Center for Internet Security®

CIS Microsoft Office Word 2013 Benchmark

v1.1.0 - 09-30-2016

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 is the final release of the Microsoft Office Word 2013 Benchmark v1.1.0. CIS encourages you to migrate to a more recent, supported version of this technology.

This document, Security Configuration Benchmark for Microsoft Word 2013, provides prescriptive guidance for establishing a secure configuration posture for Microsoft Word 2013 running on Windows 7. This guide was tested against Microsoft Office 2013. 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 Word 2013 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:

Editor
Jordan Rakoske

Recommendations

1 User Configuration

1.1 Collaboration Settings

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

1.1.1 Co-Authoring

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

1.2 Customizable Error Messages

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

1.3 Disable Items in User Interface

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

1.3.1 Custom

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

1.3.2 Predefined

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

1.4 File Tab

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

1.4.1 Check Accessibility

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

1.5 Japanese Find

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

1.6 Miscellaneous

This section contains settings to configure Miscellaneous settings within Word

1.6.1 Server Settings

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

1.6.2 (L1) Ensure 'Use Online Translation Dictionaries' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to prevent online dictionaries from being used for the translation of text through the Research pane.

If you enable or do not configure this policy setting, the online dictionaries can be used to translate text through the Research pane.

If you disable this policy setting, the online dictionaries cannot be used to translate text through the Research pane. The recommended state for this setting is: `Disabled`.

Rationale:

Some organizations do not allow Internet access of any kind on certain devices or for certain users. In these instances, Internet access could violate organizational or regulatory compliance standards. For devices and users that manage extremely sensitive data Internet access can be prohibited to help prevent an attacker from gaining access to the sensitive information.

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\15.0\common\research\translation
Criteria
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Miscellaneous\Use
Online Translation Dictionaries
```

Impact:

When this policy setting is configured to Disabled, users will not be able to translate text through the Research pane by using the online dictionaries.

Default Value:

Not Configured

1.7 Review Tab

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

1.7.1 Chinese Conversion | Convert with Options

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

1.7.2 Language | Set Proofing Language...

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

1.8 Word Options

This section contains settings to configure Word options.

1.8.1 Advanced

This section contains settings to configure Advance Word options.

1.8.1.1 E-Mail Options

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

1.8.1.2 (L1) Ensure 'Custom Markup Warning' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting specifies how Word behaves when opening a document that contains custom XML markup.

If you enable this policy setting, you can set the behavior to one of the following:

- 0: Do not prompt the user and silently remove the custom XML markup.

- 1: Prompt the user regarding the loss of custom XML markup. This is the default option.

- 2: Prompt the user regarding the loss of custom XML markup, and do not allow them to suppress this prompt.

- 3: Prompt the user regarding the loss of custom XML markup, and open the file read-only.

- 4: Prompt the user regarding the loss of custom XML markup, do not allow them to suppress this prompt, and open the file read-only.

- 5: Do not prompt the user and silently remove the custom XML markup, but open the file read-only.

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

Rationale:

The removal of custom XML markup is the result of a United States court ruling on December 22, 2009. Word does not include a particular custom XML tagging implementation. Word can be configured to notify users when they are opening a document that contains custom XML markup.

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\15.0\word\options\custommarkupwarn
ing
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
Options\Advanced\Custom Markup Warning
```

Impact:

Configure this policy setting is configured to be Enabled, also select one of the following options so that the user is notified that the custom XML markup is being removed:

- 1: Prompt the user regarding the loss of custom XML markup. This is the default option.

- 2: Prompt the user regarding the loss of custom XML markup, and do not allow them to suppress this prompt.

- 3: Prompt the user regarding the loss of custom XML markup, and open the file read-only.

- 4: Prompt the user regarding the loss of custom XML markup, do not allow them to suppress this prompt, and open the file read-only.

Default Value:

Not Configured

1.8.1.3 (L1) Ensure 'Update Automatic Links at Open' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

Checks/unchecks the corresponding UI option. The recommended state for this setting is: `Disabled`.

