



# Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016

First published: December 2016  
Last updated: July 2023

## Introduction

Workstations are often targeted by malicious actors using malicious websites, emails or removable media in an attempt to extract sensitive information. Hardening applications on workstations is an important part of reducing this risk.

This publication provides recommendations on hardening Microsoft 365, Office 2021, Office 2019 and Office 2016 applications. Before implementing the recommendations in this publication, testing should be undertaken to ensure the potential for unintended negative impacts on business processes is reduced as much as possible.

The [Group Policy Administrative Templates](#) for Microsoft 365, Office 2021, Office 2019 and Office 2016 can be obtained from Microsoft. Once downloaded, the ADMX and associated ADML files can be placed in %SystemDrive%\Windows\SYSVOL\domain\Policies\PolicyDefinitions on the Domain Controller and they will be automatically loaded in the Group Policy Management Editor. For cloud-based policy configurations, equivalents are available in [Microsoft 365 Apps admin centre](#) for many of the Group Policy settings. Finally, as Group Policy settings for Microsoft Office are periodically updated by Microsoft, care should be taken to ensure the latest version is always used.

## High priorities

The following recommendations, listed in alphabetical order, should be treated as high priorities when hardening Microsoft Office deployments.

### Attack surface reduction

[Attack surface reduction](#) (ASR), a security feature of Microsoft Windows 10, forms part of Microsoft Defender Exploit Guard. It is designed to combat the threat of malware exploiting legitimate functionality in Microsoft Office applications. In order to use ASR, Microsoft Defender Antivirus must be configured as the primary real-time antivirus scanning engine on workstations.

ASR offers a number of Microsoft Office-related attack surface reduction rules, these include:

- Block executable content from email client and webmail  
BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550
- Block all Office applications from creating child processes  
D4F940AB-401B-4EFC-AADC-AD5F3C50688A
- Block Office applications from creating executable content  
3B576869-A4EC-4529-8536-B80A7769E899

- Block Office applications from injecting code into other processes  
75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84
- Block Win32 API calls from Office macro  
92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B
- Block Office communication application from creating child processes  
26190899-1602-49E8-8B27-EB1D0A1CE869.

Organisations should either implement ASR using Microsoft Defender Antivirus or use third party antivirus solutions that offer similar functionality to those provided by ASR. For older versions of Microsoft Windows, alternative measures will need to be implemented to mitigate certain threats addressed by ASR, such as the likes of [Dynamic Data Exchange \(DDE\) attacks](#).

For organisations using Microsoft Defender Antivirus, the following Group Policy setting can be implemented to enforce the above ASR rules.

| Group Policy Setting                                                                                                                                                      | Recommended Option                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|---|--------------------------------------|---|--------------------------------------|---|--------------------------------------|---|--------------------------------------|---|--------------------------------------|---|
| <b>Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |
| Configure Attack Surface Reduction rules                                                                                                                                  | <p>Enabled</p> <p>Set the state for each ASR rule:</p> <table> <tr> <td>BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550</td><td>1</td></tr> <tr> <td>D4F940AB-401B-4EFC-AADC-AD5F3C50688A</td><td>1</td></tr> <tr> <td>3B576869-A4EC-4529-8536-B80A7769E899</td><td>1</td></tr> <tr> <td>75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84</td><td>1</td></tr> <tr> <td>92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B</td><td>1</td></tr> <tr> <td>26190899-1602-49E8-8B27-EB1D0A1CE869</td><td>1</td></tr> </table> | BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550 | 1 | D4F940AB-401B-4EFC-AADC-AD5F3C50688A | 1 | 3B576869-A4EC-4529-8536-B80A7769E899 | 1 | 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84 | 1 | 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B | 1 | 26190899-1602-49E8-8B27-EB1D0A1CE869 | 1 |
| BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550                                                                                                                                      | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |
| D4F940AB-401B-4EFC-AADC-AD5F3C50688A                                                                                                                                      | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |
| 3B576869-A4EC-4529-8536-B80A7769E899                                                                                                                                      | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |
| 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84                                                                                                                                      | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |
| 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B                                                                                                                                      | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |
| 26190899-1602-49E8-8B27-EB1D0A1CE869                                                                                                                                      | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |                                      |   |

## Flash content

Microsoft Office applications offer the ability to load embedded Flash content. Unfortunately, malicious actors can use this functionality to embed malicious Flash content in Microsoft Office documents as part of spear phishing campaigns. To reduce this risk, activation of Flash content should be blocked in Microsoft Office documents.

