Center for Internet Security®

CIS Microsoft Office 2016 Benchmark

v1.1.0 - 11-30-2016

Table of Contents

Overview

This document, Security Configuration Benchmark for Microsoft Office 2016, provides prescriptive guidance for establishing a secure configuration posture for Microsoft Office 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 Office 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:

Editor
Jordan Rakoske

Recommendations

1 Computer Configuration

1.1 Miscellaneous

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

1.2 Security Settings

This section contains settings to configure Security Settings.

1.2.1 IE Security

This section contains settings to configure IE Security.

1.2.1.1 (L1) Ensure 'Protection From Zone Elevation' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)

Profile Applicability:

- Level 1

Description:

Zone Elevation

The recommended state for this setting is: `Enabled`. (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe)

Rationale:

Internet Explorer places restrictions on each web page that users can use the browser to open. Web pages on a user's local computer have the fewest security restrictions and reside in the Local Machine zone, making this security zone a prime target for malicious users and code.

Disabling or not configuring this setting could allow pages in the Internet zone to navigate to pages in the Local Machine zone to then run code to elevate privileges. This could allow malicious code or users 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:

```
HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation\"Office Application.exe"
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Security Settings\IE Security\Protection From Zone Elevation
```

Impact:

Websites that rely on navigation to other higher privileged sites may not properly function. To allow such websites to properly function, use Group Policy to add them to the Trusted sites zone.

Note Enabling this setting also disables JavaScript navigation if no security context is present.

Default Value:

Not Configured

1.2.1.2 (L1) Ensure 'Mime Sniffing Safety Feature' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether Internet Explorer MIME sniffing prevents promotion of a file of one type to a more dangerous file type. For example, it does not allow script to run from a file marked as text.

For Office, this setting is affects any web-based content that is accessed within Office. The recommended state for this setting is: `Enabled`. `(Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe)`

Rationale:

MIME file-type spoofing is a potential threat to your organization. It is recommended that you ensure these files are consistently handled to help prevent malicious file downloads that may infect your 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:

```
HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing\"Office Application.exe"
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Security Settings\IE Security\Mime Sniffing Safety Feature
```

Impact:

When set to Enabled, MIME sniffing will not promote a file of one type to a more dangerous file type. If you disable this policy setting, MIME sniffing configures Internet Explorer processes to allow promotion of a file from one type to a more dangerous file type. For example, a text file could be promoted to an executable file, which is dangerous because any code in the supposed text file would be executed.

Default Value:

Not Configured

1.2.1.3 (L1) Ensure 'Information Bar' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether the Information Bar is displayed for Internet Explorer processes when file or code installs are restricted. By default, the Information Bar is displayed for Internet Explorer processes. The recommended state for this setting is: `Enabled`. `(Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe)`

Rationale:

The information bar can help users to understand when potentially malicious content has been blocked, on the other hand, some users may be confused by the appearance of the bar or unsure how to respond.

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:

```
HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_securityband\"Office Application.exe"
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Security Settings\IE Security\Information Bar
```

Impact:

The security bar will be enabled for each of the specified applications.

Default Value:

Not Configured

1.2.1.4 (L1) Ensure 'Bind to Object' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)

Profile Applicability:

- Level 1

Description:

This setting determines whether Microsoft Internet Explorer performs its typical safety checks on Microsoft ActiveX® controls when opening URLs that are passed to it by an Office application. By default, Internet Explorer performs additional safety checks when ActiveX controls are initialized. Specifically, it prevents the control from being created if the kill bit is set in the registry. It also checks the security settings for the zone of the URL in which the control is instantiated to determine whether the control can be safely initialized. For the same behavior of the selectable applications, such as Excel and Word when they instantiate the use of Internet Explorer, the policy must be Enabled and the applications selected. The recommended state for this setting is: `Enabled. (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe)`

Rationale:

Internet Explorer performs a number of safety checks before initializing an ActiveX control. It will not initialize a control if the kill bit for the control is set in the registry, or if the security settings for the zone in which the control is located do not allow it to be initialized.

This functionality can be controlled separately for instances of Internet Explorer spawned by Office applications (for example, if a user clicks a link in an Office document or selects a menu option that loads a Web page). A security risk could occur if potentially dangerous controls are allowed to load.

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:

```
HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject\"Office Application.exe"
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Security Settings\IE Security\Bind to Object
```

Impact:

Enabling this setting can cause some disruptions for users who open Web pages that contain potentially dangerous ActiveX controls from Office applications. However, because any affected controls are usually blocked by default when Internet Explorer opens Web pages, most users should not experience significant usability issues.

Default Value:

Not Configured

1.2.1.5 (L1) Ensure 'Restrict File Download' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)

Profile Applicability:

- Level 1

Description:

Restrict File Download.

The recommended state for this setting is: `Enabled`. `(Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe)`

Rationale:

Disabling this setting allows websites to present file download prompts via code without the user specifically initiating the download. User preferences may also allow the download to occur without prompting or interacting with the user. Even if Internet Explorer prompts the user to accept the download, some websites abuse this functionality. Malicious websites may continually prompt users to download a file or present confusing dialog boxes to trick users into downloading or running a file.

If the download occurs and it contains malicious code, the 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:

```
HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload\"Office Application.exe"
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Security Settings\IE Security\Restrict File Download
```

Impact:

User initiated downloads can still occur so the majority of legitimate user download interactions remain unaffected. Hiding website-initiated prompt messages makes it impossible for a malicious website to initiate a download by itself. Such a site can no longer confuse a user into downloading a file that could then open on the user's computer to execute an attack.

However, some valid websites may initiate file downloads. If this setting is enabled, users cannot view download prompts, and remain unaware when a download is available. If such sites reside in an organization's intranet, they should display a link to prompt users to initiate valid downloads if the automatic download process does not occur. This type of functionality is already in common use on many major internet sites and should not confuse users.

It is possible that some advanced users may expect their user preferences to control this behavior, and for this reason, they may be confused when this preference is overridden by this setting.

