WHAT IS SHAREPOINT GOVERNANCE FOR MICROSOFT COPILOT?

DEFINITION SharePoint governance for Microsoft Copilot is the process of controlling sensitive content, effective access, oversharing, ownership, lifecycle, and information architecture so AI operates across an appropriately governed Microsoft 365 information environment.

AI Makes Existing Access More Important

Copilot does not create the underlying SharePoint access model. It works with the permissions and content that already exist. Information that was difficult to locate manually can become significantly easier to discover, summarize, and use through AI-driven experiences. The governance question therefore becomes: does the access users already have accurately reflect the access they should have?

Start With Sensitive Data and Effective Access

ASP begins by identifying and classifying sensitive information across SharePoint content. Sensitive-data discovery alone, however, does not establish risk. ASP correlates sensitive content with effective access to determine how users, groups, external identities, inherited permissions, direct permissions, and sharing mechanisms create actual exposure. This allows organizations to prioritize remediation based on the combination of sensitive information and inappropriate access.

Remediate Oversharing Before Expanding AI

Microsoft guidance for establishing a secure and governed foundation for Copilot emphasizes oversharing, sensitive content, access risk, lifecycle management, and governance controls. ASP operationalizes those principles through controlled remediation while preserving approved business access. Organizations can also rationalize inactive, duplicate, obsolete, or poorly governed content before exposing a broader information estate to AI-enabled discovery.

Governance Must Continue After Readiness

Copilot readiness is not a one-time permissions cleanup. Sites and content continue to change, users gain access, groups evolve, ownership changes, and new sensitive information is created. ASP extends governance into workflow automation and ongoing monitoring so organizations can continuously evaluate sensitive-data exposure, access drift, lifecycle conditions, governance exceptions, and remediation progress.

ASP PERSPECTIVE The objective is not to prevent AI from accessing enterprise information. It is to ensure AI operates over information that is appropriately classified, appropriately accessible, actively governed, and continuously monitored.