thoughtfully, and design a detailed taxonomy for categorizing documents, emails and landing pages. For example, within document libraries, place financial reports under the “Finance” folder and marketing assets under “Marketing.” Within SharePoint, you can create sites for “HR Policies”, “IT Resources”, “Product Documentation” and so on. When organizations design a logical information architecture in this manner, it enables Copilot for Microsoft 365 to infer relationships and relevance.

Consolidate multiple versions
Wherever feasible, retain only the final version of documents, presentations and so on.

You can also find old iterations of files and consolidate to only retain the most current version. The final version should clearly indicate it’s the latest. Eliminating redundant drafts and outdated versions reduces confusion and contradictions for Copilot for Microsoft 365.

Standardize file names
Make extensive use of labels, hashtags, and metadata tags on all documents, emails and pages to describe characteristics. For example, label customer support tickets with #refund, #payment-issue, or other issue tags.

You can also add product attributes like model number, market, and manufacturing year as meta datatags on images and specification sheets. Thorough labeling and tagging allows Copilot for Microsoft 365 to rapidly categorize, search and recommend content.

Promote data hygiene habits
Implement organizational training and change management to promote good data hygiene habits among employees.

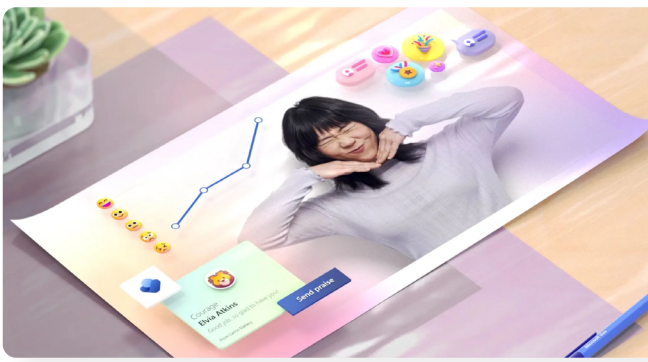
You should also provide guidelines on effectively naming files, tagging content, retaining up-to-date documents, deleting old emails and content, and other practices.

Consider gamification by recognizing top contributors to data hygiene. Organizations should also monitor data usage consent.

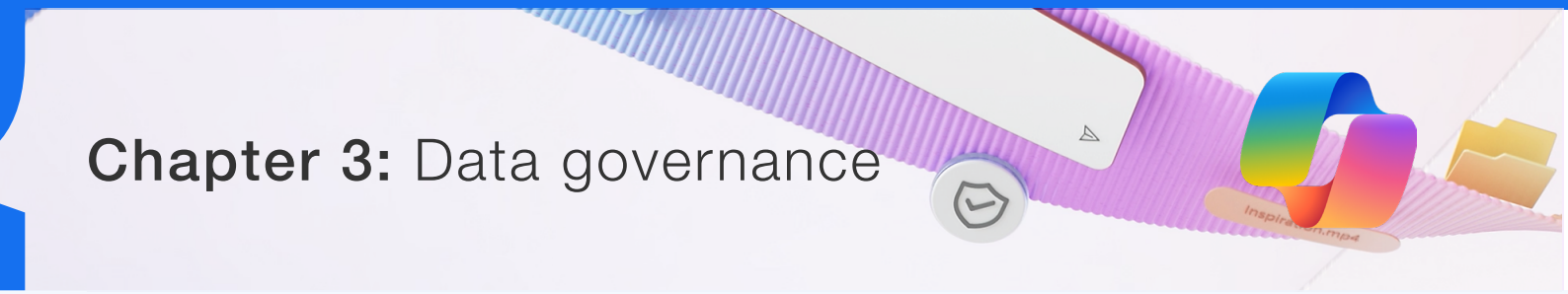
If any data sets include personal information, make sure your employees provide proper consent for use in Copilot for Microsoft 365.

Build data quality expectations into employee goal setting and reviews.

Organizations that establish a culture focused on maintaining clean, well-organized data can potentially maximize Copilot for Microsoft 365’s effectiveness.



