CENTER FOR INTERNET SECURITY

CIS Microsoft Office Excel 2016 Benchmark

v1.0.0 - 01-29-2016

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This document, Security Configuration Benchmark for Microsoft Excel 2016, provides prescriptive guidance for establishing a secure configuration posture for Microsoft Excel 2016 running on Windows 10. This guide was tested against Microsoft Office 2016. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Excel 2016 on a Microsoft Windows platform.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://community.cisecurity.org.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Contributor
Hardeep Mehrotara CISSP, CISA, GSEC, ISMSA

Editor
Jordan Rakoske

Recommendations

1 User Configuration

1.1 Customizable Error Messages

This section is intentionally blank and exists to ensure the structure of Excel benchmarks is consistent.

1.2 Data Recovery

This section contains settings to configure Data Recovery options.

1.2.1 (L1) Ensure 'Do Not Show Data Extraction Options When Opening Corrupt Workbooks' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Excel presents users with a list of data extraction options before beginning an Open and Repair operation when users choose to open a corrupt workbook in repair or extract mode.

If you enable this policy setting, Excel opens the file using the Safe Load process and does not prompt users to choose between repairing or extracting data.

If you disable or do not configure this policy setting, Excel prompts the user to select either to repair or to extract data, and to select either to convert to values or to recover formulas. The recommended state for this setting is: `Enabled`.

Rationale:

By default, when users choose to open a corrupt workbook with the Open and Repair command, Excel 2016 prompts them to choose between repairing or extracting data. Also, for cells that contain formulas, users are prompted to either convert the contents to values

or to recover formulas. If users choose to extract data instead of attempting to repair the workbook, important formulas, formatting, and VBA code could be lost unnecessarily.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\options\extractdatadisa
bleui
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Data Recovery\Do Not
Show Data Extraction Options When Opening Corrupt Workbooks
```

Impact:

Enabling this setting will prevent Excel 2016 users from choosing how workbooks are recovered, which could increase desktop support requests.

Default Value:

Not Configured

1.3 Disable Items in User Interface

This section is intentionally blank and exists to ensure the structure of Excel benchmarks is consistent.

1.3.1 Custom

This section is intentionally blank and exists to ensure the structure of Excel benchmarks is consistent.

1.3.2 Predefined

This section is intentionally blank and exists to ensure the structure of Excel benchmarks is consistent.

1.4 Excel Options

This sections contains settings for Excel Options.

1.4.1 Advanced

This section contains settings for Advances settings.

1.4.1.1 Web Options...

This sections contains settings for Web Options.

1.4.1.1.1 General

This section is intentionally blank and exists to ensure the structure of Excel benchmarks is consistent

1.4.1.1.2 (L1) Ensure 'Load Pictures from Web Pages Not Created in Excel' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Excel loads graphics when opening Web pages that were not created in Excel. It configures the "Load pictures from Web pages not created in Excel" option under the File tab | Options | Advanced | General | Web Options... | General tab.

If you enable or do not configure this policy setting, Excel loads any graphics that are included in the pages, regardless of whether they were originally created in Excel.

If you disable this policy setting, Excel will not load any pictures from Web pages that were not created in Excel. The recommended state for this setting is: `Disabled`.

Rationale:

By default, when users open Web pages in Excel 2016, Excel loads any graphics that are included in the pages, regardless of whether they were originally created in Excel. Users can change this option in the Web Options dialog box, which is available from the Advanced section of the Excel Options dialog box.

Allowing Excel to load graphics created in other programs can make Excel vulnerable to possible future zero-day attacks that use graphic files as an attack vector. If such an event occurs, this setting can be used to mitigate the vulnerability.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\internet\donotloadpictures
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel Options\Advanced\Web Options...\General\Load Pictures from Web Pages Not Created in Excel
```

Impact:

If this setting is disabled Excel will not load pictures from Web pages that were not created in Excel. This configuration can cause some disruptions for users who load Web pages in Excel that were created by other applications. Users who do not load Web pages in Excel will not be affected by this setting.

Default Value:

Not Configured

1.4.1.2 (L1) Ensure 'Ask to Update Automatic Links' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Excel prompts users to update automatic links, or whether the updates occur in the background with no prompt.

If you enable or do not configure this policy setting, Excel will prompt users to update automatic links. In addition, the "Ask to update automatic links" user interface option under File tab | Advanced | General is selected.

If you disable this policy setting, Excel updates automatic links without prompting or informing users, which could compromise the integrity of some of the information in the workbook. The recommended state for this setting is: `Enabled`.

Rationale:

If an Excel 2016 workbook contains links to other documents and users are not prompted to approve them, the contents of the workbook might change without the users' knowledge because the linked files have changed.

By default, users are prompted to update automatic links.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\options\binaryoptions\fupdateext_78_1
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel Options\Advanced\Ask to Update Automatic Links
```

Impact:

Enabling this setting enforces the default configuration in Excel, and therefore is unlikely to cause usability issues for most users.

Default Value:

Not Configured

1.4.2 Customize Ribbon

This section is intentionally blank and exists to ensure the structure of Excel benchmarks is consistent.

1.4.3 Formulas

This section is intentionally blank and exists to ensure the structure of Excel benchmarks is consistent.

1.4.4 General

This section is intentionally blank and exists to ensure the structure of Excel benchmarks is consistent.

1.4.5 Proofing

This section contains settings for Proofing and Autocorrect Options.

1.4.5.1 Autocorrect Options

This section contains settings for Autocorrect Options.

1.4.5.1.1 (L1) Ensure 'Internet and Network Paths as Hyperlinks' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether Excel automatically creates hyperlinks when users enter URL or UNC path information.

If you enable this policy setting, when users type a string of characters that Excel recognizes as a Uniform Resource Locator (URL) or Uniform Naming Convention (UNC) path to a resource on the Internet or a local network, Excel will automatically transform it into a hyperlink. Clicking the hyperlink opens it in the configured default Web browser or the appropriate application.

If you disable this policy setting, Excel will not transform URLs and UNC paths to hyperlinks.

If you do not configure this policy setting, Excel will automatically transform URLs and UNC paths to hyperlinks and users can change the behavior by selecting or deselecting the "Internet and network paths as hyperlinks" check box under File tab | Help | Options | Proofing | AutoCorrect Options... | AutoFormat as You Type tab | Replace as you type. The recommended state for this setting is: `Disabled`.

Rationale:

By default, when users type a string of characters that Excel 2016 recognizes as a Uniform Resource Locator (URL) or Uniform Naming Convention (UNC) path to a resource on the Internet or a local network, Excel will transform it into a hyperlink. Clicking the hyperlink opens it in the configured default Web browser or the appropriate application. This functionality can enable users to accidentally create links to dangerous or restricted resources, which could create a security risk.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\options\autohyperlink
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Proofing\Autocorrect Options\Internet and Network Paths as Hyperlinks
```

Impact:

If this setting is disabled, Excel users will still be able to create new hyperlinks manually, so it is unlikely to cause significant disruptions for most users.