Default Value:

Not Configured

1.2.1.6 (L1) Ensure 'Saved from URL' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls whether Internet Explorer evaluates URLs passed to it by Office applications for Mark of the Web (MOTW) comments. The recommended state for this setting is: `Enabled.(Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe)`

Rationale:

Typically, when Internet Explorer loads a Web page from a UNC share that contains a Mark of the Web (MOTW) comment that indicates the page was saved from a site on the Internet, Internet Explorer runs the page in the Internet security zone instead of the less restrictive Local Intranet security zone. This functionality can be controlled separately for instances of Internet Explorer spawned by Office applications (for example, if a user clicks a link in an Office document or selects a menu option that loads a Web page). If Internet Explorer does not evaluate the page for a MOTW, potentially dangerous code could be allowed to run.

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:

```
HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck\"Office Application.exe"
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Security Settings\IE Security\Saved from URL
```

Impact:

Enabling this setting can cause some Web pages saved on UNC shares to run in a more restrictive security zone when opened from Office applications than they would if the setting were disabled or not configured. However, a page with a MOTW indicating it was saved from an Internet site is presumed to have been designed to run in the Internet zone in the first place, so most users should not experience significant usability issues.

Default Value:

Not Configured

1.2.1.7 (L1) Ensure 'Disable User Name and Password' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls whether Internet Explorer opens URLs containing user information that are passed to it by an Office application. The recommended state for this setting is: `Enabled.(Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe)`

Rationale:

The Uniform Resource Locator (URL) standard allows user authentication to be included in URL strings in the form http://username:password@example.com. A malicious user might use this URL syntax to create a hyperlink that appears to open a legitimate Web site but actually opens a deceptive (spoofed) Web site. For example, the URL http://www.wingtiptoys.com@example.com appears to open http://www.wingtiptoys.com but actually opens http://example.com. To protect users from such attacks, Internet Explorer usually blocks any URLs using this syntax.

This functionality can be controlled separately for instances of Internet Explorer spawned by Office applications (for example, if a user clicks a link in an Office document or selects a menu option that loads a Web page). If user names and passwords in URLs are allowed, users could be diverted to dangerous Web pages, which could pose 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:

```
HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable\"Office
Application.exe"
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Security Settings\IE Security\Disable User Name and Password
```

Impact:

Enabling this setting can cause some disruptions for users who open URLs containing user authentication information from Office applications. Because such URLs are blocked by default when Internet Explorer opens Web pages through conventional means, however, most users should not experience significant usability issues.

Default Value:

Not Configured

1.2.1.8 (L1) Ensure 'Scripted Window Security Restrictions' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)

Profile Applicability:

- Level 1

Description:

Window Restrictions. The recommended state for this setting is: `Enabled.(Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe)`

Rationale:

Malicious websites often try to confuse or trick users into giving a site permission to perform an action that allows the site to take control of the users' computers in some manner. Disabling or not configuring this setting allows unknown websites to:

• Create browser windows that appear to be from the local operating system.

• Draw active windows that display outside of the viewable areas of the screen that can capture keyboard input.

• Overlay parent windows with their own browser windows to hide important system information, choices, or prompts.

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:

```
HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_window_restrictions\"Office Application.exe"
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Security Settings\IE Security\Scripted Window Security Restrictions
```

Impact:

It is unlikely that any valid applications would use such deceptive methods to accomplish a task. For this reason, it is unlikely that organization may encounter any major limitations due to using this setting.

Default Value:

Not Configured

1.2.1.9 (L1) Ensure 'Local Machine Zone Lockdown Security' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)

Profile Applicability:

- Level 1

Description:

When Internet Explorer opens a Web page, it places restrictions on what the page can do, based on the page's Internet Explorer security zone. There are several possible security zones, each with different sets of restrictions. The security zone for a page is determined by its location. For example, pages that are located on the Internet will normally be in the more restrictive Internet security zone. They might not be allowed to perform some operations, such as accessing the local hard drive. Pages that are located on your corporate network would normally be in the Intranet security zone, and have fewer restrictions.

This setting allows you to configure policy settings in the zone consistent with a selected security level, for example, Low, Medium Low, Medium, or High. The recommended state for this setting is: `Enabled.(Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe)`

Rationale:

Local Machine zone security applies to all local files and content. This feature helps to mitigate attacks where the Local Machine zone is used as an attack vector to load malicious HTML code.

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:

```
HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown\"Office Application.exe"
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Security Settings\IE Security\Local Machine Zone Lockdown Security
```

Impact:

If you enable this policy setting, the Local Machine zone security applies to all local files and content processed by the specified applications. If you disable or do not configure this policy setting, Local Machine zone security is not applied to local files or content processed by the specified applications.

Default Value:

Not Configured

1.2.1.10 (L1) Ensure 'Object Caching Protection' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting defines whether a reference to an object is accessible when the user navigates within the same domain or to a new domain. For Office, this applies to URL accessed within Office applications. By default in Internet Explorer, a reference to an object is no longer accessible when the user browses to a new domain. There is a new security context for all scriptable objects so that access to all cached objects is blocked. Additionally, access is blocked when browsing within the same domain (fully qualified domain name). A reference to an object is no longer accessible after the context has changed due to navigation. The recommended state for this setting is: `Enabled.(Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe)`

Rationale:

A malicious website may try to use object references from other domains.

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:

```
HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching\"Office Application.exe"
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Security Settings\IE Security\Object Caching Protection
```

Impact:

If you enable this policy setting, object reference is no longer accessible when navigating within or across domains for each specified application. If you disable or do not configure this policy setting, object reference is retained when navigating within or across domains in the Restricted Zone sites.

Default Value:

Not Configured

1.2.1.11 (L1) Ensure 'Consistent Mime Handling' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)

Profile Applicability:

- Level 1

Description:

Internet Explorer uses Multipurpose Internet Mail Extensions (MIME) data to determine file handling procedures for files received through a Web server. This policy setting determines whether Internet Explorer requires that all file-type information provided by Web servers be consistent.

