|  |
| --- |
| Copilot Agent governance template |

Table of Contents

[1 Purpose 3](#_Toc221013945)

[1.1 Intended audience 3](#_Toc221013946)

[1.2 How to use this document 3](#_Toc221013947)

[2 Zone & Environment Strategy 4](#_Toc221013948)

[2.1 Zone strategy 4](#_Toc221013949)

[2.1.1 Checklist 4](#_Toc221013950)

[2.1.2 Zone definition table 4](#_Toc221013951)

[2.2 Default Environment strategy 5](#_Toc221013952)

[2.2.1 Checklist 5](#_Toc221013953)

[2.2.2 Default Environment definition table 5](#_Toc221013954)

[2.3 Environment strategy 6](#_Toc221013955)

[2.3.1 Checklist 6](#_Toc221013956)

[2.3.2 Environment definition table 6](#_Toc221013957)

[2.4 Environment routing 7](#_Toc221013958)

[2.4.1 Checklist 7](#_Toc221013959)

[2.4.2 Environment routing definition table 8](#_Toc221013960)

[3 Tenant-level governance 9](#_Toc221013961)

[3.1 Checklist 9](#_Toc221013962)

[3.2 Tenant settings definition table 9](#_Toc221013963)

[4 Environment-level governance 10](#_Toc221013964)

[4.1 Checklist 10](#_Toc221013965)

[4.2 Environment settings definition table 11](#_Toc221013966)

[5 Data policies 14](#_Toc221013967)

[5.1 Checklist 15](#_Toc221013968)

[5.2 Data policies definition table 15](#_Toc221013969)

1. Purpose

Copilot Agents introduce a new way of building AI-powered experiences across Power Platform and Microsoft 365. Depending on their purpose, agents can range from personal experimentation to business-critical solutions that access data, trigger actions, and interact with users at scale.

This document provides a structured governance template for Copilot Agents. It helps organizations design and document governance decisions across environment strategy, tenant-level controls, data policies, and lifecycle considerations in a consistent and repeatable way.

The goal is not to prescribe a single “correct” setup, but to ensure that all relevant governance topics are explicitly considered, discussed, and documented.

This document reflects governance considerations and platform capabilities at the time of writing. Product features, licensing models, and enforcement options may change over time. Always validate governance decisions and configurations against current Microsoft documentation and guidance.

* 1. Intended audience

This document is intended for:

* Power Platform and Microsoft 365 architects
* Platform administrators and governance leads
* Technical consultants designing or implementing Copilot Agent governance

It assumes familiarity with Power Platform concepts such as environments, DLP policies, and tenant settings.

* 1. How to use this document

This document combines checklists and governance decision tables to support structured Copilot Agent governance design and documentation.

* **Checklists** are used to ensure that all relevant governance topics are explicitly discussed. They help drive conversations during workshops or design sessions and reduce the risk of blind spots.
* **Decision tables** capture the outcome of those discussions. They document agreed decisions, enforcement scope, and rationale, and serve as a reference for implementation, operational governance, audits and future reviews

The document can be used as:

* A design template during governance workshops
* A governance documentation artifact
* A living document that evolves as Copilot adoption matures

1. Zone & Environment Strategy

Copilot Agents can vary significantly in purpose, complexity, and risk. Some agents are created for personal productivity or experimentation, while others support team processes or business-critical workloads.

To govern these differences effectively, this document uses a zone-based environment strategy. The strategy separates Copilot Agents into logical zones based on intended use, risk profile, and maturity, and maps those zones to appropriate environments and governance controls.

This approach enables consistent governance while still allowing flexibility for experimentation, adoption, and scale.

* 1. Zone strategy

The zone strategy defines logical groupings for Copilot Agents based on their intended usage and risk level.

Zones are not technical constructs but governance classifications that help determine:

* Where agents are allowed to be created and hosted
* Which environments are appropriate
* What level of governance and controls are required

Each zone represents a different balance between flexibility and control and serves as the foundation for environment and governance decisions in the sections that follow.

* + 1. Checklist
* Are Copilot Agent zones clearly defined (e.g. Personal, Team, Advanced)?
* Is an ownership model defined for each Copilot Agent zone?
* Are the allowed environment types per zone agreed (e.g. Personal, Dev, Test, Prod)?
* Is usage of the Default environment explicitly defined per zone? See *2.2 Default Environment strategy*
* Are ALM requirements defined per zone?
* Is cost ownership defined per zone?
  + 1. Zone definition table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Zone** | **Intended use** | **Who can create agents** | **Environment model** | **Allowed maturity** | **Notes** |
| Zone 1 – Personal Agents | Individual productivity & learning | All licensed users | Personal developer environment | Experimental | No business-critical data |
| Zone 2 – Team Agents | Team or department solutions | Approved makers | Dedicated Dev / Test / Prod | Business internal | Owned by team |
| Zone 3 – Advanced Agents | Business-critical / external | IT / Pro dev teams | Dedicated Dev / Test / Prod | Production-grade | Security review required |

* 1. Default Environment strategy

The Default environment exists in every Power Platform tenant and is available to all licensed users by design. Because of this, it often becomes the unintended starting point for building Copilot Agents, especially during early experimentation or adoption phases.