Default Value:

Not Configured

1.4.6 Save

This section contains settings for Save options.

1.4.6.1 (L1) Ensure 'Do Not Show AutoRepublish Warning Alert' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Excel displays an alert before republishing a workbook to the World Wide Web.

If you enable this policy setting, no warning appears when the user saves a published workbook when AutoRepublish is enabled.

If you disable or do not configure this policy setting, a message dialog appears every time the user saves a published workbook when AutoRepublish is enabled. From this dialog, the user can disable AutoRepublish temporarily or permanently, or select "Do not show this message again" to prevent the dialog from appearing after every save. If the user selects "Do not show this message again", Excel will continue to automatically republish the data after every save without informing the user. The recommended state for this setting is: `Disabled`.

Rationale:

AutoRepublish is a feature in Excel 2016 that allows workbooks to be automatically republished to the World Wide Web each time the workbook is saved. A number of changes might need to be made to allow the workbook to be successfully published, including the following:

• External references are converted to values.

• Hidden formulas become visible.

• The Set precision as displayed option, which appears beneath the When calculating this workbook heading in the Advanced section of the Excel Options dialog box, is no longer available.

These types of changes can mean that the version on the Web page might not be the same as the Excel file.

By default, a message dialog box appears every time the user saves a published workbook when AutoRepublish is enabled. From this dialog box, the user can disable AutoRepublish temporarily or permanently, or select Do not show this message again to prevent the dialog box from appearing after every save. If the user selects Do not show this message again, Excel will continue to automatically republish the data after every save without informing the user.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\options\disableautorepu
blishwarning
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel Options\Save\Do
Not Show AutoRepublish Warning Alert
```

Impact:

Configuring this setting to "Always show the alert before publishing" reinforces the default functionality in Excel 2016, and is therefore unlikely to cause usability issues for most users

Default Value:

Not Configured

1.4.6.2 (L1) Ensure 'Default File Format' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls the default file format for saving workbooks in Excel.

If you enable this policy setting, you can set the default file format for Excel from among the following options:

- Excel Workbook (.xlsx).This option is the default configuration in Excel 2016.

- Excel Macro-Enabled Workbook (.xlsm)

- Excel Binary Workbook (.xlsb)

- Web Page (.htm; .html)

- Excel 97-2003 Workbook (.xls)

- Excel 5.0/95 Workbook (.xls)

- OpenDocument Spreadsheet (*.ods)

Users can choose to save workbooks in a different file format than the default.

If you disable or you do not configure this policy setting, Excel saves new workbooks in the Office Open XML format with an .xlsx extension. The recommended state for this setting is: `Enabled`.

Rationale:

By default, when users create new workbook files, Excel 2016 saves them in the new Excel 2016 format. Users can change this functionality by clicking the Office button, clicking Excel Options, and then selecting a file format from the Default file format list.

Disabling this setting allows users to choose from any of the available default file formats. If a new workbook is created in an earlier format, some users may not be unable to open or use the file, or they may choose a format that is less secure than the Excel 2016 format.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\options\defaultformat
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Save\Default File Format
```

Impact:

Enabling this setting does not prevent users from choosing a different file format for a new Excel file, and therefore, it is unlikely to affect usability for most users.

Default Value:

Not Configured

1.4.6.3 (L1) Ensure 'Disable AutoRepublish' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows administrators to disable the AutoRepublish feature in Excel. If users choose to publish Excel data to a static Web page and enable the AutoRepublish feature, Excel saves a copy of the data to the Web page every time the user saves the workbook. By default, a message dialog displays every time the user saves a published workbook when AutoRepublish is enabled. From this dialog, the user can disable AutoRepublish temporarily or permanently, or select "Do not show this message again" to prevent the dialog from appearing after every save. If the user selects "Do not show this message again", Excel will continue to automatically republish the data after every save without informing the user.

If you enable this policy setting, the AutoRepublish feature is turned off and Excel users will need to publish data to the Web manually.

If you disable or do not configure this policy setting, users can enable the AutoRepublish feature to automatically republish workbooks saved as type Web Page. The recommended state for this setting is: `Enabled`.

Rationale:

If users choose to publish Excel data to a static Web page and enable the AutoRepublish feature, Excel 2016 saves a copy of the data to the Web page every time the user saves the workbook. If the page is on a Web server, anyone who has access to the page will be able to see the updated data after every save, which can lead to the undesired disclosure of sensitive or incorrect information.

By default, a message dialog box displays every time the user saves a published workbook when AutoRepublish is enabled. From this dialog box, the user can disable AutoRepublish temporarily or permanently, or select Do not show this message again to prevent the dialog box from appearing after every save. If the user selects Do not show this message again, Excel will continue to automatically republish the data after every save without informing the user.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\options\disableautorepu
blish
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Save\Disable AutoRepublish
```

Impact:

If there is a critical business need to use the AutoRepublish feature, it might not be possible to enable this setting. However, in most situations users will be able to publish data to the Web manually.

Default Value:

Not Configured

1.4.7 Security

This sections contains settings to configure Security Options.

1.4.7.1 Cryptography

This section is intentionally blank and exists to ensure the structure of Excel benchmarks is consistent.

1.4.7.2 Trust Center

This section contains settings for configuring Trust Center settings.

1.4.7.2.1 File Block Settings

This section contains File Block Settings.

1.4.7.2.1.1 (L1) Ensure 'Excel 2 Macrosheets and Add-in Files' is set to Enabled(Open/Save blocked, use open policy) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open, view, edit, or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.

- Save blocked: Saving of the file type will be blocked .

- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

- Block: Both opening and saving of the file type will be blocked, and the file will not open.

- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.

- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will be blocked. The recommended state for this setting is: `Enabled. (Open/Save blocked, use open policy)`

Rationale:

By default, users can open, view, or edit this type of document in Excel 2016. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\fileblock\xl2macros
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings\Excel 2 Macrosheets and Add-in Files
```

Impact:

If your users require open, save, or view ability and you block some or all of these abilities, you could affect the productivity of your organization.

Default Value:

Not Configured

1.4.7.2.1.2 (L1) Ensure 'Excel 3 Macrosheets and Add-in Files' is set to Enabled(Open/Save blocked, use open policy) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open, view, edit, or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.

- Save blocked: Saving of the file type will be blocked.

- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

- Block: Both opening and saving of the file type will be blocked, and the file will not open.

- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.

- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will be blocked. The recommended state for this setting is: `Enabled. (Open/Save blocked, use open policy)`

Rationale:

By default, users can open, view, or edit this type of document in Excel 2016. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\fileblock\xl3macros
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings\Excel 3 Macrosheets and Add-in Files
```

Impact:

If your users require open, save, or view ability and you block some or all of these abilities, you could affect the productivity of your organization.

Default Value:

Not Configured

1.4.7.2.1.3 (L1) Ensure 'Excel 95-97 Workbooks and Templates' is set to Enabled(Open/Save Blocked, Use Open Policy) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open, view, edit, or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.

- Save blocked: Saving of the file type will be blocked.

- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

- Block: Both opening and saving of the file type will be blocked, and the file will not open.

- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.

- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked. The recommended state for this setting is: `Enabled`. (Open/Save Blocked, Use Open Policy)

Rationale:

By default, users can open, view, or edit this type of document in Excel 2016. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\fileblock\xl95
97workbooksandtemplates
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\File Block Settings\Excel 95-97 Workbooks and Templates
```

Impact:

If your users require open, save, or view ability and you block some or all of these abilities, you could affect the productivity of your organization.

Default Value:

Not Configured

1.4.7.2.1.4 (L1) Ensure 'Excel 2 Worksheets' is set to Enabled(Open/Save blocked, use open policy) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open, view, edit, or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.

- Save blocked: Saving of the file type will be blocked.

- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

- Block: Both opening and saving of the file type will be blocked, and the file will not open.

- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.

- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will be blocked. The recommended state for this setting is: `Enabled. (Open/Save blocked, use open policy)`

Rationale:

By default, users can open, view, or edit this type of document in Excel 2016. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\fileblock\xl2worksheets
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings\Excel 2 Worksheets
```

Impact:

If your users require open, save, or view ability and you block some or all of these abilities, you could affect the productivity of your organization.

Default Value:

Not Configured

1.4.7.2.1.5 (L1) Ensure 'Excel 4 Worksheets' is set to Enabled(Open/Save blocked, use open policy) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open, view, edit, or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.

- Save blocked: Saving of the file type will be blocked.

- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

- Block: Both opening and saving of the file type will be blocked, and the file will not open.

- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.

- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will be blocked The recommended state for this setting is: `Enabled. (Open/Save blocked, use open policy)`

Rationale:

By default, users can open, view, or edit this type of document in Excel 2016. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\fileblock\xl4worksheets
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings\Excel 4 Worksheets
```

Impact:

If your users require open, save, or view ability and you block some or all of these abilities, you could affect the productivity of your organization.

Default Value:

Not Configured

1.4.7.2.1.6 (L1) Ensure 'Excel 3 Worksheets" is set to Enabled (Open/Save blocked, use open policy) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open, view, edit, or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.

- Save blocked: Saving of the file type will be blocked.

- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

- Block: Both opening and saving of the file type will be blocked, and the file will not open.

- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.

- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will be blocked. The recommended state for this setting is: `Enabled. (Open/Save blocked, use open policy)`

Rationale:

By default, users can open, view, or edit this type of document in Excel 2016. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\fileblock\xl3worksheets
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings\Excel 3 Worksheets
```

Impact:

If your users require open, save, or view ability and you block some or all of these abilities, you could affect the productivity of your organization.

Default Value:

Not Configured

1.4.7.2.1.7 (L1) Ensure 'dBase III /IV Files' is set to Enable (Open/Save blocked, use open policy) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open, view, edit, or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.

- Save blocked: Saving of the file type will be blocked.

- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

- Block: Both opening and saving of the file type will be blocked, and the file will not open.

- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.

- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked. The recommended state for this setting is: `Enabled. (Open/Save blocked, use open policy)`

Rationale:

By default, users can open dBase III / IV files in Excel. If a vulnerability is discovered that affects these file types, you can use this setting to protect your organization against attacks by temporarily preventing users from opening files in these formats until a security update is available.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\fileblock\dbas
efiles
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\File Block Settings\dBase III /IV Files
```

Impact:

If your users must work with business-critical files that include these file types, enabling this setting could cause significant disruptions. Users who do not work with dBase III / IV files will likely not be affected by this setting.

Default Value:

Not Configured

1.4.7.2.1.8 (L1) Ensure 'Web Pages and Excel 2003 XML Spreadsheets' is set to Enabled (Open/Save blocked, use open policy) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open, view, edit, or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.

- Save blocked: Saving of the file type will be blocked.

- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

- Block: Both opening and saving of the file type will be blocked, and the file will not open.

- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.

- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked. The recommended state for this setting is: `Enabled`. (Open/Save blocked, use open policy)

Rationale:

By default, users can open, view, or edit specific web-related file types and Excel 2003 XML workbook files in Excel 2016. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\fileblock\html
andxmlssfiles
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\File Block Settings\Web Pages and Excel 2003 XML
Spreadsheets
```

Impact:

Enabling this setting requires the following file types to open in Protected View:

- *.mht
- *.mhtml
- *.htm
- *.html
- *.xml
- *.xlmss

Saving and editing these file types is not allowed.

Default Value:

Not Configured

1.4.7.2.1.9 (L1) Ensure 'Excel 95 Workbooks' is set to Enabled (Open/Save Blocked, Use Open Policy) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open, view, edit, or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.

- Save blocked: Saving of the file type will be blocked.

- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

- Block: Both opening and saving of the file type will be blocked, and the file will not open.

- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.

- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked. The recommended state for this setting is: `Enabled. (Open/Save Blocked, Use Open Policy)`

Rationale:

By default, users can open, view, or edit this type of document in Excel 2016. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\fileblock\xl95
workbooks
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\File Block Settings\Excel 95 Workbooks
```

Impact:

If your users require open, save, or view ability and you block some or all of these abilities, you could affect the productivity of your organization.

Default Value:

Not Configured

1.4.7.2.1.10 (L1) Ensure 'Default File Block Behavior' is set to Enabled (Blocked files are not opened) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine if users can open, view, or edit Excel files.

