Microsoft SharePoint Online

M365 Minimum Viable Secure Configuration Baseline

Draft Version 0.1

October 2022
Cybersecurity and Infrastructure Security Agency
Secure Cloud Business Applications (SCuBA)

Record of Changes

No.	Date	Reference	A=Add
			M=Modify
			D=Delete
				Description of Change

v0.1	17 October 2022	Entire document	M	Initial Draft w/Edit

Table of Contents

This page is intentionally blank.

1. Introduction

SharePoint Online is a web-based collaboration and document management platform. Though highly flexible, it is primarily used to store documents and communicate information across organizations. Organizations can use SharePoint Online to create sites, pages, document libraries, lists, and custom applications.

In this baseline, the types of SharePoint Online users are defined as follows (Note: These terms vary in use across Microsoft documentation and within the context of different M365 workloads (e.g., Teams verses SharePoint Online)):

1. **Internal users**: members of the agency's M365 organization.
2. **External users**: members of a different M365 organization.
3. **Business to Business (B2B) Guest users**: external users that are formally invited to collaborate and added to the agency's Azure Active Directory (AAD) as guest users. These users authenticate with their home organization/tenant and are granted access by virtue of being listed as guest users on the tenant's AAD.
4. **Unmanaged users**: users that are not members of any M365 tenant or organization (e.g., recipients of an "Anyone link.").

External sharing within SharePoint Online is defined as users within an organization sharing content with people outside the organization (such as external users, B2B guest users, or unmanaged users), or with licensed users on multiple Microsoft 365 (m365) subscriptions if the agency has more than one subscription. SharePoint has external sharing settings at both the organizational level and the site level (previously called the "site collection" level). To allow external sharing on any site, it must be allowed at the organization level. Then, external sharing can be restricted for other sites. If a site's external sharing option and the organization-level sharing option don't match, the most restrictive value will always be applied.

Source: https://docs.microsoft.com/en-us/sharepoint/external-sharing-overview

1.1 Resources

License Compliance and Copyright

Portions of this document are adapted from documents in Microsoft's M365 and Azure GitHub repositories. The respective documents are subject to copyright and are adapted under the terms of the Creative Commons Attribution 4.0 International license. Source documents are linked throughout this document. The United States Government has adapted selections of these documents to develop innovative and scalable configuration standards to strengthen the security of widely used cloud-based software services.

1.2 Assumptions

The **License Requirements** sections of this document assume the organization is using an M365 E3 or G3 license level. Therefore, only licenses that are not included in E3/G3 are listed.

2. Baselines

2.1 File and Folder Links Default Sharing Settings SHALL Be Set to "Specific People (Only the People the User Specifies)"

This policy ensures that when sharing files in SharePoint, there are several possible scopes, including agency-wide or “anyone with the link.”

2.1.1 Policy

- File and folder links default sharing setting SHALL be set to “Specific People (Only the People the User Specifies).”

2.1.2 Resources

- File and folder links | Microsoft Documents

2.1.3 License Requirements

- N/A

2.1.4 Implementation

In the **SharePoint admin center**:

1. In the left-hand navigation bar, click **Policies** -> **Sharing** to display sharing settings.
2. Under **File and folder links**, ensure that the default link type is set to **Specific people (only the people the user specifies)**.

2.2 External Sharing SHOULD be Set to “New and Existing Guests” and Managed Through Approved Domains and/or Security Groups Per Interagency Collaboration Needs.

SharePoint allows sharing with users who are outside the agency, which is convenient but may pose a data loss or other information security risk. This working group recommends allowlisting by domains and security groups per interagency collaboration needs.

Note: Adjusting this setting will adjust external sharing for OneDrive and Teams to the same, selected level. OneDrive and Teams can be less permissive (not more permissive) than SharePoint Online.

Adding approved domains and/or security groups will also be reflected in One Drive external sharing settings.

External access may be granted on a per-domain basis. This may be desirable in some cases, e.g., for agency-to-agency collaboration (see the CIO Council's Interagency Collaboration Program’s OMB Max Site for a list of .gov domains for sharing).

2.2.1 Policy

- External sharing SHOULD be limited to approved domains and security groups per interagency collaboration needs.

2.2.2 Resources

- Manage sharing settings | Microsoft Documents

2.2.3 License Requirements

- N/A

2.2.4 Implementation

To adjust sharing settings, in the **SharePoint admin center**:

1. Select **Policies** -> **Sharing**.
2. Adjust external sharing slider to **New and Existing Guests.**
3. Expand **More external sharing settings.**
4. Select **Limit external sharing by domain**.
5. Select **Add domains.**
6. Add domains.
7. Select **Save.**
8. Select **Allow only users in specific security groups to share externally**.
9. Select **Manage security groups.**
10. Add security groups.
11. Select **Save.**

2.3 Sensitive SharePoint Sites SHOULD Adjust Their Default Sharing Settings to Those Best Aligning to Their Sensitivity Level

SharePoint allows sharing with users who are outside the agency, which is convenient but may pose a data loss or other information security risk. This working group recommends outside of the default organizational settings agencies should evaluate each created site and adjust sharing settings best aligned to their respective sensitivity level.