Chapter 3: Data governance



Best practices

Assign a data steward to oversee preparation and continue maintaining quality
Organizations have sensitive information under their control which include financial data, proprietary data, credit card numbers, health records or social security numbers. As such, they should consider designating an experienced data governance expert or a team of governance experts as the official data steward for Microsoft 365. This person should be responsible for auditing data, establishing access rules, training users on data hygiene, while also continuously monitoring how Microsoft 365 and Copilot for Microsoft 365 utilize organizational data.

Having an accountable data steward helps ingrain excellent data habits and promotes accountability across the AI lifecycle. To help protect their sensitive data and reduce the risk from oversharing, organizations must prevent their users from inappropriately sharing sensitive data with people who shouldn't have it. They can accomplish this goal by implementing sensitivity labels and data loss protection (DLP) policies.

Document your data policies and practices related to Microsoft 365 and Copilot for Microsoft 365 utilization

As a best practice, organizations should formally outline their data management policies, access rules, use cases, and procedures related to data security and governance in Microsoft 365.

As previously stated, the powerful security tools within the Microsoft 365 and Azure ecosystems can help organizations tighten permissions and implement "just enough access." The policies and settings that administrators define in these tools are used not only by Microsoft 365 to prevent data oversharing, but also by Copilot for Microsoft 365.

Organizations that don't document their data governance policies should consider doing so prior to implementing Copilot for Microsoft 365. Drafting a comprehensive data governance policy should codify rules for:

- Restricted data
- Anonymization procedures
- Stewardship roles
- Employee training requirements
- Access authorization procedures
- Monitoring practices
- Other enforceable policies

An organization should share its data governance policy across the entire company and regularly update it. For example, it can create a data governance policy that defines the confidential data that's restricted from user access, the requirements for anonymous protection of certain datasets and the designation of a data governance expert or team to continually oversee its Microsoft 365 data practices.

Formalizing governance requirements helps create accountability across an organization.

Robust governance is crucial to ensure that both Microsoft 365 and Copilot for Microsoft 365 comply with legal and ethical data standards. As a best practice, organizations should appoint cross-functional data, security and compliance teams to enact data restrictions, anonymization, stewardship, policies and training.

Even though initial audits, access restrictions and governance policies are crucial when first deploying Microsoft 365 and Copilot for Microsoft 365, companies should view data governance as an iterative, continuous process. Why? Because data assets and usage patterns inevitably evolve over time. For example:

- **Organizations add new data repositories as business needs change.** New repositories require auditing and proper access controls need to be put in place.
- **Users and permissions change.** In business, change is a constant occurrence, especially as employees come and go. For example, new employees join or existing employees change roles. Administrators should grant/revoke access accordingly.
- **Regulations and compliance requirements change.** Data policies must reflect any new restrictions.

To keep pace, organizations should perform regular reviews and updates, such as:

- Monthly audits of new data sources that can require access changes
- Quarterly scans of permissions and external sharing to identify any new overexposure
- Update annual policy reviews based on new regulations and refresh employee training

Appointing a data governance expert or governance team to oversee this continuous process helps establish it as an evolving set of data policies and access controls. This process also enables Microsoft 365 and Copilot for Microsoft 365 governance to adapt to changes over time.

Chapter 4
Security

To prevent oversharing, organizations should consider implementing the following best practices:

Conduct an access review for sites, documents, emails and other content
Identify any overexposed assets and have data owners create inventory for SharePoint sites, document libraries, email mailboxes and other data assets.

You should also identify areas where user permissions are broader than required. For example, an “HR Benefits” SharePoint site that’s visible to all employees instead of just the HR team.

