ARTIFICIAL INTELLIGENCE | INTERMEDIATE | 3 DAYS

Microsoft 365 Copilot Administration, Security and Compliance

The tenant readiness work that has to happen before Copilot is switched on. Covers the oversharing problem, sensitivity labels and DLP with Microsoft Purview, search and access scoping, the Copilot Control System, and the audit trail your compliance team will eventually ask for.

Why Copilot Administration and Security?

Fix oversharing first

Copilot surfaces everything a user can already reach. Most tenants are not ready for that.

Evidence, not assurances

Leave able to produce the audit trail a regulator or internal auditor will accept.

Purview in practice

Labels, DLP and retention configured against Copilot specifically, not in the abstract.

Admin-centre fluency

Operate the Copilot Control System with confidence rather than clicking hopefully.

What you'll be able to do

- ✓ Assess tenant readiness and identify blockers before a Copilot rollout
- ✓ Diagnose and remediate oversharing across SharePoint, OneDrive and Teams
- ✓ Apply sensitivity labels and information protection so Copilot respects classification
- ✓ Configure data loss prevention policies covering Copilot interactions
- ✓ Scope search and access to limit what Copilot can reach
- ✓ Operate the Copilot Control System and admin centre controls day to day
- ✓ Produce audit, eDiscovery and compliance evidence for Copilot activity
- ✓ Plan licensing, phased deployment and ongoing operational review

Who this is for

- Microsoft 365 administrators and architects
- Security, compliance and information governance teams
- SharePoint and Teams administrators
- IT leadership accountable for a Copilot rollout

Curriculum

01 Tenant Readiness and Prerequisites

- What Copilot can access, and why that is a data governance question first
- Prerequisite services, licences and configuration
- Running a readiness assessment and scoring the gaps
- Building the remediation plan and sequencing it against the rollout date
- Stakeholder alignment: who owns which decision

02 The Oversharing Problem

- How permissions sprawl accumulates in SharePoint, OneDrive and Teams
- Discovering overshared sites, orphaned content and broad-access links
- Site access reviews and permission remediation at scale
- Sharing policies, link defaults and expiry settings
- **Hands-on:** identify and remediate oversharing in a sample tenant

03 Sensitivity Labels and Information Protection

- Designing a label taxonomy that people will actually apply
- Automatic and recommended labelling with trainable classifiers
- How labels change what Copilot can use and what it produces
- Label inheritance in Copilot-generated content
- **Hands-on:** configure labelling and verify Copilot behaviour against it

04 Data Loss Prevention and Copilot Interactions

- DLP policy design covering prompts, responses and generated content
- Protecting regulated data categories and sensitive information types
- Policy tips, blocking and user education at the point of use
- Testing policies without disrupting legitimate work
- **Hands-on:** build and validate a DLP policy scoped to Copilot

05 Search, Access Control and Scoping

- Restricting search scope to limit what Copilot can retrieve
- Site-level and container-level access restrictions
- Conditional access and device compliance implications
- Guest access, external sharing and third-party content
- Balancing restriction against genuine business usefulness

06 Copilot Control System and Admin Operations

- Navigating Copilot administration in the Microsoft 365 admin centre
- Managing which Copilot experiences and agents are available
- Approving, restricting and inventorying agents in the tenant
- Unified data risk reporting and drilldowns
- Establishing an operational review cadence

07 Audit, eDiscovery and Compliance Evidence

- What Copilot activity is logged and where it lands
- Audit search and building a defensible evidence trail
- eDiscovery and legal hold covering Copilot interactions
- Retention and deletion policy for prompts and responses
- Communication compliance for AI interactions

08 Deployment, Licensing and Ongoing Operations

- Licence assignment strategy and phased user onboarding
- Pilot design, success criteria and go or no-go gates
- Support model, escalation paths and known-issue handling
- Monitoring for policy drift and configuration decay
- **Hands-on:** build a deployment and governance runbook