2.3.1 Policy

- Sharing settings for specific SharePoint sites SHOULD align to their sensitivity level.

2.3.2 Resources

- Managing SharePoint Online Security: A Team Effort | Microsoft Build

2.3.3 License Requirements

- N/A

2.3.4 Implementation

To limit external sharing by domain, in the **SharePoint admin center**:

1. Select **Sites.**
2. Select **Active sites.**

3. Select **Site name.**
4. Select **Add domains.**
5. Select **Policies.**
6. Under **external sharing**, select **Edit**.
7. Select permissions aligning to the risk posture associated with the sensitivity of the SharePoint site.
8. Select **Save.**

2.4 Expiration Times for Guest Access to a Site or OneDrive, and Reauthentication Expiration Times for People Who Use a Verification Code, SHOULD Be Determined by Mission Needs / Agency Policy or Else Defaulted to 30 Days.

SharePoint allows sharing with users who are outside the agency, which is convenient but may pose a data loss or other information security risk. This working group recommends setting an expiration time for guest access to the site or OneDrive.

Note: Adjusting this setting will adjust external sharing for OneDrive and Teams to the same, specified expiration times.

2.4.1 Policy

- Expiration timers for 'guest access to a site or OneDrive' and 'people who use a verification code' SHOULD be set.
- Expiration timers SHOULD be set to 30 days.

2.4.2 License Requirements

- N/A

2.4.3 Resources

- Managing SharePoint Online Security: A Team Effort | Microsoft Build

2.4.4 Implementation

To limit external sharing by domain, in the **SharePoint admin center**:

1. Select **Policies** -> **Sharing**.
2. Expand **More external sharing settings.**
3. Select **Guest access to a site or OneDrive will expire automatically after this many days.**
4. Enter "30" days.
5. Select **People who use a verification code must reauthenticate after this many days**.
6. Enter "30" days.

2.5 Users SHALL Be Prevented from Running Custom Scripts

Allowing users to run custom scripts can potentially allow malicious scripts to run in a trusted environment. For this reason, running custom scripts should not be allowed.

2.5.1 Policy

- Users SHALL be prevented from running custom scripts.

2.5.2 Resources

- Allow or prevent custom script | Microsoft Documents

2.5.3 License Requirements

- N/A

2.5.4 Implementation

In the **SharePoint Classic admin center**:

1. Scroll to the **Custom Script** setting and select both of the following:
   a. **Prevent users from running custom script on personal sites.**
   b. **Prevent users from running custom script on self-service created sites.**

3. Acknowledgements

In addition to acknowledging the important contributions of a diverse team of Cybersecurity and Infrastructure Security Agency (CISA) experts, CISA thanks the following federal agencies and private sector organizations that provided input during the development of the Secure Business Cloud Application's security configuration baselines in response to Section 3 of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*:

- Consumer Financial Protection Bureau (CFPB)
- Department of the Interior (DOI)
- National Aeronautics and Space Administration (NASA)
- Sandia National Laboratories (Sandia)
- U.S. Census Bureau (USCB)
- U.S. Geological Survey (USGS)
- U.S. Office of Personnel Management (OPM)
- U.S. Small Business Administration (SBA)

The cross-agency collaboration and partnerships developed during this initiative serve as an example for solving complex problems faced by the federal government.

Cybersecurity Innovation Tiger Team (CITT) Leadership
Beau Houser (USCB), Sanjay Gupta (SBA), Michael Witt (NASA), James Saunders (OPM), Han Lin (Sandia), Andrew Havely (DOI).

CITT Authors

Trafenia Salzman (SBA), Benjamin McChesney (OPM), Robert Collier (USCB), Matthew Snitchler (Sandia), Darryl Purdy (USCB), Brandon Frankens (NASA), Brandon Goss (NASA), Nicole Bogeajis (DOI/USGS), Kevin Kelly (DOI), Adnan Ehsan (CFPB), Michael Griffin (CFPB), Vincent Urias (Sandia), Angela Calabaza (Sandia).

CITT Contributors

Dr. Mukesh Rohatgi (MITRE), Lee Szilagyi (MITRE), Nanda Katikaneni (MITRE), Ted Kolovos (MITRE), Thomas Comeau (MITRE), Karen Caraway (MITRE), Jackie Whieldon (MITRE), Jeanne Firey (MITRE), Kenneth Myers (General Services Administration).