Rationale:

By default, when user's open documents Word automatically updates any links to external content, such as graphics, Excel worksheets, and PowerPoint slides. To disable automatic updating, the user can click the Office Button, click Word Options, click Advanced, scroll to the General section, and then clear the Update automatic links at open check box.

If Word is configured to automatically update links when documents are open, document content can change without the user's knowledge, which could put important information at 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\15.0\word\options\DontUpdateLinks
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
Options\Advanced\Update Automatic Links at Open
```

Impact:

Disabling this setting might cause disruptions for users who work with Word documents that contain external content. Consider educating users on the methods for updating links manually.

Default Value:

Not Configured

1.8.2 Customized Ribbon

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

1.8.3 Display

This section contains settings to configure Word Display Settings

1.8.3.1 (L1) Ensure 'Hidden Text' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether text that is formatted as hidden displays on Word users' monitor screens.

If you enable this policy setting, Word displays hidden text at all times. Hidden text on monitor screens displays as underlined with a dotted line.

If you disable or do not configure this policy setting, Word does not display text formatted as hidden unless "Show/Hide ¶" is selected or Word is configured to show hidden text in the "Display" section of the "Word Options" dialog. The recommended state for this setting is: `Enabled`.

Rationale:

By default, Word does not display text formatted as hidden unless Show/Hide ¶ is selected or Word is configured to show hidden text in the Display section of the Word Options dialog box. If a document that contains hidden text is distributed, any sensitive information in the document could be at 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\15.0\word\options\showhiddentext
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
Options\Display\Hidden Text
```

Impact:

Enabling this setting could create issues for Word users when they format documents that contain hidden text for printing or distribution. Displaying hidden text can change the way a document flows as well as make it difficult to judge the number of pages in a document and where Word will insert automatic page breaks.

Default Value:

Not Configured

1.8.4 General

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

1.8.5 Proofing

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

1.8.6 Save

This section contains Word save options.

1.8.6.1 (L1) Ensure 'Default File Format' is set to Enabled (Word Document (.docx)) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines the default file format for saving files in Word.

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

- Word Document (*.docx): This option is the default configuration in Word.

- Single Files Web Page (*.mht)

- Web Page (*.htm; *.html)

- Web Page, Filtered (*.htm, *.html)

- Rich Text Format (*.rtf)

- Plain Text (*.txt)

- Word 6.0/95 (*.doc)

- Word 6.0/95 - Chinese (Simplified) (*.doc)

- Word 6.0/95 - Chinese (Traditional) (*.doc)

- Word 6.0/95 - Japanese (*.doc)

- Word 6.0/95 - Korean (*.doc)

- Word 97-2002 and 6.0/95 - RTF

- Word 5.1 for Macintosh (*.mcw)

- Word 5.0 for Macintosh (*.mcw)

- Word 2.x for Windows (*.doc)

- Works 4.0 for Windows (*.wps)

- WordPerfect 5.x for Windows (*.doc)

- WordPerfect 5.1 for DOS (*.doc)

- Word Macro-Enabled Document (*.docm)

- Word Template (*.dotx)

- Word Macro-Enabled Template (*.dotm)

- Word 97 - 2003 Document (*.doc)

- Word 97 - 2003 Template (*.dot)

- Word XML Document (*.xml)

- Strict Open XML Document (*.docx)

- OpenDocument Text (*.odt)

Users can choose to save presentations or documents in a different file format than the default.

If you disable or do not configure this policy setting, Word saves new files in the Office Open XML format: Word files have a .docx extension. For users who run recent versions of Word, Microsoft offers the Microsoft Office Compatibility Pack, which enables them to open and save Office Open XML files. If some users in your organization cannot install the Compatibility Pack, or are running versions of Word older than Microsoft Office 2000 with Service Pack 3, they might not be able to access Office Open XML files.