The following Group Policy setting can be implemented to block the use of Flash in Microsoft Office.

| Group Policy Setting                                                              | Recommended Option   |
|-----------------------------------------------------------------------------------|----------------------|
| <b>Computer Configuration\Policies\Administrative Templates\MS Security Guide</b> |                      |
| Block Flash activation in Office documents                                        | Block all activation |

## Latest version

Newer versions of Microsoft Office offer significant improvements in security features, functionality and stability. It is often the lack of improved security features that allows malicious actors to easily compromise older versions of

Microsoft Office. To reduce this risk, the latest supported version of Microsoft Office (Microsoft 365 or Office 2021) should be used.

## Loading external content

Dynamic Data Exchange (DDE) is a protocol used for transferring data between applications. For example, using external data sources to automatically update content in Microsoft Excel spreadsheets. Unfortunately, malicious actors can use DDE functionality, and other methods of loading external content, for malicious purposes. To reduce this risk, organisations should disable the ability to load data from external data sources in Microsoft Excel and Microsoft Word.

The following registry entries can be implemented using Group Policy preferences to assist in the prevention of loading malicious data from external data sources when using Microsoft Excel and Microsoft Word.

| Registry Entry                                                         | Recommended Option       |
|------------------------------------------------------------------------|--------------------------|
| <b>HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security</b> |                          |
| DataConnectionWarnings                                                 | REG_DWORD 0x00000002 (2) |
| RichDataConnectionWarnings                                             | REG_DWORD 0x00000002 (2) |
| WorkbookLinkWarnings                                                   | REG_DWORD 0x00000002 (2) |
| <b>HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security</b>  |                          |
| AllowDDE                                                               | REG_DWORD 0x00000000 (0) |

The following Group Policy settings can be implemented to assist in the prevention of loading malicious data from external data sources when using Microsoft Excel and Microsoft Word.

| Group Policy Setting                                                                                                                  | Recommended Option |
|---------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>User Configuration\Policies\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center\External Content</b> |                    |
| Always prevent untrusted Microsoft Query files from opening                                                                           | Enabled            |
| Don't allow Dynamic Data Exchange (DDE) server launch in Excel                                                                        | Enabled            |
| Don't allow Dynamic Data Exchange (DDE) server lookup in Excel                                                                        | Enabled            |
| <b>User Configuration\Policies\Administrative Templates\Microsoft Word 2016\Word Options\Advanced</b>                                 |                    |
| Update automatic links at Open                                                                                                        | Disabled           |

## Macros

Microsoft Office files can contain embedded code (known as a macro) written in the Visual Basic for Applications (VBA) programming language.

A macro can contain a series of commands that can be coded or recorded, and replayed at a later time to automate repetitive tasks. Macros are powerful tools that can be easily created by novice users to greatly improve their productivity. However, malicious actors can also create macros to perform a variety of malicious activities, such as assisting to compromise workstations in order to exfiltrate or deny access to sensitive information. To reduce this risk, organisations should either disable or secure their use of Microsoft Office macros.

For information on securing the use of Microsoft Office macros see the [Restricting Microsoft Office macros](#) publication.

## Object Linking and Embedding packages

Object Linking and Embedding (OLE) packages allow for content from other applications to be embedded into Microsoft Excel spreadsheets, Microsoft PowerPoint presentations and Microsoft Word documents. Unfortunately, like Microsoft Office macros, malicious actors can use OLE packages to execute malicious code. To reduce this risk, organisations should prevent the activation of OLE packages in Microsoft Excel, Microsoft PowerPoint and Microsoft Word.

The following registry entries can be implemented using Group Policy preferences to prevent the activation of OLE packages in Microsoft Excel, Microsoft PowerPoint and Microsoft Word.

| Registry Entry                                                              | Recommended Value        |
|-----------------------------------------------------------------------------|--------------------------|
| <b>HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security</b>      |                          |
| PackagerPrompt                                                              | REG_DWORD 0x00000002 (2) |
| <b>HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\PowerPoint\Security</b> |                          |
| PackagerPrompt                                                              | REG_DWORD 0x00000002 (2) |
| <b>HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security</b>       |                          |
| PackagerPrompt                                                              | REG_DWORD 0x00000002 (2) |

## Patching vulnerabilities

To address vulnerabilities identified in Microsoft Office, Microsoft regularly releases patches. If patches are not applied in an appropriate timeframe it can allow malicious actors to easily compromise workstations. To reduce this risk, patches should be applied in an appropriate timeframe as determined by the severity of vulnerabilities they address and any mitigating measures already in place.