For example, if the MIME type of a file is text/plain but the MIME data indicates that the file is really an executable file, Internet Explorer changes its extension to reflect this executable status. This capability helps ensure that executable code cannot masquerade as other types of data that may be trusted. The recommended state for this setting is: `Enabled.(Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe)`

Rationale:

Users can use Internet Explorer to unknowingly download malicious content disguised with an incorrect filename extension or incorrectly marked in the MIME header. Once downloaded, an incorrect handler can run the file, enabling the malicious content to cause damage to the users system or 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:

```
HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling\"Office Application.exe"
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Security Settings\IE Security\Consistent Mime Handling
```

Impact:

Internet Explorer use both the extension of the filename and the MIME information to decide how to handle a file. Enabling this setting requires that information in the MIME header matches the file extension provided. Since mismatched files will be blocked by enabling this setting, you should insure that any web server under your control is set up correctly.

Default Value:

Not Configured

1.2.1.12 (L1) Ensure 'Add-on Management' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)

Profile Applicability:

- Level 1

Description:

Add-on Management. The recommended state for this setting is: `Enabled.(Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe)`

Rationale:

Internet Explorer add-ons are pieces of code that run in Internet Explorer to provide additional functionality. Rogue add-ons may contain viruses or other malicious code.

Disabling or not configuring this setting could allow malicious code or users to become active on user computers or the network. For example, a malicious user can monitor and then use keystrokes that a user types into Internet Explorer. Even legitimate add-ons may demand resources that compromise the performance of Internet Explorer and the operating systems of user computers.

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:

```
HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_addon_management\"Office Application.exe"
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Security Settings\IE Security\Add-on Management
```

Impact:

Some legitimate programs, including ones from Microsoft, use add-ons to display documents, audio, and video in Internet Explorer. The organization's Group Policy should incorporate approved, commonly-used add-ons to avoid limiting important user functionality.

Default Value:

Not Configured

1.2.1.13 (L1) Ensure 'Navigate URL' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls whether Internet Explorer attempts to load malformed URLs that are passed to it from Office applications. The recommended state for this setting is: `Enabled.(Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe)`

Rationale:

To protect users from attacks, Internet Explorer usually does not attempt to load malformed URLs. This functionality can be controlled separately for instances of Internet Explorer spawned by Office applications (for example, if a user clicks a link in an Office document or selects a menu option that loads a Web page). If Internet Explorer attempts to load a malformed URL, a security risk could occur in some cases.

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:

```
HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_validate_navigate_url\"Office Application.exe"
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Security Settings\IE Security\Navigate URL
```

Impact:

Enabling this setting does not block any legitimate URLs, and is therefore unlikely to cause usability issues for any Office users.

Default Value:

Not Configured

1.2.1.14 (L1) Ensure 'Restrict ActiveX Install' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)

Profile Applicability:

- Level 1

Description:

Restrict ActiveX Install. The recommended state for this setting is: `Enabled.(Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe)`

Rationale:

Microsoft ActiveX controls allow unmanaged, unprotected code to run on the user computers. ActiveX controls do not run within a protected container in the browser like other types of HTML or Microsoft Silverlight-based controls.

Disabling or not configuring this setting does not block prompts for ActiveX control installations and these prompts display to users. 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:

```
HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_activexinstall\"Office Application.exe"
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Security Settings\IE Security\Restrict ActiveX Install
```

Impact:

Microsoft ActiveX controls allow unmanaged, unprotected code to run on the user computers. ActiveX controls do not run within a protected container in the browser like other types of HTML or Microsoft Silverlight-based controls.

Disabling or not configuring this setting does not block prompts for ActiveX control installations and these prompts display to users. This could allow malicious code to become active on user computers or the network.

Default Value:

Not Configured

1.3 Updates

This section contains settings to configure Updates.

1.3.1 (L1) Ensure 'Enable Automatic Updates' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether the Office automatic updates are enabled or disabled for all Office products installed by using Click-to-Run. This policy has no effect on Office products installed via Windows Installer.

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

Rationale:

Security updates help prevent malicious attacks on Office applications. Timely application of Office updates helps ensure the security of devices and the applications running on the devices. Without these updates, devices and the applications running on those devices are more susceptible to security 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:

```
HKLM\software\policies\microsoft\office\16.0\common\officeupdate\enableautomaticupdate
s
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Updates\Enable Automatic Updates
```

Impact:

Office updates for Click-to-Run installations of Microsoft Office are applied in the background and have no adverse effect on users.

Default Value:

Not Configured

1.3.2 (L1) Ensure 'Hide Option to Enable or Disable Updates' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to hide the user interface (UI) options to enable or disable Office automatic updates from users. These options are found in the Product Information area of all Office applications installed via Click-to-Run. This policy setting has no effect on Office applications installed via Windows Installer.

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

Rationale:

Security updates help prevent malicious attacks on Office applications. Timely application of Office updates helps ensure the security of devices and the applications running on the devices. Without these updates, devices and the applications running on those devices are more susceptible to security attacks.

Enabling this policy setting helps prevent users from disabling automatic updates for Office.

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:

```
HKLM\software\policies\microsoft\office\16.0\common\officeupdate\hideenabledisableupda
tes
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Microsoft Office 2016
(Machine)\Updates\Hide Option to Enable or Disable Updates
```

Impact:

Office updates for Click-to-Run installations of Microsoft Office are applied in the background and have no adverse effect on users.

Default Value:

Not Configured

1.4 Volume Activation

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

2 User Configuration

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

2.1 Business Data

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

2.1.1 Database

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

2.1.2 Synchronization

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

2.1.3 Web Service

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

2.2 Collaboration Settings

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

2.2.1 Co-Authoring

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

2.2.2 Default Message Text for a reply...

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

2.2.3 Default Message Text for a Review Request...

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

2.3 Contact Card

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

2.3.1 Contact Card

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

2.4 Customizable Error Messages

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

2.5 Disable Items in User Interface

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

2.6 DLP

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

2.7 Document Information Panel

This sections contains settings to configure Document Information Panel.

