TLP:CLEAR

# SHAREPOINT & ONEDRIVE

## Secure Cloud Business Applications Minimum Viable Secure Configuration Baselines

Version: 1.0

Publication: 12/2023

Cybersecurity and Infrastructure Security Agency



TLP:CLEAR

# REVISION HISTORY

| Version | Summary of revisions | Edited By | Date |
|---|---|---|---|
| 1.0 | • Creation | CISA | 08/13/2023 |

# CONTENTS

# 1. CISA M365 SECURITY CONFIGURATION BASELINE FOR SHAREPOINT ONLINE AND ONEDRIVE

Microsoft 365 (M365) SharePoint Online is a web-based collaboration and document management platform. It is primarily used to collaborate on documents and communicate information in projects. M365 OneDrive is a cloud-based file storage system primarily used to store a user's personal files, but it can also be used to share documents with others. This secure configuration baseline (SCB) provides specific policies to strengthen the security of both services.

The Secure Cloud Business Applications (SCuBA) project run by the Cybersecurity and Infrastructure Security Agency (CISA) provides guidance and capabilities to secure federal civilian executive branch (FCEB) agencies' cloud business application environments and protect federal information that is created, accessed, shared, and stored in those environments.

The CISA SCuBA SCBs for M365 help secure federal information assets stored within M365 cloud business application environments through consistent, effective, and manageable security configurations. CISA created baselines tailored to the federal government's threats and risk tolerance with the knowledge that every organization has different threat models and risk tolerance. Non-governmental organizations may also find value in applying these baselines to reduce risks.

The information in this document is being provided "as is" for INFORMATIONAL PURPOSES ONLY. CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial entities or commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoritism by CISA. This document does not address, ensure compliance with, or supersede any law, regulation, or other authority. Entities are responsible for complying with any recordkeeping, privacy, and other laws that may apply to the use of technology. This document is not intended to, and does not, create any right or benefit for anyone against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

## 1.1 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 at a minimum. Therefore, only licenses not included in E3/G3 are listed.

## 1.3 KEY TERMINOLOGY

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

# 2. BASELINE POLICIES

## 2.1 EXTERNAL SHARING

This section helps reduce security risks related to sharing files with users external to the agency. This includes guest users, users who use a verification code, and users who access an Anyone link.

## 2.2 POLICIES

### 2.2.1 MS.SHAREPOINT.1.1v1

External sharing for SharePoint SHALL be limited to **Existing guests** or **Only People in your organization**.

- *Rationale:* Sharing information outside the organization via SharePoint increases the risk of unauthorized access. By limiting external sharing, administrators decrease the risk of unauthorized access to information.
- *Last modified:* June 2023

### 2.2.2 MS.SHAREPOINT.1.2v1

External sharing for OneDrive SHALL be limited to **Existing guests** or **Only People in your organization**.

- *Rationale:* Sharing files outside the organization via OneDrive increases the risk of unauthorized access. By limiting external sharing, administrators decrease the risk of unauthorized access to information.
- *Last modified:* June 2023

### 2.2.3 MS.SHAREPOINT.1.3v1

External sharing SHALL be restricted to approved external domains and/or users in approved security groups per interagency collaboration needs.

- *Rationale:* By limiting sharing to domains and/or approved security groups used for interagency collaboration purposes, administrators help prevent sharing with unknown organizations and individuals.
- *Last modified:* June 2023
- *Note:* This policy is only applicable if the external sharing slider on the admin page is set to any value other than **Only People in your organization**.

### 2.2.4 MS.SHAREPOINT.1.4v1

Guest access SHALL be limited to the email the invitation was sent to.

- *Rationale:* Email invitations allow external guests to access shared information. By requiring guests to sign in using the same account where the invite was sent, administrators help ensure only the intended guest can use the invite.
- *Last modified:* June 2023
- *Note:* This policy is only applicable if the external sharing slider on the admin page is set to any value other than **Only People in your organization**.