If you enable this policy setting, you can set one of these options:

- Blocked files are not opened

- Blocked files open in Protected View and cannot be edited

- Blocked files open in Protected View and can be edited

If you disable or do not configure this policy setting, the behavior is the same as the "Blocked files are not opened" setting. Users will not be able to open blocked files. The recommended state for this setting is: `Enabled. (Blocked files are not opened)`

Rationale:

By default, users can open, view, or edit a large number of file types in Excel 2016. Some file types are safer than others, as some could allow malicious code to become active on user computers or the network. For this reason, disabling or not configuring this setting could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\fileblock\open
inprotectedview
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\File Block Settings\Set Default File Block Behavior
```

Impact:

Enabling this setting prevents users from opening, viewing, or editing certain types of files in Excel 2016. Productivity in your organization could be affected if users who require access to any of these file types cannot access them.

Default Value:

Not Configured

1.4.7.2.1.11 (L1) Ensure 'Excel 4 Macrosheets and Add-in Files' is set to Enabled (Enabled: Open/Save blocked, use open policy) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open, view, edit, or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.

- Save blocked: Saving of the file type will be blocked.

- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

- Block: Both opening and saving of the file type will be blocked, and the file will not open.

- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.

- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will be blocked. The recommended state for this setting is: `Enabled. (Enabled: Open/Save blocked, use open policy)`

Rationale:

By default, users can open, view, or edit this type of document in Excel 2016. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\fileblock\xl4macros
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings\Excel 4 Macrosheets and Add-in Files
```

Impact:

If your users require open, save, or view ability and you block some or all of these abilities, you could affect the productivity of your organization.

Default Value:

Not Configured

1.4.7.2.1.12 (L1) Ensure 'Excel 4 Workbooks' is set to Enabled (Enabled: Open/Save blocked, use open policy) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open, view, edit, or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.

- Save blocked: Saving of the file type will be blocked.

- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

- Block: Both opening and saving of the file type will be blocked, and the file will not open.

- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.

- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will be blocked. The recommended state for this setting is: `Enabled. (Enabled: Open/Save blocked, use open policy)`

Rationale:

By default, users can open, view, or edit this type of document in Excel 2016. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\fileblock\xl4workbooks
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings\Excel 4 Workbooks
```

Impact:

If your users require open, save, or view ability and you block some or all of these abilities, you could affect the productivity of your organization.

Default Value:

Not Configured

1.4.7.2.1.13 (L1) Ensure 'Dif and Sylk Files' is set to Enabled (Open/Save blocked, use open policy) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open, view, edit, or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.

- Save blocked: Saving of the file type will be blocked.

- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

- Block: Both opening and saving of the file type will be blocked, and the file will not open.

- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.

- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked. The recommended state for this setting is: `Enabled. (Open/Save blocked, use open policy)`

Rationale:

DIF and SYLK are text-only file formats that are used to exchange data between different applications, such as Excel 2016. If a vulnerability is discovered that affects these kinds of files, you can use this setting to protect your organization against attacks by temporarily preventing users from opening files in these formats until a security patch is available.

By default, users can open DIF (.dif) and SYLK (.slk) files in Excel.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\fileblock\difa
ndsylkfiles
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\File Block Settings\Dif and Sylk Files
```

Impact:

Enabling this setting will prevent users from viewing or editing DIF and SYLK files in Excel 2016. If your users must work with business-critical files of these types, enabling this setting could cause significant disruptions. Users who do not work with DIF or SYLK files will likely not be affected by this setting.

Default Value:

Not Configured

1.4.7.2.2 Protected View

This section contains Protected View Settings.

1.4.7.2.2.1 (L1) Ensure 'Turn Off Protected View For Attachments Opened from Outlook' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine if Excel files in Outlook attachments open in Protected View.

If you enable this policy setting, Outlook attachments do not open in Protected View.

If you disable or do not configure this policy setting, Outlook attachments open in Protected View. The recommended state for this setting is: `Disabled`.

Rationale:

Enabling this setting allows Outlook 2016 attachments to open outside of Protected View. Email is a common way to spread files containing malicious code. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\protectedview\
disableattachmentsinpv
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\Protected View\Turn Off Protected View For Attachments
Opened from Outlook
```

Impact:

Opening Office 2016 files, such as the Office 2016 versions of Word, Excel, PowerPoint, and OneNote, is a common action. Users are unlikely to notice much difference when opening and viewing files in Protected View. Users who want to modify these kinds of files must save them to a safe location and then open them.

When Office 2016 application files open in Protected View, some functionality is unavailable. The process of dragging the file to a new location and then opening it takes more time than simply double-clicking the file to open it, modifying it, and then saving it to the same location. For these reasons, administrators may receive some complaints from users potentially confused about how to modify files originally only available to them in Protected View.

Default Value:

Not Configured

1.4.7.2.2.2 (L1) Ensure 'Do Not Open Files From The Internet Zone in Protected View' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine if files downloaded from the Internet zone open in Protected View.

If you enable this policy setting, files downloaded from the Internet zone do not open in Protected View.

If you disable or do not configure this policy setting, files downloaded from the Internet zone open in Protected View. The recommended state for this setting is: `Disabled`.

Rationale:

Enabling this setting allows files that users download from the Internet zone open outside of Protected View. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\protectedview\
disableinternetfilesinpv
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\Protected View\Do Not Open Files From The Internet Zone
in Protected View
```

Impact:

When files open in Protected View, some functionality will be unavailable and productivity in your organization could be affected. When this is undesirable, users will have to add

sites to their trusted sites list in Internet Explorer, thus allowing the files to be opened in normal view with all functionality available.

Default Value:

Not Configured

1.4.7.2.2.3 (L1) Ensure 'Do Not Open Files in Unsafe Locations in Protected View' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting lets you determine if files located in unsafe locations will open in Protected View. If you have not specified unsafe locations, only the "Downloaded Program Files" and "Temporary Internet Files" folders are considered unsafe locations.

If you enable this policy setting, files located in unsafe locations do not open in Protected View.

If you disable or do not configure this policy setting, files located in unsafe locations open in Protected View. The recommended state for this setting is: `Disabled`.