This policy setting is often set in combination with the "Save As Open XML in Compatibility Mode" policy setting. The recommended state for this setting is: `Enabled. (Word Document (.docx))`

Rationale:

By default, when users create new document files, Word saves them in the new Word format. Users can change this functionality by clicking the Office button, clicking Word 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 document 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 Word 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\15.0\word\options\defaultformat
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
Options\Save\Default File Format
```

Impact:

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

Default Value:

Not Configured

1.8.7 Security

This section contains settings to configure Security Options.

1.8.7.1 Cryptography

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

1.8.7.2 Trust Center

This section contains settings to configure Trust Center within Word.

1.8.7.2.1 File Block Settings

This Section contains settings for configuring File Block settings.

1.8.7.2.1.1 (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 Word 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`.

Rationale:

By default, users can open, view, or edit a large number of file types in Word. 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\15.0\word\security\fileblock\openi
nprotectedview
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
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 Word. 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

1.8.7.2.1.2 (L1) Ensure 'Word 2 and Earlier Binary Documents 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 Word 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 Word. 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\15.0\word\security\fileblock\word2 files
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word Options\Security\Trust Center\File Block Settings\Word 2 and Earlier Binary Documents 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

1.8.7.2.1.3 (L1) Ensure 'Word 6.0 Binary Documents 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 Word 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 Word. 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\15.0\word\security\fileblock\word60files
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word Options\Security\Trust Center\File Block Settings\Word 6.0 Binary Documents 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. For more information, see Plan file block settings for Office at http://technet.microsoft.com/en-us/library/cc179230.aspx.

Default Value:

Not Configured

1.8.7.2.1.4 (L1) Ensure 'Word 95 Binary Documents 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 Word 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 Word. 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\15.0\word\security\fileblock\word95files
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word Options\Security\Trust Center\File Block Settings\Word 95 Binary Documents 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

1.8.7.2.1.5 (L1) Ensure 'Word 97 Binary Documents 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 Word 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 Word. 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\15.0\word\security\fileblock\word97files
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word Options\Security\Trust Center\File Block Settings\Word 97 Binary Documents 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

1.8.7.2.2 Protected View

This section contains settings to configure Protected view options.

1.8.7.2.2.1 (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\15.0\word\security\protectedview\d
isableinternetfilesinpv
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
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

1.8.7.2.2.2 (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\15.0\word\security\protectedview\d
isableunsafelocationsinpv
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
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

1.8.7.2.2.3 (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 Word 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 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\15.0\word\security\protectedview\disableattachmentsinpv
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word Options\Security\Trust Center\Protected View\Turn Off Protected View for Attachments Opened from Outlook
```

Impact:

Opening Office files, such as the Office 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 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

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

Profile Applicability:

- Level 1

Description:

This 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) 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\15.0\word\security\filevalidation\
disableeditfrompv
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
Options\Security\Trust Center\Protected View\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

1.8.7.2.3 Trusted Locations

This section contains settings to configure Trusted Locations.

1.8.7.2.3.1 (L1) Ensure 'Allow Trusted Locations on the Network' is set 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\15.0\word\security\trusted
locations\allownetworklocations
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
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

1.8.7.2.3.2 (L1) Ensure 'Disable 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 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\15.0\word\security\trusted
locations\alllocationsdisabled
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
Options\Security\Trust Center\Trusted Locations\Disable 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

1.8.7.2.4 (L1) Ensure 'Scan Encrypted Macros in Word Open XML Documents' to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether encrypted macros in Open XML documents 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`.

Rationale:

When an Office Open XML document is rights-managed or password protected, any macros that are embedded in the document 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 the default configuration is changed, Word will not require encrypted macros to be scanned before loading. Word will handle them as specified by the Office 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\15.0\word\security\wordbypassencry
ptedmacroscan
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
Options\Security\Trust Center\Scan Encrypted Macros in Word Open XML Documents
```

Impact:

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

Default Value:

Not Configured

1.8.7.2.5 (L1) Ensure 'Disable Trust Bar Notification for Unsigned Application Add-ins and Block Them' to Enable (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether the specified Office application notifies 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 this 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\15.0\word\security\notbpromptunsignedaddin
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
Options\Security\Trust Center\Disable Trust Bar Notification for Unsigned Application
Add-ins and Block Them
```

Impact:

This setting only applies if the Office 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

1.8.7.2.6 (L1) Ensure 'Require That Application Add-ins Are Signed By Trusted Publisher' to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether add-ins for this applications must be digitally signed by a trusted publisher.