For more information on determining the severity of vulnerabilities and appropriate timeframes for applying patches see the [Patching applications and operating systems](#) publication.

## Medium priorities

The following recommendations, listed in alphabetical order, should be treated as medium priorities when hardening Microsoft Office deployments.

### ActiveX

While ActiveX controls can be used for legitimate business purposes to provide additional functionality for Microsoft Office, they can also be used by malicious actors to gain unauthorised access to sensitive information or to execute malicious code. To reduce this risk, ActiveX controls should be disabled for Microsoft Office.

The following Group Policy setting can be implemented to disable the use of ActiveX controls in Microsoft Office.

| Group Policy Setting                                                                                | Recommended Option |
|-----------------------------------------------------------------------------------------------------|--------------------|
| <b>User Configuration\Policies\Administrative Templates\Microsoft Office 2016\Security Settings</b> |                    |
| Disable All ActiveX                                                                                 | Enabled            |

### Add-ins

While add-ins can be used for legitimate business purposes to provide additional functionality for Microsoft Office, they can also be used by malicious actors to gain unauthorised access to sensitive information or to execute malicious code. To reduce this risk, add-in use should be managed.

The following Group Policy settings can be implemented to manage add-ins in Microsoft Excel, Microsoft PowerPoint, Microsoft Project, Microsoft Visio and Microsoft Word.

| Group Policy Setting                                                                                                           | Recommended Option |
|--------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>User Configuration\Policies\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center</b>           |                    |
| Disable Trust Bar Notification for unsigned application add-ins and block them                                                 | Enabled            |
| Require that application add-ins are signed by Trusted Publishers                                                              | Enabled            |
| <b>User Configuration\Policies\Administrative Templates\Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center</b> |                    |
| Disable Trust Bar Notification for unsigned application add-ins and block them                                                 | Enabled            |
| Require that application add-ins are signed by Trusted Publishers                                                              | Enabled            |

**User Configuration\Policies\Administrative Templates\Microsoft Project 2016\Project Options\Security\Trust Center**

Disable Trust Bar Notification for unsigned application add-ins and block them Enabled

Require that application add-ins are signed by Trusted Publishers Enabled

**User Configuration\Policies\Administrative Templates\Microsoft Visio 2016\Visio Options\Security\Trust Center**

Disable Trust Bar Notification for unsigned application add-ins and block them Enabled

Require that application add-ins are signed by Trusted Publishers Enabled

**User Configuration\Policies\Administrative Templates\Microsoft Word 2016\Word Options\Security\Trust Center**

Disable Trust Bar Notification for unsigned application add-ins and block them Enabled

Require that application add-ins are signed by Trusted Publishers Enabled

Alternatively, the following Group Policy settings can be implemented to disable all add-ins in Microsoft Excel, Microsoft PowerPoint, Microsoft Project, Microsoft Visio and Microsoft Word.

| Group Policy Setting                                                                                                           | Recommended Option |
|--------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>User Configuration\Policies\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center</b>           |                    |
| Disable all application add-ins                                                                                                | Enabled            |
| <b>User Configuration\Policies\Administrative Templates\Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center</b> |                    |
| Disable all application add-ins                                                                                                | Enabled            |
| <b>User Configuration\Policies\Administrative Templates\Microsoft Project 2016\Project Options\Security\Trust Center</b>       |                    |
| Disable all application add-ins                                                                                                | Enabled            |
| <b>User Configuration\Policies\Administrative Templates\Microsoft Visio 2016\Visio Options\Security\Trust Center</b>           |                    |
| Disable all application add-ins                                                                                                | Enabled            |

## User Configuration\Policies\Administrative Templates\Microsoft Word 2016\Word Options\Security\Trust Center

|                                 |         |
|---------------------------------|---------|
| Disable all application add-ins | Enabled |
|---------------------------------|---------|

## Extension Hardening

Extension Hardening mitigates a number of scenarios whereby malicious actors would deceive users into opening malicious Microsoft Excel files. By default, users will be warned when file content or MIME type doesn't match the file extension; however, users can still allow such files to open. As such, it is important that only Microsoft Excel files that pass integrity checks are allowed to be opened. To reduce this risk, Extension Hardening functionality should be enabled for Microsoft Excel.