Rationale:

Enabling this setting allows users to open files located in unsafe locations that do not require Protected View. As a result, malicious code could become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\protectedview\
disableunsafelocationsinpv
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\Protected View\Do Not Open Files in Unsafe Locations in
Protected View
```

Impact:

The Downloaded Program Files folder and the Temporary Internet Files folder are considered unsafe locations. You may specify additional unsafe locations.

Some functionality is not available when files are opened in Protected View. In such cases, users must move the files from unsafe locations to save locations in order to access them with full functionality

Default Value:

Not Configured

1.4.7.2.2.4 (L1) Ensure 'Document Behavior if File Validation Fails' is set to Enabled (Open in Protected View and Unchecked for "Do not allow edit") (Scored)

Profile Applicability:

- Level 1

Description:

his policy setting controls how Office handles documents when they fail file validation.

If you enable this policy setting, you can configure the following options for files that fail file validation:

- Block files completely. Users cannot open the files.

- Open files in Protected View and disallow edit. Users cannot edit the files. This is also how Office handles the files if you disable this policy setting.

- Open files in Protected View and allow edit. Users can edit the files. This is also how Office handles the files if you do not configure this policy setting.

If you disable this policy setting, Office follows the "Open files in Protected View and disallow edit" behavior.

If you do not configure this policy setting, Office follows the "Open files in Protected View and allow edit" behavior. The recommended state for this setting is: `Enabled. (Open in Protected View and Unchecked for "Do not allow edit)`

Rationale:

Disabling or not configuring this setting allows users to open and edit files that have failed file validation outside of Protected View. As a result, malicious code or users could become active on user computers or the network. For example, a malicious user may purposely put invalid data in a file. The invalid data could force the program to fail or execute its code in an unexpected manner, giving the malicious user control of the application.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\filevalidation
\disableeditfrompv
HKEY_USERS\\software\policies\microsoft\office\16.0\excel\security\filevalidation\open
inprotectedview
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\Protected View\Set Document Behavior if File Validation
Fails
```

Impact:

By default, users can only open files in Protected View after the files fail validation to help prevent malicious code from running on user computers or the network. In this way, the application is protected from attacks attempting to induce unexpected execution paths. You can block files from opening at all, but this also prevents users from accessing any data in the file.

Using this setting allows the application to open files, and thus users to view valid data and detect invalid data that is visible. However, users cannot correct invalid data in the file. To do so, users must open such files on another isolated computer where this setting is set to a lower security level.

Default Value:

Not Configured

1.4.7.2.3 Trusted Locations

This section contains Trusted Locations settings.

1.4.7.2.3.1 (L1) Ensure 'Allow Trusted Locations on The Network' to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether trusted locations on the network can be used.

If you enable this policy setting, users can specify trusted locations on network shares or in other remote locations that are not under their direct control by clicking the "Add new location" button in the Trusted Locations section of the Trust Center. Content, code, and add-ins are allowed to load from trusted locations with minimal security and without prompting the user for permission.

If you disable this policy setting, the selected application ignores any network locations listed in the Trusted Locations section of the Trust Center.

If you also deploy Trusted Locations via Group Policy, you should verify whether any of them are remote locations. If any of them are remote locations and you do not allow remote locations via this policy setting, those policy keys that point to remote locations will be ignored on client computers.

Disabling this policy setting does not delete any network locations from the Trusted Locations list, but causes disruption for users who add network locations to the Trusted Locations list. Users are also prevented from adding new network locations to the Trusted Locations list in the Trust Center. We recommended that you do not enable this policy setting (as the "Allow Trusted Locations on my network (not recommended)" check box also states). Therefore, in practice, it should be possible to disable this policy setting in most situations without causing significant usability issues for most users.

If you do not enable this policy setting, users can select the "Allow Trusted Locations on my network (not recommended)" check box if desired and then specify trusted locations by clicking the "Add new location" button. The recommended state for this setting is: `Disabled`.

Rationale:

By default, files located in trusted locations and specified in the Trust Center are assumed to be safe. Content, code, and add-ins are allowed to load from trusted locations with minimal security and without prompting the user for permission.

By default, users can specify trusted locations on network shares or in other remote locations that are not under their direct control by selecting the Allow Trusted Locations on my network (not recommended) check box in the Trusted Locations section of the Trust Center. If a dangerous file is opened from a trusted location, it will not be subject to typical security measures and could affect users' computers or data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\trusted
locations\allownetworklocations
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\Trusted Locations\Allow Trusted Locations on The Network
```

Impact:

Disabling this setting will cause disruption for users who add network locations to the Trusted Locations list. However, this practice is discouraged (as the Allow Trusted Locations on my network (not recommended) check box itself states), so in practice it should be possible to disable this setting in most situations without causing significant usability issues for most users.

Default Value:

Not Configured

1.4.7.2.3.2 (L1) Ensure 'Disabled all Trusted Locations' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows administrators to disable all trusted locations in the specified applications. Trusted locations specified in the Trust Center are used to define file locations that are assumed to be safe. Content, code, and add-ins are allowed to load from trusted locations with a minimal amount of security, without prompting the users for permission. If a dangerous file is opened from a trusted location, it will not be subject to standard security measures and could harm users' computers or data.

If you enable this policy setting, all trusted locations (those specified in the Trust Center) in the specified applications are ignored, including any trusted locations established by Office 2016 during setup, deployed to users using Group Policy, or added by users themselves. Users will be prompted again when opening files from trusted locations.

If you disable or do not configure this policy setting, all trusted locations (those specified in the Trust Center) in the specified applications are assumed to be safe. The recommended state for this setting is: `Enabled`.

Rationale:

Trusted locations specified in the Trust Center are used to define file locations that are assumed to be safe. Content, code, and add-ins are allowed to load from trusted locations with a minimal amount of security, without prompting the users for permission. If a dangerous file is opened from a trusted location, it will not be subject to standard security measures and could harm users' computers or data.

By default, files located in trusted locations (those specified in the Trust Center) are assumed to be safe.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\trusted
locations\alllocationsdisabled
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\Trusted Locations\Disabled all Trusted Locations
```

Impact:

If there are business-critical reasons to access some files in a more trusted environment, disabling trusted locations could cause usability problems.

Default Value:

Not Configured

1.4.7.2.4 (L1) Ensure 'Trust Access To Visual Basic Project' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether automation clients such as Microsoft Visual Studio 2005 Tools for Microsoft Office (VSTO) can access the Visual Basic for Applications project system in the specified applications. VSTO projects require access to the Visual Basic for Applications project system in Excel, PowerPoint, and Word, even though the projects do not use Visual Basic for Applications. Design-time support of controls in both Visual Basic and C# projects depends on the Visual Basic for Applications project system in Word and Excel.

If you enable this policy setting, VSTO and other automation clients can access the Visual Basic for Applications project system in the specified applications. Users will not be able to change this behavior through the "Trust access to the VBA project object model" user interface option under the Macro Settings section of the Trust Center.

If you disable this policy setting, VSTO does not have programmatic access to VBA projects. In addition, the "Trust access to the VBA project object model" check box is cleared and users cannot change it. Note: Disabling this policy setting prevents VSTO projects from interacting properly with the VBA project system in the selected application.

If you do not configure this policy setting, automation clients do not have programmatic access to VBA projects. Users can enable this by selecting the "Trust access to the VBA project object model" in the "Macro Settings" section of the Trust Center. However, doing so allows macros in any documents the user opens to access the core Visual Basic objects, methods, and properties, which represents a potential security hazard.

The recommended state for this setting is: `Disabled`.