From a governance perspective, this introduces risks related to ownership, data access, and lifecycle management. These risks are amplified for Copilot Agents, as agents may access data, trigger actions, and interact with users across Microsoft 365.

As a general principle, the Default environment should not be treated as a long-term home for Copilot Agents. Instead, its usage should be explicitly defined, restricted, and documented as part of the overall zone and environment strategy.

* + 1. Checklist
* Is Copilot Studio creation allowed in the Default environment?
* Is the Default environment read-only for Copilot Agents (publishing blocked)?
* Are data policies applied to the Default environment?
* Is environment routing enabled to avoid long-term usage of the Default environment?
  + 1. Default Environment definition table

|  |  |  |
| --- | --- | --- |
| **Topic** | **Decision** | **Rationale** |
| Agent creation in Default environment | Restricted | Prevent unmanaged agents. |
| Agent publishing from Default environment |  |  |
| DLP applied to Default environment |  |  |
| Long-term agent hosting in Default environment |  |  |

* 1. Environment strategy

The environment strategy defines how Power Platform environments are structured, classified, and governed based on the previously defined zone strategy.

While zones describe intent and risk, environments provide the technical boundaries in which Copilot Agents are built, tested, and operated. This section documents how different environment types are used, how they map to zones, and how governance expectations vary between them.

The environment strategy ensures that Copilot Agents are hosted in environments that match their purpose, maturity, and risk profile, and that governance controls can be applied consistently and at scale.

* + 1. Checklist
* Are environment types clearly defined and mapped to zones?
* Is there a defined model for structuring environments (e.g. per department, per project, per topic, or hybrid)?
* Is there a clear separation between development, test, and production environments?
* Is the intended purpose of each environment type documented?
* Are environment groups used where consistent governance across environments is required?
* Are managed environments used for business-critical or production workloads?
* Are naming conventions defined for environments (including zone, purpose, and workload)?
* Is ownership clearly defined per environment (business owner and platform owner)?
* Are lifecycle rules defined for environments (creation, review, and cleanup)?
* Is there a process for identifying and retiring unused or non-compliant environments?
* Are environment monitoring and reporting expectations defined (e.g., insights, usage metrics, audit events)?
* Are environment ALM and release controls defined (e.g., pipelines, solution lifecycles)?
* Is cost ownership defined per environment (team, department, or central IT)?
* Is there an agreed model for who is responsible for Copilot Agent-related consumption in each environment?
  + 1. Environment definition table

This table documents which Power Platform environments are used, how they are classified, and how they map to the zone strategy.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Environment name** | **Environment type** | **Zone** | **Managed** | **Environment group** |
| PP-Dev-Marketing | Sandbox | Zone 2 – Team Agents | No | - |
| PP-Test-Marketing | Sandbox | Zone 2 – Team Agents | No | - |
| PP-Prod-Marketing | Production | Zone 2 – Team Agents | Yes | - |
|  |  |  |  |  |
|  |  |  |  |  |

This table captures governance decisions and operational guidelines that apply across environments.

|  |  |  |
| --- | --- | --- |
| **Topic** | **Decision** | **Applies to** |
| Environment structuring model | e.g. per department, per project, per topic, or hybrid | All environments |
| Naming convention | Include zone, purpose, and workload | All environments |
| Ownership model | Business owner and platform owner | Per environment |
| Environment creation criteria | When and by whom environments may be created | New environments |
| Lifecycle review frequency | e.g. quarterly / bi-annual | All environments |
| Cleanup and retirement rules | Criteria for decommissioning | Unused environments |
| Exception handling | How deviations are approved and documented | Specific cases |
| Cost ownership model |  | All environments |
| ALM and deployment model |  |  |

* 1. Environment routing

Environment routing makes sure makers are sent to the right place when they start building an app, flow, or Copilot Agent. Copilot Agents are often created during experimentation or rapid iteration. Without routing, this typically leads to:

* Agents being created in the Default environment
* Unclear ownership and lifecycle
* Increased governance and security risk

Environment routing does not replace environment design or governance. It supports early-stage creation and experimentation by steering makers toward an appropriate starting environment.