The following Group Policy setting can be implemented to enable Extension Hardening functionality in Microsoft Excel.

| Group Policy Setting                                                                                    | Recommended Option                |
|---------------------------------------------------------------------------------------------------------|-----------------------------------|
| <b>User Configuration\Policies\Administrative Templates\Microsoft Excel 2016\Excel Options\Security</b> |                                   |
| Force file extension to match file type                                                                 | Enabled<br>Always match file type |

## File Type Blocking

File Type Blocking can be used to block insecure file types such as legacy, binary and beta file types from opening in Microsoft Office. By failing to block such file types, malicious actors can exploit vulnerabilities in these file types to execute malicious code on workstations. To reduce this risk, insecure file types should be prevented from opening in Microsoft Office.

The following Group Policy settings can be implemented to block specified file types in Microsoft Excel, Microsoft PowerPoint, Microsoft Visio and Microsoft Word.

| Group Policy Settings                                                                                                                    | Recommended Option                                                |
|------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| <b>User Configuration\Policies\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings</b> |                                                                   |
| dBase III / IV files                                                                                                                     | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Dif and Sylk files                                                                                                                       | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Excel 2 macrosheets and add-in files                                                                                                     | Enabled<br>File block setting: Open/Save blocked, use open policy |

|                                                                                                                                                    |                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Excel 2 worksheets                                                                                                                                 | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Excel 3 macrosheets and add-in files                                                                                                               | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Excel 3 worksheets                                                                                                                                 | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Excel 4 macrosheets and add-in files                                                                                                               | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Excel 4 workbooks                                                                                                                                  | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Excel 4 worksheets                                                                                                                                 | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Excel 95 workbooks                                                                                                                                 | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Excel 95-97 workbooks and templates                                                                                                                | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Excel 97-2003 workbooks and templates                                                                                                              | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Set default file block behavior                                                                                                                    | Enabled<br>Blocked files are not opened                           |
| Web pages and Excel 2003 XML spreadsheets                                                                                                          | Enabled<br>File block setting: Open/Save blocked, use open policy |
| <b>User Configuration\Policies\Administrative Templates\Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\File Block Settings</b> |                                                                   |
| PowerPoint 97-2003 presentations, shows, templates and add-in files                                                                                | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Set default file block behavior                                                                                                                    | Enabled<br>Blocked files are not opened                           |
| <b>User Configuration\Policies\Administrative Templates\Microsoft Visio 2016\Visio Options\Security\Trust Center\File Block Settings</b>           |                                                                   |

|                                                                                                                                        |                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Visio 2000-2002 Binary Drawings, Templates and Stencils                                                                                | Enabled<br>File block setting: Open/Save blocked                  |
| Visio 2003-2010 Binary Drawings, Templates and Stencils                                                                                | Enabled<br>File block setting: Open/Save blocked                  |
| Visio 5.0 or earlier Binary Drawings, Templates and Stencils                                                                           | Enabled<br>File block setting: Open/Save blocked                  |
| <b>User Configuration\Policies\Administrative Templates\Microsoft Word 2016\Word Options\Security\Trust Center\File Block Settings</b> |                                                                   |
| Set default file block behavior                                                                                                        | Enabled<br>Blocked files are not opened                           |
| Word 2 and earlier binary documents and templates                                                                                      | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Word 2000 binary documents and templates                                                                                               | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Word 2003 binary documents and templates                                                                                               | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Word 2007 and later binary documents and templates                                                                                     | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Word 6.0 binary documents and templates                                                                                                | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Word 95 binary documents and templates                                                                                                 | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Word 97 binary documents and templates                                                                                                 | Enabled<br>File block setting: Open/Save blocked, use open policy |
| Word XP binary documents and templates                                                                                                 | Enabled<br>File block setting: Open/Save blocked, use open policy |

## Office File Validation

Office File Validation (OFV) checks that the format of a Microsoft Office file conforms to an expected standard. By default, Microsoft Office files that fail OFV checking will be opened in Protected View, with users given the option to enable editing. Alternatively, OFV can be configured to open Microsoft Office files in Protected View in an enforced read-only state or simply block them from opening. If Microsoft Office is configured to disable OFV, users may be unaware that they are opening a Microsoft Office file that may be malicious in nature. To reduce this risk, OFV functionality should be enabled for Microsoft Office.