2.7.1 (L1) Ensure 'Document Information Panel Beaconing UI' is set to Enabled (Always show UI) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether users see a security warning when they open custom Document Information Panels that contain a Web beaconing threat. InfoPath can be used to create custom Document Information Panels that can be attached to Excel workbooks, PowerPoint presentations, and Word documents.

The recommended state for this setting is: `Enabled. (Always show UI)`

Rationale:

InfoPath can be used to create custom Document Information Panels that can be attached to Excel workbooks, PowerPoint presentations, and Word documents.

A malicious user could insert a Web beacon into an InfoPath form that is used to create a custom Document Information Panel. Web beacons can be used to contact an external server when users open the form. Information could be gathered by the form, or information entered by users could be sent to an external server and cause them to be vulnerable to additional 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\common\documentinformationpanel\beaconing
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Document Information Pane\Document Information Panel Beaconing UI
```

Impact:

Enabling this setting and selecting "Always show UI" from the drop-down menu can cause some disruptions for users who often open documents containing custom Document Information Panels.

Default Value:

Not Configured

2.8 Downloading Framework Components

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

2.9 File Open/Save Dialog Box

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

2.9.1 Places Bar Locations

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

2.9.2 Restricted Browsing

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

2.10 First Run

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

2.11 Global Options

This section contains settings for configuring Global Options.

2.11.1 Customize

This section contains settings to configure Customize settings within Office.

2.11.1.1 Shared Workspace

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

2.11.1.1.1 Define Shared Workspace URL's

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

2.11.1.2 (L1) Ensure 'Disable UI Extending from Documents and Templates' is set to Enabled (Disallow in Access, Excel, InfoPath, Outlook, PowerPoint, Publisher, Word) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Office applications load any custom user interface (UI) code included with a document or template. Office allows developers to extend the UI with customization code that is included in a document or template.

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

Rationale:

The Office release allows developers to extend the UI with customization code that is included in a document or template. If the customization code is written by an inexperienced or malicious developer, it could limit the accessibility or availability of important application commands. Commands could also be added that launch macros that contain malicious code.

By default, Office applications load any UI customization code included with a document or template when opening it.

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\common\toolbars\"Office
Application Name"\noextensibilitycustomizationfromdocument
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Global
Options\Customize\Disable UI Extending from Documents and Templates
```

Impact:

Enabling this setting will prevent developers from using documents and templates to extend the UI, which some organizations do to increase user productivity. If your organization makes use of a modified UI, it might not be feasible for you to enable this setting. Sometimes only specific teams in an organization require a modified UI, and this setting could be enabled for the rest of the organization.

Default Value:

Not Configured

2.12 Graph Settings

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

2.13 Help

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

2.14 IME (Japanese)

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

2.15 Improved Error Reporting

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

2.16 Language Preferences

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

2.16.1 Display Language

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

2.16.2 Editing Languages

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

2.16.2.1 Enabled Editing Languages

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

2.17 Manage Restricted Permissions

This section contains setting to configure Manage Restricted Permissions.

2.17.1 (L1) Ensure 'Prevent Users From Changing Permissions on Rights Managed Content' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Office users can change permissions for content that is protected with Information Rights Management (IRM).

The Information Rights Management feature of Office allows individuals and administrators to specify access permissions to Word documents, Excel workbooks, PowerPoint presentations, InfoPath templates and forms, and Outlook e-mail messages. This functionality helps prevent sensitive information from being printed, forwarded, or copied by unauthorized people.

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

Rationale:

The Information Rights Management feature of the Office release allows individuals and administrators to specify access permissions to Word documents, Excel workbooks, PowerPoint presentations, InfoPath templates and forms, and Outlook e-mail messages. This functionality helps prevent sensitive information from being printed, forwarded, or copied by unauthorized people.

This setting can be used to prevent Office users from changing the IRM permissions of a document. If this setting is Enabled, users can open and edit documents for which they have the appropriate permissions, but they cannot create new rights-managed content, add IRM to existing documents, change existing IRM permissions, or remove IRM from documents. This configuration can prevent users from making effective use of IRM to protect documents

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\common\drm\disablecreation
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Manage Restricted
Permissions\Prevent Users From Changing Permissions on Rights Managed Content
```

Impact:

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

Default Value:

Not Configured

2.17.2 (L1) Ensure 'Never Allow Users to Specify Groups When Restricting Permission for Documents' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Office users can assign permissions to distribution lists when using Information Rights Management.

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

Rationale:

By default, Office users can specify distribution lists when using Information Rights Management (IRM) to restrict access to Excel workbooks, InfoPath templates, Outlook e-mail messages, PowerPoint presentations, or Word documents. If users are not fully aware of the distribution list's membership before assigning it permission to open or modify a document, sensitive information 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\16.0\common\drm\neverallowdls
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Manage Restricted Permissions\Never Allow Users to Specify Groups When Restricting Permission for Documents
```

Impact:

Enabling this setting could cause some disruptions for Office users who are accustomed to specifying distribution groups when defining permissions for a document. These users will have to list users individually in the Permission dialog box to assign them permission to read or modify the document. Users who do not use Information Rights Management will not be affected by this setting.

Default Value:

Not Configured

2.17.3 (L1) Ensure 'Always Require Users to Connect to Verify Permission' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether users are required to connect to the Internet or a local network to have their licenses confirmed every time they attempt to open Excel workbooks, InfoPath forms or templates, Outlook e-mail messages, PowerPoint presentations, or Word documents that are protected by Information Rights Management (IRM). This policy is useful if you want to log the usage of files with restricted permissions on the server.

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

Rationale:

By default, users are not required to connect to the network to verify permissions. If users do not need their licenses confirmed when attempting to open Office documents, they might be able to access documents after their licenses have been revoked. Also, it is not possible to log the usage of files with restricted permissions if users' licenses are not confirmed.