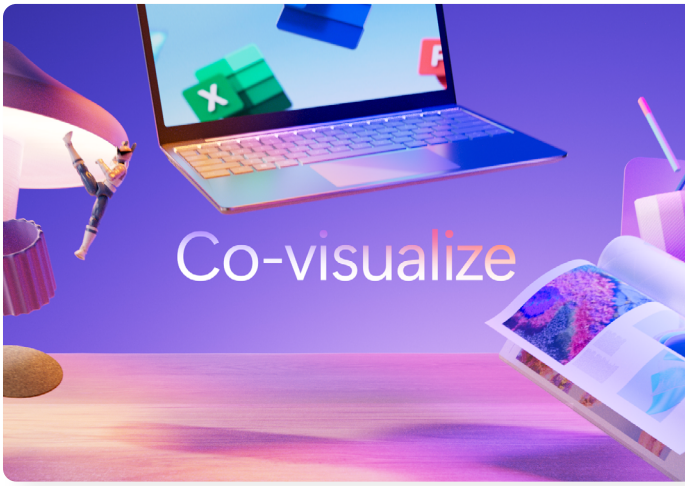
Tighten permissions on overexposed assets so only authorized users have access
Using the example in the previous item, restrict the “HR Benefits” site access to only HR department members. Similarly, limit confidential product roadmap documents to relevant product managers only. Configure external sharing and access expiration on emails and documents to limit exposure.

Validate that restricting access doesn’t impede any users’ ability to do their jobs
Survey and interview users of restricted assets to confirm they still have access to all necessary information for their role. For example, ensure Sales can still access client contact information and project specs even if the company restricted HR data.

Test search functionality to confirm users can only access information relevant to their roles
Perform searches on the sampling of documents, sites and emails as different internal roles.

Confirm if the finance staff can’t access HR data.

Validate cross-department teams retain access to shared project resources. Tuning permissions can be an iterative process.



Name	Description	License
Microsoft Purview Information Protection	**Classify and optionally encrypt documents and emails based on sensitivity. You can create policies to restrict access to only authorized users. For example, you can:** · Classify documents or emails containing employee salaries as "Highly Confidential" and restrict access only to the HR team. · Classify client data as "Confidential" and only allow sales reps assigned to that client to access it. · Classify financial reports as "Internal Only" and automatically encrypt them to prevent external sharing. · Classify executive communications as "Internal Eyes Only" and restrict access to members of the leadership team.	1. Business Premium (Plan 1) 2. Microsoft 365 E3 (Plan 1) 3. Microsoft 365 E5 (Plan 2) or as an add-on
Microsoft Purview sensitivity labels	**Classify and optionally encrypt documents and emails based on sensitivity. You can create policies to restrict access to only authorized users. For example, you can:** · Classify documents or emails containing employee salaries as "Highly Confidential" and restrict access only to the HR team. · Classify client data as "Confidential" and only allow sales reps assigned to that client to access it. · Classify financial reports as "Internal Only" and automatically encrypt them to prevent external sharing. · Classify executive communications as "Internal Eyes Only" and restrict access to members of the leadership team.	1. Business Premium (Manual Label) 2. Microsoft 365 E3 (Manual Label) 3. Office 365 E3 (Manual Label) 4. Microsoft 365 E5 (Automatic Label) 5. Office 365 E5 (Automatic Label) or as an add-on
Microsoft Entra conditional access policies	**Grant or restrict access to Microsoft 365 information and services, including SharePoint, based on conditions like user location, device or network. These policies are useful for limiting access when the system detects risks or user credentials become compromised. For example, you can:** · Require multifactor authentication to access SharePoint sites containing financial data when connecting remotely. · Block external sharing of sites containing internal presentations unless users are connecting through managed devices on the corporate network. · Require managed devices to access sites containing proprietary source code. · Block access to sites containing press releases before public announcement date. · Block access or require step-up authentication with another factor in cases where the system detects impossible travel, which is often an indicator of credential theft.	1. Business Premium 2. Microsoft 365 E3 3. Microsoft 365 E5 or as an add-on
Microsoft Entra Privileged Identity	**Provide accessible admin access, enforce the principle of least privilege, and limit permanent standing privileges by only granting a user the permissions they need. For example you can:** · Grant privileged roles like SharePoint admin or global admin only for approved business hours to minimize standing access. · Require multifactor authentication and justification to activate privileged access to data or apps. · Limit privileged access like Billing Administrator to five hours per week maximum. · Require approval to activate Microsoft 365 Global Administrator role access.	Microsoft 365 E5 or as an add-on
SharePoint site access reviews	**Require and automate access reviews of site owners, members and access requests to revoke permissions that users don't need or no longer require. Access reviews ensure users only retain the access they need for their role. For example, you can:** · Automatically revoke permissions to HR or financial systems after 90 days unless reviewed and approved. · Require business justification each quarter for external user accounts to validate ongoing need for access. · Require quarterly reviews of user access and remove access for departed employees. · Enforce policy time limits to external user access for collaboration sites.	
Microsoft Graph connectors and plugins	**Limit access to connected external data using Microsoft Graph connectors or plugins. For example, you can:** · Define the access scope that users and groups require to access connected data providers. · Require user account-based service authentication for connected services and data used with Copilot for Microsoft 365 plugins. · Limit extended search capabilities to external content indexed through Microsoft Graph connectors to only users who should have access.	

