SharePoint Integration (Import)

1. Purpose and Scope

This document provides a comprehensive explanation of how Pickit's SharePoint Import feature works, the permissions required, and the security measures in place to protect organizational content.

It is intended for IT administrators, compliance officers, and security teams evaluating the use of Pickit for importing files from Microsoft SharePoint into Pickit libraries or collections.

---

2. Delegated Permissions – Core Concept

The SharePoint Import integration uses Microsoft's **delegated permissions** model, which ensures that:

- Pickit can only act **on behalf of a logged-in Microsoft 365 user**.
- The actions are limited to files and folders the user has explicit permission to view in SharePoint.
- There is **no elevation** of privileges — Pickit cannot access sites, libraries, or files the user could not access directly in SharePoint.

All requests are made within the authenticated user's browser session, ensuring that Microsoft's access controls remain in full effect.

---

3. Why Read Permission Scopes are Required

When a user enables the import feature, Microsoft's OAuth consent screen may display permission scopes such as:

> *"Read items in all site collections"*
>
> *"View user basic profile"*

This language, set by Microsoft, is intentionally broad and covers any site, library, or folder the user might have access to.

In practice, Pickit's import process:

- Only reads from specific folders or libraries the user selects.
- Never accesses or indexes unrelated SharePoint content.
- Operates within the **boundaries of the user's existing SharePoint permissions**.

---

4. Import Feature – How It Works

The SharePoint Import functionality allows users to:

1. **Sign in with Microsoft 365** via Azure AD to establish delegated permissions.
2. **Browse SharePoint content** they have access to directly from within Pickit.
3. **Select one or more folders or files** to import into Pickit collections.
4. **Optionally enable synchronization** so that changes in SharePoint are reflected in Pickit.

---

5. Synchronization Feature – Detailed Operation

If the user enables import sync:

- Pickit creates a **mapping** between SharePoint items and Pickit assets.
- The sync runs every **4–6 hours**, but only when:
  - The user is logged into Pickit.
  - The delegated permissions token is still valid.
- If a file is **updated in SharePoint**, Pickit replaces the version stored in the linked Pickit collection.
- If a new file is added to the mapped SharePoint location, it is imported during the next sync.

Important:

Because the import operates entirely within the **user's browser session**, there is **no background service** that can pull data from SharePoint when the user is offline.

---

6. Data Flow

1. **User Authentication** – The user logs into Pickit via Microsoft Azure AD OAuth 2.0.
2. **Permission Consent** – Microsoft shows the user which read-based scopes Pickit requires.
3. **Token Issuance** – Upon consent, an access token is stored securely in the user's browser cache.
4. **Content Selection** – The user chooses which folders/files in SharePoint to import.
5. **Data Transfer** – Files are fetched securely via Microsoft Graph API and stored in Pickit.
6. **Sync Updates (if enabled)** – Pickit checks the mapped SharePoint items periodically (only when the user is online).

---

7. Security Measures

- **Delegated Access Only** – Pickit cannot access SharePoint files outside the user's own permissions.
- **Read-Only Scopes** – The import integration does not include write or delete permissions in SharePoint.
- **Encrypted Transfer** – All data is transmitted over TLS 1.2+ secure connections.
- **Granular Mapping** – Only user-selected locations are scanned and imported.
- **Session Boundaries** – Tokens expire per Microsoft policy; no long-term storage.

---

8. Risk Assessment & Mitigation

Risk	Potential Impact	Mitigation
Broad permission wording	May cause user concern	Transparent documentation explaining delegated nature of access
Token compromise	Could allow unauthorized reading of accessible SharePoint files	Tokens stored in browser only, revocable at any time via Microsoft 365 admin

Unintended import	User may import sensitive files by mistake	User-controlled selection, no auto-import outside mapped folders
Compliance	Risk of handling regulated data	GDPR-compliant workflows, administrator control over access revocation

---

9. Compliance & Governance

- **GDPR & Data Privacy** – Pickit only processes files the user selects; no scanning or indexing of unrelated SharePoint content.
- **Data Residency** – Imported files are stored in Pickit's asset library as chosen by the user; no replication outside intended use.
- **Admin Oversight** – Microsoft 365 administrators can audit, revoke, or limit Pickit's SharePoint access at any time.

---

10. Access Token Storage Policy

Pickit follows a **strict token storage policy**:

- Access tokens are stored **only** in the user's browser cache.
- No tokens are saved on Pickit servers, databases, or any external storage.
- Tokens are removed when the user logs out or clears their browser cache.
- This policy is enforced across all Pickit products and audited regularly.

---

11. Summary

The SharePoint Import feature in Pickit is built to be **secure, controlled, and fully user-driven**.

By operating exclusively on delegated, read-only permissions, restricting execution to active browser sessions, and maintaining a strict local-only token policy, Pickit ensures that imported content comes only from authorized sources and under the direct control of the user.