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\common\drm\requireconnection
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Manage Restricted
Permissions\Always Require Users to Connect to Verify Permission
```

Impact:

Enabling this setting could create problems for users who need to open rights-managed files when they are not connected to the Internet, such as mobile users. Consider surveying

your organization to determine users' need for offline use of rights-managed files before enabling this setting.

Default Value:

Not Configured

2.17.4 (L1) Ensure 'Always Expand Groups in Office When Restricting Permission for Documents' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether group names automatically expand to display all the members of the group when selected in the Permissions dialog box.

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

Rationale:

By default, when users select a group name while applying Information Rights Management (IRM) permissions to Excel workbooks, InfoPath templates, Outlook e-mail messages, PowerPoint presentations, or Word documents in the Permissions dialog box, the members of the group are not displayed. This functionality can make it possible for users to unknowingly give read or change permissions to inappropriate people.

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\common\drm\autoexpanddls\auto
expanddlsenable
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Manage Restricted
Permissions\Always Expand Groups in Office When Restricting Permission for Documents
```

Impact:

Enabling this setting changes the way the Permissions dialog box displays names, but should not create significant usability issues for most users.

Default Value:

Not Configured

2.17.5 (L1) Ensure 'Allow Users With Earlier Versions of Office to Read with Browsers...." is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting will allow users with earlier versions of Office to read documents with browsers supporting Information Rights Management.

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

Rationale:

The Windows Rights Management Add-on for Internet Explorer provides a way for users who do not use the Office release to view, but not alter, files with restricted permissions. By default, IRM-enabled files are saved in a format that cannot be viewed by using the Windows Rights Management Add-on. If this setting is enabled, an embedded rights-managed HTML version of the content is saved with each IRM-enabled file, which can be viewed in Internet Explorer using the add-on. This configuration increases the size of rights-managed files, in some cases significantly.

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\common\drm\includehtml
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Manage Restricted
Permissions\Allow Users With Earlier Versions of Office to Read with Browsers....
```

Impact:

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

Default Value:

Not Configured

2.18 Microsoft Office Document Cache

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

2.19 Microsoft Office SmartArt

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

2.20 Microsoft Save as PDF and XPS add-ins

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

2.21 Miscellaneous

This section contains settings to configure Miscellaneous settings.

2.21.1 Workflow Cache

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

2.21.2 (L1) Ensure 'Control Blogging' is set to Enabled (All Blogging Disabled) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether users can compose and post blog entries from Word.

The recommended state for this setting is: `Enabled. (All Blogging Disabled)`

Rationale:

The blogging feature in Word enables users to compose blog entries and post them to their blogs directly from Word, without using any additional software.

By default, users can post blog entries to any compatible blogging service provider, including Windows Live Spaces, Blogger, a SharePoint or Community Server site, and others. If your organization has policies that govern the posting of blog entries, allowing users to access the blogging feature in Word might enable them to violate those policies.

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\common\blog\disableblog
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office
2016\Miscellaneous\Control Blogging
```

Impact:

Disabling the blogging feature in Word may cause disruptions for users who use Word to compose and post blog entries. Any users who have a legitimate need to post blog entries will have to use another tool.

Default Value:

Not Configured

2.21.3 (L1) Ensure 'Block Signing into Office' is set to Enabled (None allowed) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether users can provide credentials to Office using either their Microsoft Account or the user ID assigned by your organization for accessing Office 365.

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

Rationale:

Signing into Office allows users to connect to cloud services (such as SharePoint services in Office 365). By signing into Office, the user's status and other information could be made publicly available. In addition, organizations may not want users to access cloud services because of the potential downloading of malware or uploading of confidential information to cloud services. For example, a user could upload a highly confidential document from the organization's intranet to OneDrive and then share that file with other users on the Internet.

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\common\signin\signinoptions
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Miscellaneous\Block
Signing into Office
```

Impact:

Users will not be unable to connect to cloud services (such as SharePoint services in Office 365) and access the files and services provided by the cloud services.

Default Value:

Not Configured -If you disable or do not configure this policy setting, users can sign in by using either ID.

2.22 Office Converters

This section contains settings to configure Office Converters.

2.22.1 (L1) Ensure 'Block Opening of Pre-Release Versions of File Formats New to PowerPoint Through the Compatibility Pack for Office and PowerPoint Converter' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether users with the Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint File Formats installed can open Office Open XML files saved with pre-release versions of PowerPoint. PowerPoint Open XML files usually have the following extensions: .pptx, .pptm, .potx, .potm, .ppsx, .ppsm, .ppam, .thmx, .xml.

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

Rationale:

The Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint File Formats enables users of Microsoft PowerPoint 2000, PowerPoint 2002, and Office PowerPoint 2003 to open files saved in the Office Open XML format used by PowerPoint. PowerPoint Open XML files usually have the following extensions:

• .pptx

• .pptm

• .potx

• .potm

• .ppsx

• .ppsm

• .ppam

• .thmx

• .xml

By default, the Compatibility Pack does not open files that were saved in pre-release versions of the new Office Open XML format, which underwent some minor changes prior to the final release of PowerPoint. If this configuration is changed through a registry modification or by some other mechanism, users with the Compatibility Pack installed can open files saved by some pre-release versions of PowerPoint, but not by others, which can lead to inconsistent file opening 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\powerpoint\security\fileblock
\powerpoint12betafilesfromconverters
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Office 2016
Converters\Block Opening of Pre-Release Versions of File Formats New to PowerPoint
2016 Through the Compatibility Pack for Office 2013 and PowerPoint 2016 Converter
```

Impact:

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

Note See Plan block file format settings in the Office Resource Kit for more information about using Group Policy to manage and enforce file format requirements. Also, see the "File Block Technology" section in Chapter 4 of the Microsoft Office Security Guide for information about the Microsoft Office Isolated Conversion Environment (MOICE), which provides another method.

Default Value:

Not Configured

2.22.2 (L1) Ensure 'Block Opening of Pre-release Versions of File Formats New to Excel Through The Compatibility Pack for Office and Excel Converter' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether users with the Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint File Formats installed can open Office Open XML files saved with pre-release versions of Excel. Excel Open XML files usually have the following extensions: .xlsx, .xlsm, .xltx, .xltm, .xlam.