Chapter 5
License management

Organizations should consider implementing the following best practices for managing their Copilot for Microsoft 365 licenses:

Review Copilot for Microsoft 365 usage data and trends frequently to optimize the number of licenses
Microsoft 365 usage reports show how people in your organization are using Microsoft 365 services. Run usage reports in the Microsoft 365 admin center to see which users are actively using Copilot for Microsoft 365 within their Office apps. Organizations should identify inactive assigned licenses they can revoke and allocate to other productive users.

Regularly review trends to right-size licenses. For example, if 10% of assigned Copilot for Microsoft 365 licenses show minimal usage, consider reassigning those licenses to high-potential candidates.

Remind users to use Copilot for Microsoft 365 to maximize value from licenses
Send regular tips on taking advantage of Copilot for Microsoft 365 in Office apps through email campaigns or internal promotions. Offer to reassign unused licenses if adoption is low. For example, an email newsletter can showcase Copilot for Microsoft 365 use cases and productivity gains to spur adoption. Doing so maximizes the value derived from assigned licenses.

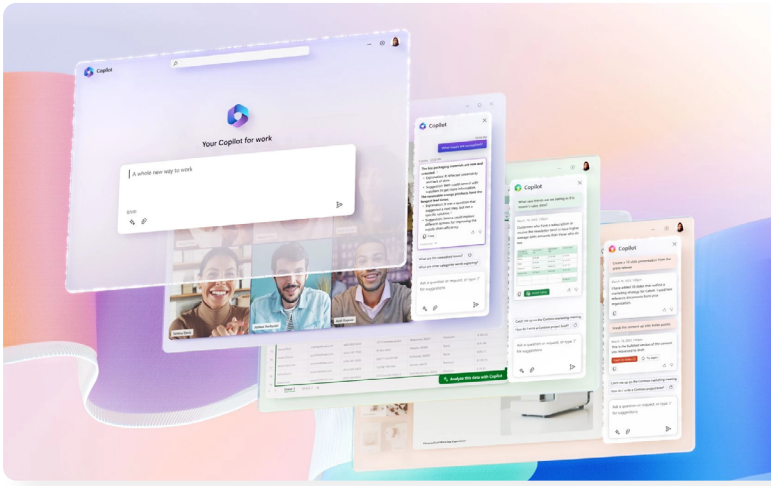
Administrators should also complement their Copilot for Microsoft 365 licensing rollout with training programs that teach employees how to optimize Copilot for Microsoft 365 features.

You can also garner executive sponsorship to encourage adoption and send regular communications highlighting Copilot for Microsoft 365's capabilities.

Evangelizing the use of Copilot for Microsoft 365 is key to driving adoption and realizing ROI from your AI investments.

Monitor adoption and usage of Copilot for Microsoft 365 licenses
Monitor adoption and usage of Copilot for Microsoft 365 licenses over time through auditing tools like Microsoft 365 usage analytics. Doing so helps ensure that employees use Copilot for Microsoft 365 capabilities that are in line with organizational policies and in compliance with Microsoft's license terms.