Rationale:

VSTO projects require access to the Visual Basic for Applications project system in Excel 2016, PowerPoint 2016, and Word 2016, even though the projects do not use Visual Basic for Applications. Design-time support of controls in both Visual Basic and C# projects depends on the Visual Basic for Applications project system in Word and Excel.

By default, Excel, Word, and PowerPoint do not allow automation clients to have programmatic access to VBA projects. Users can enable this by selecting the Trust access to the VBA project object model in the Macro Settings section of the Trust Center. However, doing so allows macros in any documents the user opens to access the core Visual Basic objects, methods, and properties, which represents a potential security hazard.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\accessvbom
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\Trust Access To Visual Basic Project
```

Impact:

Disabling this setting enforces the default configuration in Excel 2016, Word 2016, and PowerPoint 2016 and is therefore unlikely to cause significant usability issues for most users.

Default Value:

Not Configured

1.4.7.2.5 (L1) Ensure 'Disable Trust Bar Notification For Unsigned Application Add-ins And Block Them' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether the specified Office 2016 applications notify users when unsigned application add-ins are loaded or silently disable such add-ins without notification. This policy setting only applies if you enable the ''Require that application add-ins are signed by Trusted Publisher'' policy setting, which prevents users from changing this policy setting.

If you enable this policy setting, applications automatically disable unsigned add-ins without informing users.

If you disable this policy setting, if an application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

If you do not configure this policy setting, the disable behavior applies, and in addition, users can configure this requirement themselves in the ''Add-ins'' category of the Trust Center for the application. The recommended state for this setting is: `Enabled`.

Rationale:

By default, if an application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\notbpromptunsi
gnedaddin
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\Disable Trust Bar Notification For Unsigned Application
Add-ins And Block Them
```

Impact:

This setting only applies if the Office 2016 application is configured to require that all add-ins are signed by a trusted publisher. By default, users can configure this requirement themselves in the Add-ins category of the Trust Center for the application. To enforce this requirement, you must enable the Require that application add-ins are signed by Trusted Publisher setting in Group Policy, which prevents users from changing the setting themselves.

Default Value:

Not Configured

1.4.7.2.6 (L1) Ensure 'Require That Application Add-ins are Signed By Trusted Publisher' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether add-ins for the specified Office 2016 applications must be digitally signed by a trusted publisher.

If you enable this policy setting, the specified Office 2016 applications check the digital signature for each add-in before loading it. If an add-in does not have a digital signature, or if the signature did not come from a trusted publisher, the application disables the add-in and notifies the user. Microsoft provides four certificates for the Office 2016 release, which you can add to the Trusted Publishers list. These certificates must be added to the Trusted Publishers list if you require that all add-ins be signed by a trusted publisher. The Microsoft certificates are named Mscert01.cer, Mscert02.cer, Mscert03.cer, Mscert04.cer, and can be found on the Microsoft Web site. The Office 2016 release stores certificates for trusted publishers in the Internet Explorer trusted publisher store. Earlier versions of Office stored trusted publisher certificate information (specifically, the certificate thumbprint) in a special Office trusted publisher store. The Office 2016 release still reads trusted publisher certificate information from the Office trusted publisher store, but it does not write information to this store. Therefore, if you created a list of trusted publishers in a previous version of Office and you upgrade to the Office 2016 release, your trusted publisher list will still be recognized. However, any trusted publisher certificates that you add to the list will be stored in the Internet Explorer trusted publisher store.

The recommended state for this setting is: `Enabled`.

Rationale:

By default, Office 2016 applications do not check the digital signature on application add-ins before opening them. Disabling or not configuring this setting may allow an application to load a dangerous add-in. As a result, malicious code could become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\requireaddinsig
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center\Require That Application Add-ins are Signed By Trusted Publisher
```

Impact:

Enabling this setting could cause disruptions for users who rely on add-ins that are not signed by trusted publishers. These users will either have to obtain signed versions of such add-ins or stop using them.

Default Value:

Not Configured

1.4.7.2.7 (L1) Ensure 'VBA Macro Notification Settings' is set to Enabled (Disable all Except Digitally Signed Macros) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls how the specified applications warn users when Visual Basic for Applications (VBA) macros are present.

If you enable this policy setting, you can choose from four options for determining how the specified applications will warn the user about macros:

- Disable all with notification: The application displays the Trust Bar for all macros, whether signed or unsigned. This option enforces the default configuration in Office.

- Disable all except digitally signed macros: The application displays the Trust Bar for digitally signed macros, allowing users to enable them or leave them disabled. Any unsigned macros are disabled, and users are not notified.

- Disable all without notification: The application disables all macros, whether signed or unsigned, and does not notify users.

- Enable all macros (not recommended): All macros are enabled, whether signed or unsigned. This option can significantly reduce security by allowing dangerous code to run undetected.

If you disable this policy setting, "Disable all with notification" will be the default setting.

If you do not configure this policy setting, when users open files in the specified applications that contain VBA macros, the applications open the files with the macros disabled and display the Trust Bar with a warning that macros are present and have been disabled. Users can inspect and edit the files if appropriate, but cannot use any disabled functionality until they enable it by clicking "Enable Content" on the Trust Bar. If the user clicks "Enable Content", then the document is added as a trusted document.

Important: If "Disable all except digitally signed macros" is selected, users will not be able to open unsigned Access databases.

Also, note that Microsoft Office stores certificates for trusted publishers in the Internet Explorer trusted publisher store. Earlier versions of Microsoft Office stored trusted publisher certificate information (specifically, the certificate thumbprint) in a special Office trusted publisher store. Microsoft Office still reads trusted publisher certificate information from the Office trusted publisher store, but it does not write information to this store.

Therefore, if you created a list of trusted publishers in a previous version of Microsoft Office and you upgrade to Office, your trusted publisher list will still be recognized. However, any trusted publisher certificates that you add to the list will be stored in the Internet Explorer trusted publisher store. The recommended state for this setting is: `Enabled`. (Disable all Except Digitally Signed Macros)

Rationale:

By default, when users open files in Excel 2016 that contain VBA macros, Excel 2016 opens the files with the macros disabled, and displays the Trust Bar with a warning that macros are present and have been disabled. Users may then enable these macros by clicking Options on the Trust Bar and selecting the option to enable them.

Disabling or not configuring this setting may allow dangerous macros to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\vbawarnings
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\VBA Macro Notification Settings
```

Impact:

This configuration causes documents and templates that contain unsigned macros to lose any functionality supplied by those macros. To prevent this loss of functionality, users can install the macros in a trusted location, unless the Disable all trusted locations setting is configured to Enabled, which will block them from doing so. If your organization does not

use any officially sanctioned macros, consider choosing No Warnings for all macros but disable all macros for even stronger security.

