

Adding AI integrations into your work environment.

Managing the integration of AI connectors with Microsoft 365 environments requires a clear boundary between the efficiency gains and the potential for data leakage or corruption.

Below is a list of risk and disclaimer designed for an IT managed services context.

Risks of AI Integration with M365 & SharePoint

- **Data Hallucination & Accuracy:** AI may generate confident but factually incorrect responses based on SharePoint data. If used for decision-making or client communication, this can lead to professional liability.
- **Permissions "Bleed":** AI tools often bypass the "security by obscurity" that humans rely on. If a SharePoint site has loose permissions (e.g., "Internal Everyone"), the AI will surface sensitive data (payroll, HR files) to users who shouldn't see it but technically have access.
- **Data Sovereignty & Privacy:** Depending on the connector used, data may be processed outside of your specific M365 geographic region. This can lead to breaches of industry-specific compliance (e.g., HIPAA, GDPR, or Australian Privacy Principles).
- **Prompt Injection:** Unauthorized or malicious prompts can "trick" the AI into bypassing safety filters or revealing restricted information stored within the indexed emails and sites.
- **Lack of Point-in-Time Recovery:** Standard M365 sync settings are not a substitute for a dedicated backup. If an AI tool is granted "Write" access and erroneously modifies or deletes large batches of files/emails, these changes may sync across the environment instantly.

The Backup Warning

CRITICAL: Standard Microsoft 365 "Native Protection" is insufficient when deploying AI connectors. AI tools interact with data at scale and speed. In the event of an AI-driven "logic error" resulting in mass data corruption, over-writing of files, or accidental deletion, Microsoft's standard retention policies may not allow for a granular "undo" of the damage.

A third-party, point-in-time backup solution is mandatory to ensure data can be rolled back to a state prior to the AI integration or any specific AI-led incident.

Client Disclaimer Template

AI Connector Implementation Disclaimer

1. Scope of Service: TranTech Computers ("the Company") provides the technical bridge between AI services and your Microsoft 365 environment. The Company does not control the logic, accuracy, or output generated by the third-party AI model.

2. Data Security & Permissions: The Client acknowledges that the AI will have access to all data the authenticated user account can "see." It is the Client's responsibility to ensure that SharePoint permissions and Folder Access levels are strictly audited prior to implementation. The Company is not liable for the disclosure of sensitive information resulting from improper internal permission structures.

3. Data Integrity & Backups: The Client understands that AI interactions can result in automated data modification. The Company strongly advises the use of an independent, third-party backup solution. The Company shall not be held liable for data loss, corruption, or "hallucinated" content produced by the AI connector.

4. No Guarantee of Accuracy: Outputs generated by AI connectors are for informational purposes only. All AI-generated emails, summaries, and file modifications should be reviewed by a human professional.

5. Acceptance of Risk: By proceeding with this integration, the Client accepts all inherent risks associated with Large Language Models (LLMs) and third-party AI connectors, including potential impacts on data privacy and system stability.

Disclaimer: TranTech accepts no responsibility or liability for risks, operational outcomes, or potential data leakage associated with third-party or integrated AI models. Users interact with AI platforms at their own discretion and risk.

Name: _____ Signed: _____

Date: _____

Next Steps for Implementation:

- **Audit Permissions:** Run a SharePoint sharing report to see what is currently "Public" or "Organization-wide."
- **Verify Backup:** Ensure your current backup solution (e.g., Veeam, Datto, or AvePoint) is successfully backing up the specific SharePoint sites and Mailboxes being indexed by the AI.