Administrators should proactively adjust assignments if usage is lower than expected. Once administrators assign Copilot for Microsoft 365 licenses, they should configure appropriate policies and permissions around usage. For example, restricting external sharing of Copilot for Microsoft 365 outputs, limiting the number of monthly interactions for specific users, disabling certain Copilot for Microsoft 365 capabilities as needed and implementing appropriate security controls. Thoughtful policy configuration further optimizes Copilot for Microsoft 365's value.



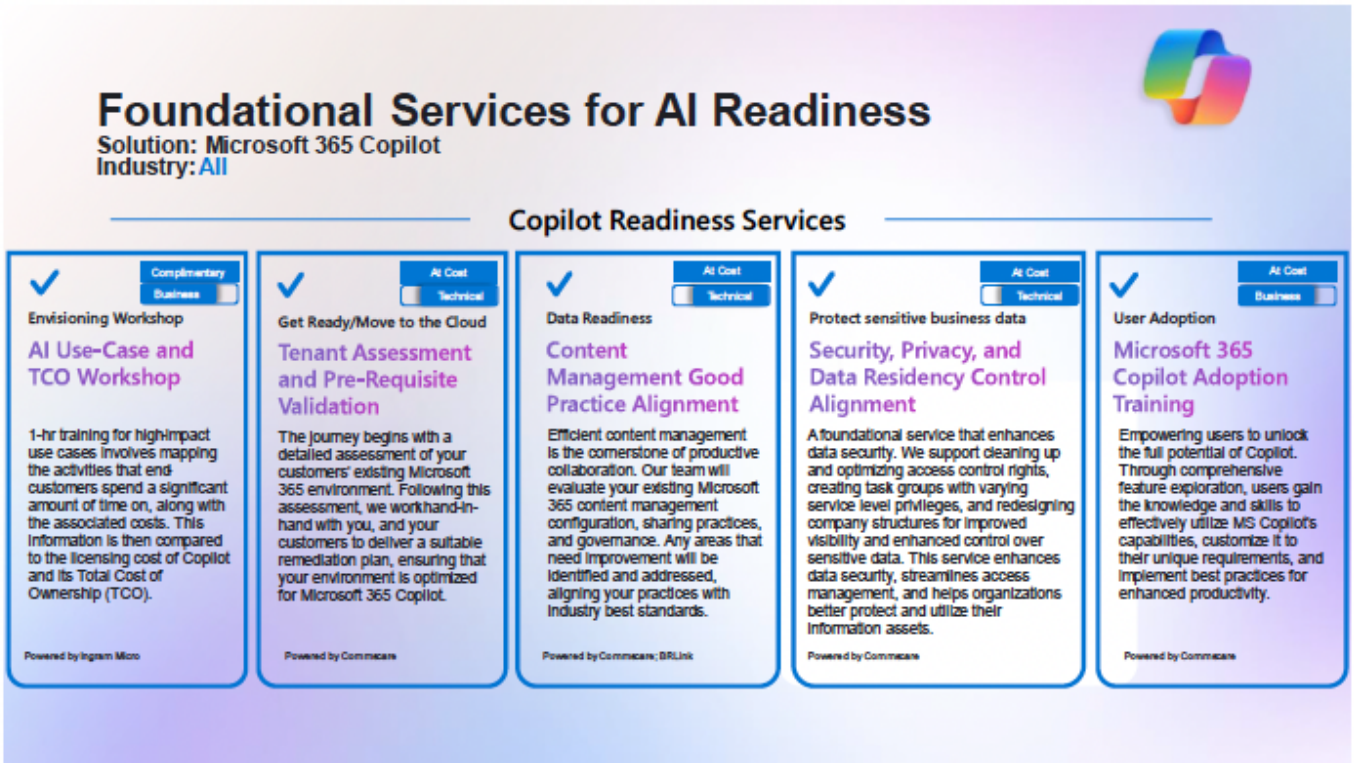
Chapter 6
How Ingram Micro can help

Ingram Micro is dedicated to assisting partners through this exciting AI journey. Microsoft 365 Copilot is the first generally available AI service, but there will be more exciting services being launched.