If you enable this policy setting, this application checks 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, this application disables the add-in and notifies the user. Microsoft provides four certificates for Office, 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. 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. 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 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. For more information about trusted publishers, see the Office Resource Kit.

If you disable or do not configure this policy setting, this application does not check the digital signature on application add-ins before opening them. If a dangerous add-in is loaded, it could harm users' computers or compromise data security. The recommended state for this setting is: `Enabled`.

Rationale:

By default, Office 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\15.0\word\security\requireaddinsig
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
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.

Office 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. Office still reads trusted publisher certificate information from the Office trusted publisher store, but 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 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.

Default Value:

Not Configured

1.8.7.2.7 (L1) Ensure 'Trust Access to Visual Basic Project' 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, 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.

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\15.0\word\security\accessvbom
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
Options\Security\Trust Center\Trust Access to Visual Basic Project
```

Impact:

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

Default Value:

Not Configured

1.8.7.2.8 (L1) Ensure 'VBA Macro Notification Settings' to Enabled (Disable all Except Digitally Signed) (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)`

Rationale:

By default, when user's open files in Word that contain VBA macros, Word 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\15.0\word\security\vbawarnings
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
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

1.8.7.3 (L1) Ensure 'Make Hidden Markup Visible' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

Checks/unchecks the corresponding UI option. The recommended state for this setting is: `Enabled`.

Rationale:

Users may leave sensitive information in a Word document and distribute it outside of their trusted circle without realizing that this information is still present in the document.

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\15.0\word\options\showmarkupopensa
ve
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
Options\Security\Make Hidden Markup Visible
```

Impact:

Hidden markup includes revision marks. If a document has a large number of revision marks and comments, it may be difficult to read until those marks are accepted and/or removed. Users will hae to know how to rehide the revisions to read the document easily.

Default Value:

Not Configured

1.8.7.4 (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\15.0\word\security\filevalidation\
enableonload
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
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

1.8.7.5 (L1) Ensure 'Warn Before Printing, Saving or Sending a File That Contains Tracked Changes or Comments' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

Checks/unchecks the corresponding UI option. The recommended state for this setting is: `Enabled`.

Rationale:

Tracked changes or comments embedded within a document may contain sensitive, insulting, or embarrassing information that the document owner forgot that she or one of the other contributors or reviewers had placed there.