The following Group Policy settings can be implemented to enable OFV functionality in Microsoft Excel, Microsoft PowerPoint and Microsoft Word.

| Group Policy Settings                                                                                             | Recommended Option |
|-------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>User Configuration\Policies\Administrative Templates\Microsoft Excel 2016\Excel Options\Security</b>           |                    |
| Turn off file validation                                                                                          | Disabled           |
| <b>User Configuration\Policies\Administrative Templates\Microsoft PowerPoint 2016\PowerPoint Options\Security</b> |                    |
| Turn off file validation                                                                                          | Disabled           |
| <b>User Configuration\Policies\Administrative Templates\Microsoft Word 2016\Word Options\Security</b>             |                    |
| Turn off file validation                                                                                          | Disabled           |

## Running external programs

Microsoft PowerPoint offers the ability to assign the 'Run Program' functionality to action buttons. In doing so, clicking on an action button would automatically execute the assigned program without prompting. This functionality could be leveraged by malicious actors to execute a malicious program or leverage other legitimate programs to further a targeted cyber intrusion. To reduce this risk, the ability to run external programs using action buttons should be disabled.

The following Group Policy setting can be implemented to disable the ability to use action buttons to run external programs in Microsoft PowerPoint.

| Group Policy Settings                                                                                             | Recommended Option               |
|-------------------------------------------------------------------------------------------------------------------|----------------------------------|
| <b>User Configuration\Policies\Administrative Templates\Microsoft PowerPoint 2016\PowerPoint Options\Security</b> |                                  |
| Run Programs                                                                                                      | disable (don't run any programs) |

## Protected View

Protected View can be used to open Microsoft Office files from untrusted locations in a sandboxed environment. By default, Protected View is enabled for Microsoft Office files that have been downloaded from the internet, opened from a defined unsafe location or opened as an attachment from Microsoft Outlook. However, organisations can choose to disable Protected View for any or all of these scenarios. If so, malicious actors could exploit any of these avenues to deliver a malicious Microsoft Office file to a user's workstation. To reduce this risk, Protected View should be enabled for Microsoft Office.

The following Group Policy settings can be implemented to enable Protected View functionality in Microsoft Excel, Microsoft PowerPoint and Microsoft Word.

| Group Policy Settings                                                                                                                         | Recommended Option     |
|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <b>User Configuration\Policies\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center\Protected View</b>           |                        |
| Always open untrusted database files in Protected View                                                                                        | Enabled                |
| Do not open files from the Internet zone in Protected View                                                                                    | Disabled               |
| Do not open files in unsafe locations in Protected View                                                                                       | Disabled               |
| Set document behaviour if file validation fails                                                                                               | Enabled<br>Block files |
| Turn off Protected View for attachments opened from Outlook                                                                                   | Disabled               |
| <b>User Configuration\Policies\Administrative Templates\Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\Protected View</b> |                        |
| Do not open files from the Internet zone in Protected View                                                                                    | Disabled               |
| Do not open files in unsafe locations in Protected View                                                                                       | Disabled               |
| Set document behaviour if file validation fails                                                                                               | Enabled<br>Block files |
| Turn off Protected View for attachments opened from Outlook                                                                                   | Disabled               |
| <b>User Configuration\Policies\Administrative Templates\Microsoft Word 2016\Word Options\Security\Trust Center\Protected View</b>             |                        |
| Do not open files from the Internet zone in Protected View                                                                                    | Disabled               |
| Do not open files in unsafe locations in Protected View                                                                                       | Disabled               |
| Set document behaviour if file validation fails                                                                                               | Enabled<br>Block files |
| Turn off Protected View for attachments opened from Outlook                                                                                   | Disabled               |

## Trusted documents

Macros, ActiveX controls and other active content in trusted documents are assumed to be safe by Microsoft Office. Malicious actors can exploit this trust by modifying trusted documents to contain malicious code. To reduce this risk, trusted documents should be disabled for Microsoft Office.