Partnering with Ingram Micro means having a reliable support system and access to top-notch training resources. We're committed to empowering you and your team with the skills needed to thrive in today's fast-paced environment.

In addition, Ingram Micro offers extensive go-to-market support and resources to help partners successfully monetize your cloud business. This includes Ingram Micro's established foundational services for AI readiness that can be delivered on behalf of the partner, or it can be trained by the trainer. These readiness pillars assist the partners in adhering to best practices throughout the adoption of AI services like Microsoft 365 Copilot.

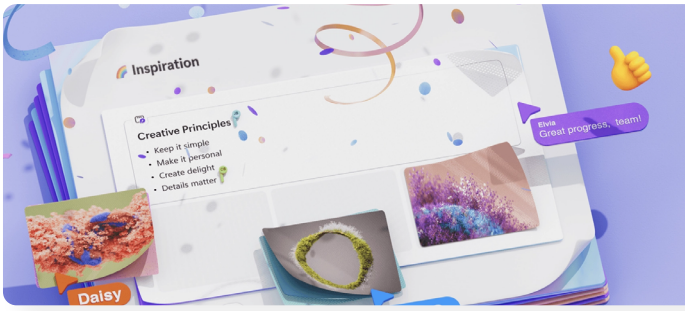
Please reach out to your Ingram Micro representative if you have questions or if you're interested in engaging with any of the below services.



Chapter 7
Summary

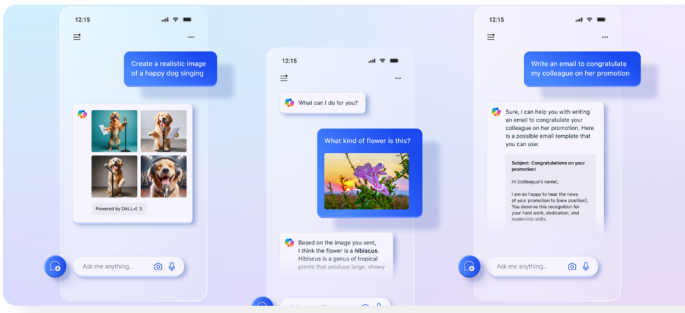
AI is transforming the way businesses operate, innovate and compete in the digital era. It can help organizations improve productivity, efficiency, customer satisfaction and revenue growth by automating tasks, enhancing decision-making and enabling new capabilities.

However, deploying and managing AI solutions can be challenging, especially for SMBs that either lack the resources and expertise to leverage this technology or simply don't have the time resource available. That's why Copilot for Microsoft 365 is designed to make AI accessible and affordable for SMBs.



Copilot for Microsoft 365 is providing a comprehensive and integrated suite of cloud-based services that empower SMBs to create, deploy and manage AI solutions with ease.

It also has a unique offering that combines the power of Microsoft Azure, Microsoft 365 and Microsoft Dynamics 365 to deliver a unified and consistent AI experience across various scenarios and domains.



Copilot for Microsoft 365 enables SMBs to:
- Build and customize AI models using no-code or low-code tools, such as Power Platform and Azure Cognitive Services, that simplify and accelerate the development process.
- Integrate AI into their existing workflows and applications, such as Outlook, Teams, SharePoint and Excel, to enhance collaboration, communication and data analysis.
- Use Dynamics 365 and Azure Synapse Analytics to leverage AI to gain insights and optimize outcomes across various business functions, such as marketing, sales, customer service, finance and operations.
- Manage and monitor AI solutions using a centralized dashboard that provides visibility, control and security over AI assets and activities.

With Copilot for Microsoft 365, SMBs can take advantage of the benefits of AI without the complexity and cost of traditional AI solutions. Copilot for Microsoft 365 helps SMBs unlock the full potential of AI and drive digital transformation in their organizations.