Default Value:

Not Configured

1.4.7.2.8 (L1) Ensure 'Store Macro In Personal Macro Workbook by Default' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls the default location for storing macros in Excel.

If this policy setting is enabled, Excel stores macros in users' personal macro workbook.

If you disable or do not configure this policy setting, Excel stores macros in the active workbook from which they are created.

Note: In the user interface (UI), the "Store macro in" drop down list box in the Record Macro dialog box (Macros | Record Macro) allows users to choose whether to store the new macro in the current workbook, a new workbook, or their personal macro workbook (Personal.xlsb), a hidden workbook that opens every time Excel starts.

By default, Excel displays the "Store macro in" box with "This Workbook" already selected in the drop-down list. If a user saves a macro in the active workbook and then distributes the workbook to others, the macro is distributed along with the workbook. If you enable this policy setting, Excel displays the "Store macro in" box with "Personal Macro Workbook" already selected. Users can still select one of the other two options in the drop-down menu. The recommended state for this setting is: `Enabled`.

Rationale:

The Record Macro dialog box includes a drop-down menu that allows users to choose whether to store the new macro in the current workbook, a new workbook, or their personal macro workbook (Personal.xlsb), a hidden workbook that opens every time Excel 2016 starts.

By default, Excel displays the Record Macro dialog box with This Workbook already selected in the drop-down menu. If a user saves a macro in the active workbook and then distributes the workbook to others, the macro is distributed along with the workbook, which could put workbook data at risk if the macro is triggered accidentally or intentionally.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\options\binaryoptions\f
globalsheet_37_1
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Trust Center\Store Macro In Personal Macro Workbook by Default
```

Impact:

Enabling this setting does not prevent users from selecting a different location for storing macros, so it is unlikely to cause significant usability issues for most users.

Default Value:

Not Configured

1.4.7.3 (L1) Ensure 'Turn Off File Validation' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you turn off the file validation feature.

If you enable this policy setting, file validation will be turned off.

If you disable or do not configure this policy setting, file validation will be turned on. Office Binary Documents (97-2003) are checked to see if they conform against the file format schema before they are opened. The recommended state for this setting is: `Disabled`.

Rationale:

The file validation feature ensures that Office Binary Documents are checked to see if they conform against the file format schema before they are opened, which may help protect against certain types of attacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\filevalidation
\enableonload
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Turn Off File Validation
```

Impact:

If you enable this policy setting, file validation will be turned off. If you disable or do not configure this policy setting, file validation will be turned on. Office Binary Documents (97-2003) are checked to see if they conform against the file format schema before they are opened.

Default Value:

Not Configured

1.4.7.4 (L1) Ensure 'Force File Extension to Match File Type' is set to Enabled(Always match file type) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls how Excel loads file types that do not match their extension. Excel can load files with extensions that do not match the files' type. For example, if a comma-separated values (CSV) file named example.csv is renamed example.xls (or any other file extension supported by Excel 2003 and earlier only), Excel can properly load it as a CSV file.

If you enable this policy setting, you can choose from three options for working with files that have non-matching extensions:

- Allow different - Excel opens the files properly without warning users that the files have non-matching extensions. If users subsequently edit and save the files, Excel preserves both the true, underlying file format and the incorrect file extension.

- Allow different, but warn - Excel opens the files properly, but warns users about the file type mismatch. This option is the default configuration in Excel.

- Always match file type - Excel does not open any files that have non-matching extensions.

If you disable or do not configure this policy setting, if users attempt to open files with the wrong extension, Excel opens the file and displays a warning that the file type is not what Excel expected. The recommended state for this setting is: `Enabled. (`Always match file type)

Rationale:

Excel 2016 can load files with extensions that do not match the files' type. For example, if a comma-separated values (CSV) file named example.csv is renamed example.xls, Excel can properly load it as a CSV file.

Some attacks target specific file formats. If Excel is allowed to load files with extensions that do not match their file types, a malicious person can deceive users into loading dangerous files that have incorrect extensions.

By default, if users attempt to open files with the wrong extension, Excel opens the file and displays a warning that the file type is not what Excel expected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\extensionharde
ning
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel
Options\Security\Force File Extension to Match File Type
```

Impact:

Earlier versions of Excel did not enforce file type matching. Enabling this setting and selecting Always match file type might cause disruptions for users who rely on the functionality of earlier versions of Excel, and could interfere with the operation of tools and scripts that rely on it.

Default Value:

Not Configured

1.4.7.5 (L1) Ensure' Scan Encrypted Macros in Excel Open XML Workbooks' is set to Enable (Scan encrypted macros (default)) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether encrypted macros in Open XML workbooks be are required to be scanned with anti-virus software before being opened.

If you enable this policy setting, you may choose one of these options:

- Scan encrypted macros: encrypted macros are disabled unless anti-virus software is installed. Encrypted macros are scanned by your anti-virus software when you attempt to open an encrypted workbook that contains macros.

- Scan if anti-virus software available: if anti-virus software is installed, scan the encrypted macros first before allowing them to load. If anti-virus software is not available, allow encrypted macros to load.

- Load macros without scanning: do not check for anti-virus software and allow macros to be loaded in an encrypted file.

If you disable or do not configure this policy setting, the behavior will be similar to the "Scan encrypted macros" option. The recommended state for this setting is: `Enabled. (Scan encrypted macros (default))`

Rationale:

When an Office Open XML workbook is rights-managed or password-protected, any macros that are embedded in the workbook are encrypted along with the rest of the workbook's contents.

By default, these encrypted macros will be disabled unless they are scanned by antivirus software immediately before being loaded. If this default configuration is modified, Excel 2016 will not require encrypted macros to be scanned before loading. Excel will handle them as specified by the Office 2016 System macro security settings, which can cause macro viruses to load undetected and lead to data loss or reduced application functionality.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\excel\security\excelbypassencryptedmacroscan
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Scan Encrypted Macros in Excel Open XML Workbooks
```

Impact:

Disabling this setting enforces the default configuration in Excel 2016, and is therefore unlikely to cause usability issues for most users.

Default Value:

Not Configured

1.5 File Tab

This section is intentionally blank and exists to ensure the structure of Excel benchmarks is consistent.

1.5.1 Check Accessibility

This section is intentionally blank and exists to ensure the structure of Excel benchmarks is consistent.

1.6 Miscellaneous

This section is intentionally blank and exists to ensure the structure of Excel benchmarks is consistent.

1.6.1 Server Settings

This section is intentionally blank and exists to ensure the structure of Excel benchmarks is consistent.