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

Rationale:

The Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint File Formats enables users of Microsoft Excel 2000, Microsoft Excel 2002, and Microsoft Office Excel 2003 to open files saved in the Office Open XML format used by Excel. Excel Open XML files usually have the following extensions:

• .xlsx

• .xlsm

• .xltx

• .xltm

• .xlam

By default, the Compatibility Pack does not open files that were saved in pre-release versions of the new Office Open XML format, which underwent some minor changes prior to the final release of Excel. If this configuration is changed through a registry modification or by some other mechanism, users with the Compatibility Pack installed can open files saved by some pre-release versions of Excel, but not by others, which can lead to inconsistent file opening 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\fileblock\excel12betafilesfromconverters
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Office 2016 Converters\Block Opening of Pre-release Versions of File Formats New to Excel 2016 Through The Compatibility Pack for Office 2016 and Excel 2016 Converter
```

Impact:

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

Note See Plan block file format settings in the Office Resource Kit for more information about using Group Policy to manage and enforce file format requirements. Also, see the "File Block Technology" section in Chapter 4 of the Microsoft Office Security Guide for information about the Microsoft Office Isolated Conversion Environment (MOICE), which provides another method.

Default Value:

Not Configured

2.23 Present Online

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

2.23.1 Presentation Services

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

2.24 Privacy

This section contains settings to configure Privacy Option.

2.24.1 Trust Center

This section contains settings to configure Trust Center.

2.24.1.1 (L1) Ensure 'Disable Opt-in Wizard on First Run' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether users see the Opt-in Wizard the first time they run a Microsoft Office application.

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

Rationale:

By default, the Opt-in Wizard displays the first time users run a Microsoft Office application, which allows them to opt into Internet-based services that will help improve their Office experience, such as Microsoft Update, the Customer Experience Improvement Program, Office Diagnostics, and Online Help. If your organization has policies that govern the use of such external resources, allowing users to opt in to these services might cause them to violate the policies.

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\common\general\shownfirstrunoptin
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Privacy\Trust Center\Disable Opt-in Wizard on First Run
```

Impact:

Enabling this setting will prevent users from opting in to the services listed above. This can prevent users from receiving the latest program updates, security fixes, and Help content. If you enable this setting, consider ensuring that such updates are made available to users through alternate means.

Default Value:

Not Configured

2.24.1.2 (L1) Ensure 'Enable Customer Experience Improvement Program' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether users can participate in the Microsoft Office Customer Experience Improvement Program to help improve Microsoft Office. When users choose to participate in the Customer Experience Improvement Program (CEIP), Office applications automatically send information to Microsoft about how the applications are used. This information is combined with other CEIP data to help Microsoft solve problems and to improve the products and features customers use most often. This feature does not collect users' names, addresses, or any other identifying information except the IP address that is used to send the data.

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

Rationale:

When users choose to participate in the Customer Experience Improvement Program (CEIP), Office applications automatically send information to Microsoft about how the applications are used. This information is combined with other CEIP data to help Microsoft solve problems and to improve the products and features customers use most often. This feature does not collect users' names, addresses, or any other identifying information except the IP address that is used to send the data.

By default, users have the opportunity to opt into participation in the CEIP the first time they run an Office application. If your organization has policies that govern the use of external resources such as the CEIP, allowing users to opt in to the program might cause them to violate these policies.

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\common\qmenable
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Privacy\Trust
Center\Enable Customer Experience Improvement Program
```

Impact:

The Customer Experience Improvement Program sends data to Microsoft silently and without affecting application usage, so choosing Disabled will not cause usability issues for Office users.

Default Value:

Not Configured

2.24.1.3 (L1) Ensure 'Allow including screenshot with Office Feedback' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting manages whether the Office Feedback Tool (a.k.a. Send a Smile) allows the user to send a screenshot of their desktop with their feedback to Microsoft. The Office Feedback Tool allows users to provide Microsoft feedback regarding their positive and negative experiences when using Office.

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

Rationale:

Due to privacy concerns, users should not be able to send data to any third party unless approved by the System Administrators.

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\common\feedback\includescreenshot
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Privacy\Trust Center\Allow including screenshot with Office Feedback
```

Impact:

If you disable this policy setting, the Office Feedback Tool will not allow the user to send a screenshot of their desktop with their feedback to Microsoft.

Default Value:

Not Configured - If you do not configure this policy setting, the behavior is the equivalent of setting the policy to "Enabled".

2.24.1.4 (L1) Ensure 'Send Office Feedback' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting manages the Office Feedback Tool (a.k.a. Send a Smile). The Office Feedback Tool allows users to provide Microsoft feedback regarding their positive and negative experiences when using Office.

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

Rationale:

Due to privacy concerns, users should not be able to send data to any third party unless approved by the System Administrators.

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\common\feedback\enabled
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Privacy\Trust
Center\Send Office Feedback
```

Impact:

If you disable this policy setting, the Office Feedback Tool will be turned off. Users will not see the Smile button in any of the Office applications in which the tool is available.

Default Value:

Not Configured - If you do not configure this policy setting, the behavior is the equivalent of setting the policy to "Enabled".

2.24.1.5 (L1) Ensure 'Send personal information' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether users can send personal information to Office. When users choose to send information Office applications automatically send information to Office.

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

Rationale:

Due to privacy concerns, users should not be able to send data to any third party unless approved by the System Administrators.

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\common\sendcustomerdata
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Privacy\Trust
Center\Send personal information
```

Impact:

If you disable this policy setting, Office users cannot send personal information to Office.

Default Value:

Not Configured - If you do not configure this policy setting, the behavior is the equivalent of setting the policy to "Enabled".

2.24.1.6 (L1) Ensure Set 'Automatically Receive Small Updates to Improve Reliability' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Microsoft Office Diagnostics is enabled. Office Diagnostics enables Microsoft to diagnose system problems by periodically downloading a small file to the computer.