* + 1. Checklist
* Is environment routing enabled to reduce accidental usage of the Default environment?
* Are developer environments defined and available for routed makers?
* Is routing applied to all users or only specific user groups?
* Is environment routing enabled for Copilot Studio?
* Is environment routing enabled for Power Apps, Power Automate cloud flows and Power Automate Desktop flows where applicable?
* Is routing behavior documented and communicated to makers?
  + 1. Environment routing definition table

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Applies to** | **Decision** | **Notes** |
| Environment routing enabled | All users / Specific users | Yes / No |  |
| Target developer environment | Routed users |  | Developer environment name |
| Copilot Studio routing enabled | Routed users | Yes / No |  |
| Power Apps routing enabled | Routed users | Yes / No |  |
| Power Automate (cloud flows) routing enabled | Routed users | Yes / No |  |
| Power Automate Desktop routing enabled | Routed users | Yes / No |  |

1. Tenant-level governance

Tenant-level settings in the Power Platform Admin Center define the global guardrails for Copilot Studio. These settings apply across all environments and zones.

The purpose of this chapter is to document:

* Which Copilot Studio capabilities are enabled tenant-wide
* Who is allowed to create, publish, and share Copilot Agents
* Which advanced features are allowed or restricted by default
  1. Checklist
* Is Copilot Agent authoring restricted to approved users or roles?
* Is publishing of AI-enabled Copilot Agents restricted at tenant level?
* Are advanced agent capabilities (for example desktop flows and hosted browser) allowed at tenant level?
* Is Copilot assistance for makers or components in other Power Platform tools enabled?
* Are non-Microsoft AI providers (other large language models) allowed?
* Is Copilot telemetry and feedback allowed?
* Is there a defined owner responsible for monitoring and managing Copilot Agent-related consumption at tenant level?
  1. Tenant settings definition table

|  |  |  |
| --- | --- | --- |
| **Setting** | **Description** | **Decision** |
| Copilot Studio authors | Controls who can create and edit Copilot Agents |  |
| Publish bots with AI features | Allows publishing agents that use generative AI |  |
| Desktop flow actions in DLP | Allows agents to trigger desktop flows |  |
| Hosted browser in computer use | Enables hosted browser for agent-driven interactions |  |
| Basic Copilot feedback | Sends basic usage and reliability data to Microsoft |  |
| Additional Copilot feedback | Sends extended diagnostics and telemetry |  |
| Copilot help assistance in Power Automate via Bing | Provides AI-assisted help and suggestions in Power Automate |  |
| Copilot in Power Apps (Preview) | Enables AI assistance for app creation and editing |  |
| AI providers for other large language models (M365 Admin center) | Allows Copilot to use non-Microsoft LLM providers |  |

1. Environment-level governance

Copilot Agent governance at environment level can be enforced in different ways. Some settings apply directly to an environment, while others are enforced through environment groups or managed environments.

A **standard environment** is a Power Platform environment used to host apps, flows, and Copilot Agents with governance configured directly on the environment itself.

* Settings apply only to the individual environment
* Suitable when governance requirements differ per environment
* Requires manual configuration and maintenance per environment

**Managed environments** extend a standard environment with additional governance, monitoring, and control capabilities.

* Enable advanced controls such as insights, sharing limits, and usage monitoring
* Applied per environment, typically for business-critical or production workloads
* Can be combined with environment groups for consistent policy enforcement
* Managed environments require additional Power Platform / Copilot licensing