The following Group Policy settings can be implemented to disable the use of trusted documents in Microsoft Excel, Microsoft PowerPoint, Microsoft Visio and Microsoft Word.

| Group Policy Settings                                                                                                          | Recommended Option |
|--------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>User Configuration\Policies\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center</b>           |                    |
| Turn off trusted documents                                                                                                     | Enabled            |
| Turn off Trusted Documents on the network                                                                                      | Enabled            |
| <b>User Configuration\Policies\Administrative Templates\Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center</b> |                    |
| Turn off trusted documents                                                                                                     | Enabled            |
| Turn off Trusted Documents on the network                                                                                      | Enabled            |
| <b>User Configuration\Policies\Administrative Templates\Microsoft Visio 2016\Visio Options\Security\Trust Center</b>           |                    |
| Turn off trusted documents                                                                                                     | Enabled            |
| Turn off Trusted Documents on the network                                                                                      | Enabled            |
| <b>User Configuration\Policies\Administrative Templates\Microsoft Word 2016\Word Options\Security\Trust Center</b>             |                    |
| Turn off trusted documents                                                                                                     | Enabled            |
| Turn off Trusted Documents on the network                                                                                      | Enabled            |

## Low priorities

The following recommendations, listed in alphabetical order, should be treated as low priorities when hardening Microsoft Office deployments.

### Hidden markup

To assist users in collaborating on the development of Microsoft Office files, Microsoft Office allows users to track changes relating to insertions, deletions and formatting of content, as well as providing the ability to make comments. Users may choose to either view or hide these markups. If markup content is hidden, users may be unaware that sensitive changes or comments may still be included when Microsoft Office files are distributed to external parties or

released into the public domain. To reduce this risk, users should be made aware of hidden markup in Microsoft Office files.

The following Group Policy settings can be implemented to make users aware of hidden markup in Microsoft PowerPoint and Microsoft Word files.

| Group Policy Settings                                                                                             | Recommended Option |
|-------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>User Configuration\Policies\Administrative Templates\Microsoft PowerPoint 2016\PowerPoint Options\Security</b> |                    |
| Make hidden markup visible                                                                                        | Enabled            |
| <b>User Configuration\Policies\Administrative Templates\Microsoft Word 2016\Word Options\Security</b>             |                    |
| Make hidden markup visible                                                                                        | Enabled            |

## Reporting information

Microsoft Office contains in-built functionality, namely the Office Feedback Tool, which allows users to provide feedback, including screenshots, to Microsoft. This information if captured by malicious actors could expose sensitive information on workstations such as file names, directory names, versions of installed applications or content open in other applications. This information could subsequently be used by malicious actors to tailor malicious code to target specific workstations or users. To reduce this risk, functionality in Microsoft Office that allows reporting of information to Microsoft should be disabled.

The following Group Policy settings can be implemented to prevent users reporting information to Microsoft.

| Group Policy Setting                                                                                   | Recommended Option                          |
|--------------------------------------------------------------------------------------------------------|---------------------------------------------|
| <b>User Configuration\Policies\Administrative Templates\Microsoft Office 2016\Privacy\Trust Center</b> |                                             |
| Allow including screenshot with Office Feedback                                                        | Disabled                                    |
| Automatically receive small updates to improve reliability                                             | Disabled                                    |
| Configure the level of client software diagnostic data sent by Office to Microsoft                     | Enabled<br>Type of diagnostic data: Neither |
| Disable Opt-in Wizard on first run                                                                     | Enabled                                     |
| Enable Customer Experience Improvement Program                                                         | Disabled                                    |
| Send Office Feedback                                                                                   | Disabled                                    |
| Send personal information                                                                              | Disabled                                    |

## Contact details

If you have any questions regarding this guidance you can [write to us](#) or call us on 1300 CYBER1 (1300 292 371).

## Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

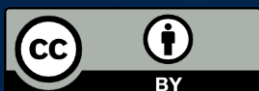
The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

## Copyright

© Commonwealth of Australia 2023.

With the exception of the Coat of Arms, the Australian Signals Directorate logo and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence ([www.creativecommons.org/licenses](http://www.creativecommons.org/licenses)).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence ([www.creativecommons.org/licenses](http://www.creativecommons.org/licenses)).

## Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website ([www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines](http://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines)).

**For more information, or to report a cyber security incident, contact us:**

**[cyber.gov.au](http://cyber.gov.au) | 1300 CYBER1 (1300 292 371)**



**Australian Government**  

---

**Australian Signals Directorate**