Control		Set Correctly	
		Yes	No
1	**User Configuration**		
1.1	**Customizable Error Messages**		
1.2	**Data Recovery**		
1.2.1	(L1) Ensure 'Do Not Show Data Extraction Options When Opening Corrupt Workbooks' is set to Enabled (Scored)	☐	☐
1.3	**Disable Items in User Interface**		
1.3.1	**Custom**		
1.3.2	**Predefined**		
1.4	**Excel Options**		
1.4.1	**Advanced**		
1.4.1.1	**Web Options...**		
1.4.1.1.1	**General**		
1.4.1.1.2	(L1) Ensure 'Load Pictures from Web Pages Not Created in Excel' is set to Disabled (Scored)	☐	☐
1.4.1.2	(L1) Ensure 'Ask to Update Automatic Links' is set to Enabled (Scored)	☐	☐
1.4.2	**Customize Ribbon**		

1.4.3	**Formulas**		
1.4.4	**General**		
1.4.5	**Proofing**		
1.4.5.1	**Autocorrect Options**		
1.4.5.1.1	(L1) Ensure 'Internet and Network Paths as Hyperlinks' is set to Disabled (Scored)	☐	☐
1.4.6	**Save**		
1.4.6.1	(L1) Ensure 'Do Not Show AutoRepublish Warning Alert' is set to Disabled (Scored)	☐	☐
1.4.6.2	(L1) Ensure 'Default File Format' is set to Enabled (Scored)	☐	☐
1.4.6.3	(L1) Ensure 'Disable AutoRepublish' is set to Enabled (Scored)	☐	☐
1.4.7	**Security**		
1.4.7.1	**Cryptography**		
1.4.7.2	**Trust Center**		
1.4.7.2.1	**File Block Settings**		
1.4.7.2.1.1	(L1) Ensure 'Excel 2 Macrosheets and Add-in Files' is set to Enabled(Open/Save blocked, use open policy) (Scored)	☐	☐
1.4.7.2.1.2	(L1) Ensure 'Excel 3 Macrosheets and Add-in Files' is set to Enabled(Open/Save blocked, use open policy) (Scored)	☐	☐
1.4.7.2.1.3	(L1) Ensure 'Excel 95-97 Workbooks and Templates' is set to Enabled(Open/Save Blocked, Use Open Policy) (Scored)	☐	☐
1.4.7.2.1.4	(L1) Ensure 'Excel 2 Worksheets' is set to Enabled(Open/Save blocked, use open policy) (Scored)	☐	☐
1.4.7.2.1.5	(L1) Ensure 'Excel 4 Worksheets' is set to Enabled(Open/Save blocked, use open policy) (Scored)	☐	☐
1.4.7.2.1.6	(L1) Ensure 'Excel 3 Worksheets" is set to Enabled (Open/Save blocked, use open policy) (Scored)	☐	☐
1.4.7.2.1.7	(L1) Ensure 'dBase III /IV Files' is set to Enable (Open/Save blocked, use open policy) (Scored)	☐	☐
1.4.7.2.1.8	(L1) Ensure 'Web Pages and Excel 2003 XML Spreadsheets' is set to Enabled (Open/Save blocked, use open policy) (Scored)	☐	☐
1.4.7.2.1.9	(L1) Ensure 'Excel 95 Workbooks' is set to Enabled (Open/Save Blocked, Use Open Policy) (Scored)	☐	☐
1.4.7.2.1.10	(L1) Ensure 'Default File Block Behavior' is set to Enabled (Blocked files are not opened) (Scored)	☐	☐
1.4.7.2.1.11	(L1) Ensure 'Excel 4 Macrosheets and Add-in Files' is set to Enabled (Enabled: Open/Save blocked, use open policy) (Scored)	☐	☐
1.4.7.2.1.12	(L1) Ensure 'Excel 4 Workbooks' is set to Enabled (Enabled: Open/Save blocked, use open policy) (Scored)	☐	☐
1.4.7.2.1.13	(L1) Ensure 'Dif and Sylk Files' is set to Enabled (Open/Save blocked, use open policy) (Scored)	☐	☐
1.4.7.2.2	**Protected View**		
1.4.7.2.2.	(L1) Ensure 'Turn Off Protected View For Attachments Opened	☐	☐

1	from Outlook' is set to Disabled (Scored)		
1.4.7.2.2.2	(L1) Ensure 'Do Not Open Files From The Internet Zone in Protected View' is set to Disabled (Scored)	☐	☐
1.4.7.2.2.3	(L1) Ensure 'Do Not Open Files in Unsafe Locations in Protected View' is set to Disabled (Scored)	☐	☐
1.4.7.2.2.4	(L1) Ensure 'Document Behavior if File Validation Fails' is set to Enabled (Open in Protected View and Unchecked for "Do not allow edit") (Scored)	☐	☐
1.4.7.2.3	**Trusted Locations**		
1.4.7.2.3.1	(L1) Ensure 'Allow Trusted Locations on The Network' to Disabled (Scored)	☐	☐
1.4.7.2.3.2	(L1) Ensure 'Disabled all Trusted Locations' is set to Enabled (Scored)	☐	☐
1.4.7.2.4	(L1) Ensure 'Trust Access To Visual Basic Project' is set to Disabled (Scored)	☐	☐
1.4.7.2.5	(L1) Ensure 'Disable Trust Bar Notification For Unsigned Application Add-ins And Block Them' is set to Enabled (Scored)	☐	☐
1.4.7.2.6	(L1) Ensure 'Require That Application Add-ins are Signed By Trusted Publisher' is set to Enabled (Scored)	☐	☐
1.4.7.2.7	(L1) Ensure 'VBA Macro Notification Settings' is set to Enabled (Disable all Except Digitally Signed Macros) (Scored)	☐	☐
1.4.7.2.8	(L1) Ensure 'Store Macro In Personal Macro Workbook by Default' is set to Enabled (Scored)	☐	☐
1.4.7.3	(L1) Ensure 'Turn Off File Validation' is set to Disabled (Scored)	☐	☐
1.4.7.4	(L1) Ensure 'Force File Extension to Match File Type' is set to Enabled(Always match file type) (Scored)	☐	☐
1.4.7.5	(L1) Ensure' Scan Encrypted Macros in Excel Open XML Workbooks' is set to Enable (Scan encrypted macros (default)) (Scored)	☐	☐
1.5	**File Tab**		
1.5.1	**Check Accessibility**		
1.6	**Miscellaneous**		
1.6.1	**Server Settings**		

Appendix: Change History

Date	Version	Changes for this version
1-29-16	1.0.0	Initial Release – Based off of Excel 2013 v1.0.0