**Environment groups** allow administrators to enforce governance settings consistently across multiple environments.

* Centralized application of governance settings across multiple environments
* Commonly used for DLP policies and environment routing
* Helps reduce configuration drift between similar environments
  1. Checklist
* Is access to and storage of Copilot Agent conversation transcripts defined per environment?
* Are maker and end-user credential options for Copilot Agents defined per environment type?
* Are AI-powered Copilot features for app makers enabled or restricted per environment?
* Is the use of the Copilot answer component in canvas apps controlled per environment?
* Is the use of Power Apps component framework (PCF) code components controlled per environment?
* Is sharing of Copilot Studio agent data with Viva Insights explicitly controlled at environment level?
* Is the use of preview and experimental AI models for makers controlled per environment?
* Is the use of external AI models in Copilot Studio controlled per environment?
* Is the AI prompts feature in Power Platform and Copilot Studio enabled or restricted per environment?
* Is authentication for Copilot Studio agents enforced per environment?
* Is channel access for published Copilot Studio agents controlled per env and aligned with data policies?
* Is sharing of Copilot Studio agents (editor and viewer permissions) controlled per environment?
* Are Generative AI settings (cross-region data movement and Bing Search grounding) explicitly controlled?
* Is Copilot Studio agent traffic protected using Global Secure Access (GSA)?
* Is the use of Computer Use capabilities in Copilot Studio (local automation and Cloud PC) explicitly controlled and approved?
* Is the use of AI insight cards in model-driven apps controlled per environment?
* Is the use of natural language search and AI-generated visualizations in model-driven app views controlled per environment?
* Is the AI-powered chat experience for analyzing data in canvas, model-driven, and Dynamics 365 Sales apps controlled per environment?
  1. Environment settings definition table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Setting** | **Microsoft Learn** | **Enforcement\*** | **Environment scope \*\*** | **Decision** |
| Transcript access for agent owners and editors | [settings-features#accessing-transcripts-from-conversations-in-copilot-studio-agents](https://learn.microsoft.com/en-us/power-platform/admin/settings-features#accessing-transcripts-from-conversations-in-copilot-studio-agents) | Environment / Environment group |  |  |
| Conversation transcript storage in Dataverse | [settings-features#accessing-transcripts-from-conversations-in-copilot-studio-agents](https://learn.microsoft.com/en-us/power-platform/admin/settings-features#accessing-transcripts-from-conversations-in-copilot-studio-agents) | Environment / Environment group |  |  |
| Control maker credential options |  | Environment / Environment group |  |  |
| AI-powered Copilot features for app makers (preview) | [settings-features#copilot-preview](https://learn.microsoft.com/en-us/power-platform/admin/settings-features#copilot-preview) | Environment / Environment group |  |  |
| Allow canvas editors to insert the Copilot answer component, which allows users to receive an AI-powered answer to a predefined data query. | [settings-features#copilot-preview](https://learn.microsoft.com/en-us/power-platform/admin/settings-features#copilot-preview) | Environment |  |  |
| Power Apps component framework for canvas apps | [settings-features#power-apps-component-framework-for-canvas-apps](https://learn.microsoft.com/en-us/power-platform/admin/settings-features#power-apps-component-framework-for-canvas-apps) | Environment / Environment group |  |  |
| Share Copilot Studio agent data with Viva Insights | [settings-features#sharing-copilot-studio-agent-data-with-viva-insights](https://learn.microsoft.com/en-us/power-platform/admin/settings-features#sharing-copilot-studio-agent-data-with-viva-insights) | Environment / Environment group |  |  |
| Cross-geo sharing of aggregated Copilot Studio analytics data | [settings-features#sharing-copilot-studio-agent-data-with-viva-insights](https://learn.microsoft.com/en-us/power-platform/admin/settings-features#sharing-copilot-studio-agent-data-with-viva-insights) | Environment / Environment group |  |  |
| Preview and experimental AI models | [settings-features#preview-and-experimental-ai-models-formerly-ai-builder](https://learn.microsoft.com/en-us/power-platform/admin/settings-features#preview-and-experimental-ai-models-formerly-ai-builder) | Environment / Environment group |  |  |
| Enable external AI models | [settings-features#external-models](https://learn.microsoft.com/en-us/power-platform/admin/settings-features#external-models) | Environment / Environment group |  |  |
| AI prompts | [settings-features#ai-prompts](https://learn.microsoft.com/en-us/power-platform/admin/settings-features#ai-prompts) | Environment / Environment group |  |  |
| Natural language grid and view search | [settings-features#natural-language-grid-and-view-search-preview](https://learn.microsoft.com/en-us/power-platform/admin/settings-features#natural-language-grid-and-view-search-preview) | Environment |  |  |
| AI-generated charts for views | [settings-features#natural-language-grid-and-view-search-preview](https://learn.microsoft.com/en-us/power-platform/admin/settings-features#natural-language-grid-and-view-search-preview) | Environment |  |  |
| Apply AI-generated chart styling | [settings-features#natural-language-grid-and-view-search-preview](https://learn.microsoft.com/en-us/power-platform/admin/settings-features#natural-language-grid-and-view-search-preview) | Environment |  |  |
| AI insight cards | [settings-features#ai-insight-cards-preview](https://learn.microsoft.com/en-us/power-platform/admin/settings-features#ai-insight-cards-preview) | Environment |  |  |
| Allow users to analyze data using an AI-powered chat experience. | [settings-features#copilot-preview](https://learn.microsoft.com/en-us/power-platform/admin/settings-features#copilot-preview) | Environment |  |  |
| Computer Use feature in Copilot Studio |  | Environment group |  |  |
| Cloud PC for Computer Use (Windows 365 for Agents) |  | Environment group |  |  |
| Authentication for agents (No authentication or Authenticate w Microsoft/Authenticate manually) |  | Environment group |  |  |
| Channel access for published agents |  | Environment group |  | Teams + Microsoft 365 Copilot, Direct Line Channels, Facebook, Dynamic 365 for customer service, SharePoint, WhatsApp |
| Protect Copilot Studio agent traffic via Global Secure Access (GSA) |  | Environment group |  |  |
| Generative AI Settings - Move data across regions (Generative AI Settings) | [geographical-availability-copilot](https://learn.microsoft.com/en-us/power-platform/admin/geographical-availability-copilot) | Environment group |  |  |
| Generative AI Settings - Bing Search and grounding with Bing Search (Generative AI Settings) |  | Environment group |  |  |
| Sharing agents with Editor permissions | [managed-environment-sharing-limits#agent-sharing-rules](https://learn.microsoft.com/en-us/power-platform/admin/managed-environment-sharing-limits#agent-sharing-rules) | Environment group / Managed Environment |  | Disabled (no editor sharing allowed) |
| Sharing agents with viewer permissions | [managed-environment-sharing-limits#agent-sharing-rules](https://learn.microsoft.com/en-us/power-platform/admin/managed-environment-sharing-limits#agent-sharing-rules) | Environment group / Managed Environment |  | Enabled – sharing limited to individual users only, with a maximum number (5) of viewers defined |