## 2.3 RESOURCES

- Overview of external sharing in SharePoint and OneDrive in Microsoft 365 | Microsoft Documents
- Manage sharing settings for SharePoint and OneDrive in Microsoft 365 | Microsoft Documents

## 2.4 LICENSE REQUIREMENTS

- N/A

## 2.5 IMPLEMENTATION

### 2.5.1 MS.SHAREPOINT.1.1v1 Instructions

1. Sign in to the **SharePoint admin center.**
2. Select **Policies** > **Sharing**.
3. Adjust external sharing slider for SharePoint to **Existing guests** or **Only people in your organization**.
4. Select **Save**.

### 2.5.2 MS.SHAREPOINT.1.2v1 Instructions

1. Sign in to the **SharePoint admin center.**
2. Select **Policies** > **Sharing**.
3. Adjust external sharing slider for OneDrive to **Existing guests** or **Only people in your organization**.
4. Select **Save**.

### 2.5.3 MS.SHAREPOINT.1.3v1 Instructions

Note: If SharePoint external sharing is set to its most restrictive setting of **Only people in your organization**, then no external sharing is allowed and no implementation changes are required for this policy item.

1. Sign in to the **SharePoint admin center.**
2. Select **Policies** > **Sharing**.
3. Expand **More external sharing settings**.
4. Select **Limit external sharing by domain**.
5. Select **Add domains**.
6. Add each approved external domain users are allowed to share files with.
7. Select **Manage security groups.**
8. Add each approved security group. Members of these groups will be allowed to share files externally.
9. Select **Save**.

### 2.5.4 MS.SHAREPOINT.1.4v1 Instructions

Note: If SharePoint external sharing is set to its most restrictive setting of **Only people in your organization,** then no external sharing is allowed and no implementation changes are required for this policy item.

1. Sign in to the **SharePoint admin center.**
2. Select **Policies** > **Sharing**.
3. Expand **More external sharing settings**.
4. Select **Guests must sign in using the same account to which sharing invitations are sent**.
5. Select **Save**.

# 3. FILE AND FOLDER DEFAULT SHARING SETTINGS

This section provides policies to set the scope and permissions for sharing links to secure default values.

## 3.1 POLICIES

### 3.1.1 MS.SHAREPOINT.2.1v1

File and folder default sharing scope SHALL be set to **Specific people (only the people the user specifies).**

- *Rationale:* By making the default sharing the most restrictive, administrators prevent accidentally sharing information too broadly.
- *Last modified: June 2023*

### 3.1.2 MS.SHAREPOINT.2.2v1

File and folder default sharing permissions SHALL be set to **View**.

- *Rationale:* Edit access to files and folders could allow a user to make unauthorized changes. By restricting default permissions to **View**, administrators prevent unintended or malicious modification.
- *Last modified:* June 2023

## 3.2 RESOURCES

- File and folder links | Microsoft Documents

## 3.3 LICENSE REQUIREMENTS

- N/A

## 3.4 IMPLEMENTATION

### 3.4.1 MS.SHAREPOINT.2.1v1 Instructions

1. Sign in to the **SharePoint admin center.**
2. Select **Policies** > **Sharing.**
3. Under **File and folder links**, set the default link type to **Specific people (only the people the user specifies).**
4. Select **Save.**

### 3.4.2 MS.SHAREPOINT.2.2v1 Instructions

1. Sign in to the **SharePoint admin center.**
2. Select **Policies** > **Sharing**.
3. Under **File and folder links**, set the permission that is selected by default for sharing links to **View**.
4. Select **Save**.

# 4. SECURING ANYONE LINKS AND VERIFICATION CODE USERS

Sharing files with external users via the usage of **Anyone links** or **Verification codes** is strongly discouraged because it provides access to data within a tenant with weak or no authentication. If these features are used, this section details some access restrictions that could provide limited security risk mitigations.

**Note**: The settings in this section are only applicable if an agency is using **Anyone links** or **Verification codes** sharing. See each policy below for details.

## 4.1 POLICIES

### 4.1.1 MS.SHAREPOINT.3.1v1

Expiration days for **Anyone links** SHALL be set to 30 days or less.

- *Rationale:* Links may be used to provide access to information for a short period of time. Without expiration, however, access is indefinite. By setting expiration timers for links, administrators prevent unintended sustained access to information.

