Copilot Readiness Audit

Preparing SharePoint & Dataverse for AI Integration

Microsoft 365 Copilot is only as powerful as the data it can access. Without proper governance, AI can expose sensitive information through "Oversharing." Use this checklist to ensure your tenant is secure and optimized for AI.

Phase 1: Data Governance & Hygiene

- [ ] **Oversharing Audit**
  Review 'Everyone except external users' and 'All Users' permissions on SharePoint sites to prevent AI from surfacing private data.
- [ ] **Sensitivity Label Implementation**
  Deploy Purview Sensitivity Labels (Confidential, Highly Confidential) to restrict Copilot from processing specific document types.
- [ ] **Just-In-Time Access Review**
  Perform an Access Review on high-risk sites (HR/Legal) to ensure only active project members have permissions.

Phase 2: Content Optimization

- [ ] **Semantic Indexing Prep**
  Ensure high-value documents have descriptive titles and metadata. Copilot relies on modern search indexing for accuracy.
- [ ] **Dataverse Virtual Table Review**
  Verify that Dataverse virtual tables are correctly mapped so Copilot for Sales or Service can surface legacy CRM data.

AI SECURITY NOTE:

Copilot respects the permissions of the current user. If a user has "Read" access to a sensitive HR folder they shouldn't have, Copilot WILL surface that data in chat. Security at the source is mandatory.