\* Enforcement: Environment | Environment group | Managed environment  
\*\* Environment scope: the names of the environments or environment groups

1. Data policies

Copilot Agents are only as powerful and as risky as the data they can access. In Copilot Studio, data access is primarily controlled through Power Platform connectors, which define how agents retrieve, send, and act on information.

This chapter focuses exclusively on connectors that are relevant to Copilot Studio.

|  |  |  |
| --- | --- | --- |
| **Name** | **Type** | **Description** |
| Microsoft Copilot Studio | General | Block agent makers from publishing or running Copilot Agents. |
| Skills with Copilot Studio | General | Block agent makers from using skills in Copilot Studio agents. |
| Chat without Microsoft Entra ID authentication in Copilot Studio | General | Block agent makers from publishing agents that aren't configured for authentication. |
| Application Insights in Copilot Studio | General | Block agent makers from connecting agents with Application Insights. |
| Microsoft Teams + M365 Channel in Copilot Studio | Channel | Block agent makers from enabling or using the Teams channel. |
| Direct Line channels in Copilot Studio | Channel | Block agent makers from enabling or using Direct Line channel. For example, the Demo website, Custom website, Mobile app, and other Direct Line channels would be blocked. |
| Facebook channel in Copilot Studio | Channel | Block agent makers from enabling or using the Facebook channel. |
| Omnichannel in Copilot Studio | Channel | Block agent makers from enabling or using the Omnichannel channel. |
| SharePoint channel in Copilot Studio | Channel | Block agent makers from enabling or using the SharePoint channel. |
| WhatsApp channel in Copilot Studio | Channel | Block agent makers from enabling or using the WhatsApp channel. |
| Knowledge source with SharePoint and OneDrive in Copilot Studio | Knowledge | Block agent makers from publishing agents configured with SharePoint as a knowledge source. |
| Knowledge source with public websites and data in Copilot Studio | Knowledge | Block agent makers from publishing agents configured with public websites as a knowledge source. |
| Knowledge source with documents in Copilot Studio | Knowledge | Block agent makers from publishing agents configured with documents as a knowledge source. |

* 1. Checklist
* Have the existing Power Platform DLP policies been reviewed?
* Do current DLP policies already cover connectors used by Copilot Studio?
* Should Copilot Agent data access be governed by existing DLP policies or by dedicated Copilot-specific policies?
* Are connector rules aligned with the environment and zone strategy?
* Is there an approval process for enabling additional connectors for Power Platform / Copilot Agents?
  1. Data policies definition table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Policy name | Assigned environments (groups) | Business connectors \* | Non-business connectors \* | Blocked connectors \* | Notes |
| DLP – Personal Agents | Personal dev environments | Microsoft Copilot Studio, Skills with Copilot Studio,  Chat without Microsoft Entra ID authentication in Copilot Studio |  | All other Copilot Studio connectors | New policy to enable testing of agents on personal level. |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| DLP – Default Environment | Default environment | None | None | All Copilot Studio Connectors | Prevent usage and reuse of existing policy |

\* Connectors that host business-use data should be classified as Business, and connectors that host personal-use data should be classified as Non-Business. Any connectors that you want to keep from being used across one or more environments should be classified as Blocked.