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\15.0\word\options\warnrevisions
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Word 2013\Word
Options\Security\Warn Before Printing, Saving or Sending a File That Contains Tracked
Changes or Comments
```

Impact:

Enabling this setting can cause users to see a warning dialog frequently if they use tracked changes or comments in many of their documents, which could be frustrating to them.

Default Value:

Not Configured

1.8.8 Track Changes and Compare

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

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**User Configuration**		
1.1	**Collaboration Settings**		
1.1.1	**Co-Authoring**		
1.2	**Customizable Error Messages**		
1.3	**Disable Items in User Interface**		
1.3.1	**Custom**		
1.3.2	**Predefined**		
1.4	**File Tab**		
1.4.1	**Check Accessibility**		
1.5	**Japanese Find**		
1.6	**Miscellaneous**		
1.6.1	**Server Settings**		
1.6.2	(L1) Ensure 'Use Online Translation Dictionaries' is set to Disabled (Scored)	☐	☐
1.7	**Review Tab**		
1.7.1	**Chinese Conversion | Convert with Options**		
1.7.2	**Language | Set Proofing Language...**		
1.8	**Word Options**		
1.8.1	**Advanced**		
1.8.1.1	**E-Mail Options**		
1.8.1.2	(L1) Ensure 'Custom Markup Warning' is set to Enabled (Scored)	☐	☐
1.8.1.3	(L1) Ensure 'Update Automatic Links at Open' is set to Disabled (Scored)	☐	☐
1.8.2	**Customized Ribbon**		
1.8.3	**Display**		
1.8.3.1	(L1) Ensure 'Hidden Text' is set to Enabled (Scored)	☐	☐
1.8.4	**General**		
1.8.5	**Proofing**		
1.8.6	**Save**		
1.8.6.1	(L1) Ensure 'Default File Format' is set to Enabled (Word Document (.docx)) (Scored)	☐	☐
1.8.7	**Security**		
1.8.7.1	**Cryptography**		
1.8.7.2	**Trust Center**		
1.8.7.2.1	**File Block Settings**		
1.8.7.2.1.1	(L1) Ensure 'Default File Block Behavior' is set to Enabled	☐	☐

	(Blocked files are not opened) (Scored)		
1.8.7.2.1.2	(L1) Ensure 'Word 2 and Earlier Binary Documents and Templates' is set to Enabled (Open/Save blocked, use open policy) (Scored)	☐	☐
1.8.7.2.1.3	(L1) Ensure 'Word 6.0 Binary Documents and Templates' is set to Enabled (Open/Save blocked, use open policy) (Scored)	☐	☐
1.8.7.2.1.4	(L1) Ensure 'Word 95 Binary Documents and Templates' is set to Enabled (Open/Save Blocked, Use Open Policy) (Scored)	☐	☐
1.8.7.2.1.5	(L1) Ensure 'Word 97 Binary Documents and Templates' is set to Enabled (Open/Save Blocked, Use Open Policy) (Scored)	☐	☐
1.8.7.2.2	**Protected View**		
1.8.7.2.2.1	(L1) Ensure 'Do Not Open Files From The Internet Zone in Protected View' is set to Disabled (Scored)	☐	☐
1.8.7.2.2.2	(L1) Ensure 'Do Not Open Files in Unsafe Locations in Protected View' is set to Disabled (Scored)	☐	☐
1.8.7.2.2.3	(L1) Ensure 'Turn Off Protected View for Attachments Opened From Outlook' is set to Disabled (Scored)	☐	☐
1.8.7.2.2.4	(L1) Ensure 'Document Behavior if File Validation Fails' is set to Enabled (Open in Protected View) Unchecked for "Do not allow edit" (Scored)	☐	☐
1.8.7.2.3	**Trusted Locations**		
1.8.7.2.3.1	(L1) Ensure 'Allow Trusted Locations on the Network' is set to Disabled (Scored)	☐	☐
1.8.7.2.3.2	(L1) Ensure 'Disable All Trusted Locations' is set to Enabled (Scored)	☐	☐
1.8.7.2.4	(L1) Ensure 'Scan Encrypted Macros in Word Open XML Documents' to Enabled (Scored)	☐	☐
1.8.7.2.5	(L1) Ensure 'Disable Trust Bar Notification for Unsigned Application Add-ins and Block Them' to Enable (Scored)	☐	☐
1.8.7.2.6	(L1) Ensure 'Require That Application Add-ins Are Signed By Trusted Publisher' to Enabled (Scored)	☐	☐
1.8.7.2.7	(L1) Ensure 'Trust Access to Visual Basic Project' to Disabled (Scored)	☐	☐
1.8.7.2.8	(L1) Ensure 'VBA Macro Notification Settings' to Enabled (Disable all Except Digitally Signed) (Scored)	☐	☐
1.8.7.3	(L1) Ensure 'Make Hidden Markup Visible' is set to Enabled (Scored)	☐	☐
1.8.7.4	(L1) Ensure 'Turn Off File Validation' is set to Disabled (Scored)	☐	☐
1.8.7.5	(L1) Ensure 'Warn Before Printing, Saving or Sending a File That Contains Tracked Changes or Comments' is set to Enabled (Scored)	☐	☐

1.8.8	Track Changes and Compare

Appendix: Change History

Date	Version	Changes for this version
08-05-15	v1.0.0	Initial Release
09-30-16	v1.0.0	1.8.7.4 (L1) Ensure 'Turn Off File Validation' is set to Disabled (Scored) Ticket #10
09-30-16	v1.1.0	Changed Recommendation Structure to match 2016 and to conform with CIS Standard.
09-30-16	v1.1.0	Changed Title Structure to conform with CIS Standard.