If you enable this policy setting, Office Diagnostics collects information about specific errors and the IP address of the computer. Office Diagnostics does not transmit any personally identifiable information to Microsoft other than the IP address of the computer requesting the update.

If you disable this policy setting, users will not receive updates from Office Diagnostics.

If you do not configure this policy setting, this policy setting is not enabled, but users have the opportunity to opt into receiving updates from Office Diagnostics the first time they run an Office application. The recommended state for this setting is: `Disabled`.

Rationale:

Office Diagnostics is used to improve the user experience by periodically downloading a small file to the computer with updated help information about specific problems. If Office Diagnostics is enabled, it collects information about specific errors and the IP address of the computer. When new help information is available, that help information is downloaded to the computer that experienced the related problems. Office Diagnostics does not transmit any personally identifiable information to Microsoft other than the IP address of the computer requesting the update.

By default, users have the opportunity to opt into receiving updates from Office Diagnostics the first time they run a Office application. If your organization has policies that govern the use of external resources such as Office Diagnostics, allowing users to opt in to this feature might cause them to violate these policies.

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\common\updatereliabilitydata
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Privacy\Trust
Center\Automatically Receive Small Updates to Improve Reliability
```

Impact:

Disabling this setting will prevent users from receiving information and advice from Microsoft about fixing and preventing Office application errors, which could cause your support department to experience an increase in desktop support requests.

Default Value:

Not Configured

2.25 Security Settings

This section contains settings to configure Security Settings.

2.25.1 Digital Signatures

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

2.25.2 Escrow Certificates

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

2.25.3 Trust Center

This section contains settings to configure Trust Center.

2.25.3.1 Protected View

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

2.25.3.2 Trusted Catalogs

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

2.25.3.3 (L1) Ensure 'Allow Mix of Policy and User Locations' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether trusted locations can be defined by users, the Office Customization Tool (OCT), and Group Policy, or if they must be defined by Group Policy alone.

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

Rationale:

When files are opened from trusted locations, all the content in the files is enabled and active. Users are not notified about any potential risks that might be contained in the files, such as unsigned macros, ActiveX controls, or links to content on the Internet.

By default, users can specify any location as a trusted location, and a computer can have a combination of user-created, OCT-created, and Group Policy-created trusted locations.

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\common\security\trusted
locations\allow user locations
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security
Settings\Trust Center\Allow Mix of Policy and User Locations
```

Impact:

Disabling this setting will cause some disruption for users who have defined their own trusted locations in the Trust Center. Applications will treat such locations like any other untrusted locations, which means that users will see Message Bar warnings about active content such as ActiveX controls and VBA macros when they open files, and they will have to choose whether to enable controls and macros or leave them disabled.

Default Value:

Not Configured

2.25.4 (L1) Ensure 'Suppress Hyperlink Warnings' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Office applications notify users about unsafe hyperlinks. Links that Office considers unsafe include links to executable files, TIFF files, and Microsoft Document Imaging (MDI) files. Other unsafe links are those that use protocols considered to be unsafe such as javascript.

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

Rationale:

Unsafe hyperlinks are links that might pose a security risk if users click them. Clicking an unsafe link could compromise the security of sensitive information or harm the computer.

Links that Office considers unsafe include links to executable files, TIFF files, and Microsoft Document Imaging (MDI) files. Other unsafe links are those that use protocols considered to be unsafe, including msn, nntp, mms, outlook, and stssync.

By default, Office applications notify users about unsafe hyperlinks and disable them until users enable them.

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\common\security\disablehyperl
inkwarning
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security
Settings\Suppress Hyperlink Warnings
```

Impact:

This setting does not alter the default configuration and therefore is unlikely to provide any usability concerns.

Default Value:

Not Configured

2.25.5 (L1) Ensure 'Protect Document Metadata for Rights Managed Office Open XML Files' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether metadata is encrypted in Office Open XML files that are protected by Information Rights Management (IRM).

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

Rationale:

By default, when Information Rights Management (IRM) is used to restrict access to an Office Open XML document, any metadata associated with the document is not encrypted. This configuration could allow potentially sensitive information such as the document author and hyperlink references to be exposed to unauthorized people.

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\common\security\drmencryptpro
perty
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security
Settings\Protect Document Metadata for Rights Managed Office Open XML Files
```

Impact:

Enabling this setting might interfere with the functioning of tools that aggregate and display metadata information for Office Open XML files, but is otherwise unlikely to cause significant usability issues.

Default Value:

Not Configured

2.25.6 (L1) Ensure 'Protect Document Metadata for Password Protected Files' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether metadata is encrypted when an Office Open XML file is password protected.

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

Rationale:

By default, when an Office Open XML document is protected with a password and saved, any metadata associated with the document is encrypted along with the rest of the document's contents. If this configuration is changed, potentially sensitive information such as the document author and hyperlink references could be exposed to unauthorized people.

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\common\security\openxmlencryptproperty
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security Settings\Protect Document Metadata for Password Protected Files
```

Impact:

Enabling this setting might interfere with the functioning of tools that aggregate and display metadata information for Office Open XML files, but is otherwise unlikely to cause significant usability issues.

Default Value:

Not Configured

2.25.7 (L1) Ensure 'Load Controls in Forms3' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to control how ActiveX controls in UserForms should be initialized based upon whether they are Safe For Initialization (SFI) or Unsafefor Initialization (UFI).

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

Rationale:

ActiveX controls are Component Object Model (COM) objects and have unrestricted access to users' computers. ActiveX controls can access the local file system and change the registry settings of the operating system. If a malicious user repurposes an ActiveX control to take over a user's computer, the effect could be significant.

To help improve security, ActiveX developers can mark controls as Safe For Initialization (SFI), which means that the developer states that the controls are safe to open and run and not capable of causing harm to any computers. If a control is not marked SFI, the control could adversely affect a computer—or it's possible the developers did not test the control in all situations and are not sure whether their control might be compromised at some future date.

SFI controls run in safe mode, which limits their access to the computer. For example, a worksheet control can both read and write files when it is in unsafe mode, but perhaps only read from files when it is in safe mode. This functionality allows the control to be used in very powerful ways when safety wasn't important, but the control would still be safe for use in a Web page.

If a control is not marked as SFI, it is marked Unsafe For Initialization (UFI), which means that it is capable of affecting a user's computer. If UFI ActiveX controls are loaded, they are always loaded in unsafe mode.

This setting allows administrators to control how ActiveX controls in UserForms should be initialized based upon whether they are SFI or UFI.

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>\keycupoliciesmsvbasecurity\loadcontrolsinforms
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security
Settings\Load Controls in Forms3
```

Impact:

Enabling this setting and selecting "2" enforces the default configuration and is therefore unlikely to cause usability issues for most users.