- *Last modified:* June 2023
- *Note:* This policy is only applicable if the external sharing slider on the admin center sharing page is set to **Anyone**.

### 4.1.2 MS.SHAREPOINT.3.2v1

The allowable file and folder permissions for links SHALL be set to **View** only.

- *Rationale:* Unauthorized changes to files can be made if permissions allow editing by anyone. By restricting permissions on links to **View only**, administrators prevent anonymous file changes.
- *Last modified:* June 2023
- *Note:* This policy is only applicable if the external sharing slider on the admin center sharing page is set to **Anyone**.

### 4.1.3 MS.SHAREPOINT.3.3v1

Reauthentication days for people who use a verification code SHALL be set to 30 days or less.

- *Rationale:* A verification code may be given out to provide access to information for a short period of time. By setting expiration timers for verification code access, administrators prevent unintended sustained access to information.
- *Last modified:* June 2023
- *Note:* This policy is only applicable if the external sharing slider on the admin center sharing page is set to **Anyone** or **New and existing guests**.

## 4.2 LICENSE REQUIREMENTS

- N/A

## 4.3 RESOURCES

- Secure external sharing recipient experience | Microsoft Documents

## 4.4 IMPLEMENTATION

### 4.4.1 MS.SHAREPOINT.3.1v1 Instructions

1. Sign in to the **SharePoint admin center.**
2. Select **Policies** > **Sharing**.
3. Scroll to the section **Choose expiration and permissions options for Anyone links**.
4. Select the checkbox **These links must expire within this many days**.
5. Enter **30** days or less.
6. Select **Save**.

### 4.4.2 MS.SHAREPOINT.3.2v1 Instructions

1. Sign in to the **SharePoint admin center.**
2. Select **Policies** > **Sharing**.
3. Scroll to the section **Choose expiration and permissions options for Anyone links**.
4. Set the configuration items in the section **These links can give these permissions**.
5. Set the **Files** option to **View**.
6. Set the **Folders** option to **View**.
7. Select **Save**.

### 4.4.3 MS.SHAREPOINT.3.3v1 Instructions

1. Sign in to the **SharePoint admin center.**

2. Select **Policies** > **Sharing**.
3. Expand **More external sharing settings**.
4. Select **People who use a verification code must reauthenticate after this many days**.
5. Enter **30** days or less.
6. Select **Save**.

# 5. CUSTOM SCRIPTS

This section provides policies for restricting custom script execution.

## 5.1 POLICIES

### 5.1.1 MS.SHAREPOINT.4.1v1

Users SHALL be prevented from running custom scripts on personal sites (aka OneDrive).

- *Rationale:* Scripts in OneDrive folders run in the context of users visiting the site and have access to everything users can access. By preventing custom scripts on personal sites, administrators block a path for potentially malicious code execution.
- *Last modified:* June 2023

### 5.1.2 SHAREPOINT.4.2v1

Users SHALL be prevented from running custom scripts on self-service created sites.

- *Rationale:* Scripts on SharePoint sites run in the context of users visiting the site and therefore provide access to everything users can access. By preventing custom scripts on self-service created sites, administrators block a path for potentially malicious code execution.
- *Last modified:* June 2023

## 5.2 RESOURCES

- Allow or prevent custom script | Microsoft Documents

## 5.3 LICENSE REQUIREMENTS

- N/A

## 5.4 IMPLEMENTATION

### 5.4.1 MS.SHAREPOINT.4.1v1 Instructions

1. Sign in to the **SharePoint admin center.**
2. Select **Settings**.
3. Scroll down and select **classic settings page**.
4. Scroll to the **Custom Script** section.
5. Select **Prevent users from running custom script on personal sites**.
6. Select **OK**.

### 5.4.2 MS.SHAREPOINT.4.2v1 Instructions

1. Sign in to the **SharePoint admin center.**
2. Select **Settings**.
3. Scroll down and select **classic settings page**.
4. Scroll to the **Custom Script** section.

5. Select **Prevent users from running custom script on self-service created sites**.
6. Select **OK**.