Default Value:

Not Configured

2.25.8 (L1) Ensure 'Encryption Type for Password Protected Office Open XML Files' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to specify an encryption type for Office Open XML files.

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

Rationale:

If unencrypted files are intercepted, sensitive information in the files can be compromised. To protect information confidentiality, Office application files can be encrypted and password protected. Only users who know the correct password will be able to decrypt such files.

On computers that run Windows Vista, the default cryptographic service provider (CSP) is Microsoft Enhanced RSA and AES Cryptographic Provider, AES-128, 128-bit. On computers that run Windows XP, the default CSP is Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype), AES-128, 128-bit.

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\common\security\openxmlencryp
tion
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security
Settings\Encryption Type for Password Protected Office Open XML Files
```

Impact:

Consider the needs of your organization and users when selecting an encryption method to enforce. If you work for a government agency, contract for a government agency, or

otherwise work with very sensitive information, you might need to select a method that complies with policies that govern how such information is processed. Remember, you will need to ensure that the selected cryptographic service provider is installed on the computers of all users who need to work with password-protected Office Open XML files.

Default Value:

Not Configured

2.25.9 (L1) Ensure 'Encryption Type for Password Protected Office 97-2003 files' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting enables you to specify an encryption type for password-protected Office 97-2003 files.

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

Rationale:

If unencrypted files are intercepted, sensitive information in the files can be compromised. To protect information confidentiality, Microsoft Office application files can be encrypted and password protected. Only users who know the correct password will be able to decrypt such files.

By default, Excel, PowerPoint, and Word use Office 97/2000 Compatible encryption, a proprietary encryption method, to encrypt password-protected Office 97-2003 files.

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\common\security\defaultencryption12
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security Settings\Encryption Type for Password Protected Office 97-2003 files
```

Impact:

Consider the needs of your organization and users when selecting an encryption method to enforce. If you work for a government agency, contract for a government agency, or otherwise work with very sensitive information, you might need to select a method that

complies with policies that govern how such information is processed. Remember that you will need to ensure that the selected cryptographic service provider is installed on the computers of all users who need to work with password-protected Office 97-2003 files.

Default Value:

Not Configured

2.25.10 (L1) Ensure 'Disable Password to Open UI' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Office users can add password encryption to documents. (Users would access this feature in Microsoft Office tab--click Info, click Protect Document, then click Encrypt with Password.)

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

Rationale:

If Office users add passwords to documents, other users can be prevented from opening the documents. This capability can provide an extra level of protection to documents that are already protected by access control lists, or provide a means of securing documents that are not protected by file-level security.

By default, users can add passwords to Excel workbooks, PowerPoint presentations, and Word documents from the Save or Save As dialog box by clicking Tools, clicking General Options, and entering appropriate passwords to open or modify the documents. If this configuration is changed, users will not be able to enter passwords in the General Options dialog box, which means they will not be able to password protect documents.

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\common\security\disablepasswordui
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security Settings\Disable Password to Open UI
```

Impact:

The recommended settings enforce the default configuration, and therefore will not affect usability. Typically, this setting should not be enabled, because doing so will prevent users from adding passwords to Office files. However, if you wish to ensure that only other mechanisms are used to secure files, you might consider enabling this setting.

Default Value:

Not Configured

2.25.11 (L1) Ensure 'Disable All Trust Bar Notifications For Security Issues' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Office applications notify users when potentially unsafe features or content are detected, or whether such features or content are silently disabled without notification.

recommended state for this setting is: `Disabled`.

Rationale:

The Message Bar in Office applications is used to identify security issues, such as unsigned macros or potentially unsafe add-ins. When such issues are detected, the application disables the unsafe feature or content and displays the Message Bar at the top of the active window. The Message Bar informs the users about the nature of the security issue and, in some cases, provides the users with an option to enable the potentially unsafe feature or content, which could harm the user's computer.

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\common\trustcenter\trustbar
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security
Settings\Disable All Trust Bar Notifications For Security Issues
```

Impact:

This setting does not modify the default configuration, and therefore is unlikely to cause any usability issues.

Default Value:

By default, if an Office application detects a security issue, the Message Bar is displayed. However, this configuration can be modified by users in the Trust Center.

2.25.12 (L1) Ensure 'Automation Security' is set to Enabled (Disable Macros by Default) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether macros can run in an Office application that is opened programmatically by another application.

The recommended state for this setting is: `Enabled. (Disable Macros by Default)`

Rationale:

By default, when a separate program is used to launch Microsoft Office Excel, PowerPoint, or Word programmatically, any macros can run in the programmatically opened application without being blocked. This functionality could allow an attacker to use automation to run malicious code in Excel, PowerPoint, or Word.

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\common\security\automationsecurity
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security
Settings\Automation Security
```

Impact:

Enabling this setting and selecting "Disable macros by default" from the drop-down menu could limit functionality if an external application programmatically opens a Office application to open a document or template containing macros.

Default Value:

Not Configured

2.25.13 (L1) Ensure 'ActiveX Control Initialization' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting specifies the Microsoft ActiveX® initialization security level for all Microsoft Office applications.

The recommended state for this setting is: `Disabled`

Rationale:

Attackers can use ActiveX controls that include malicious code to attack a computer. In addition, malicious code can be used to compromise an ActiveX control and attack a computer. To indicate the safety of an ActiveX control, developers can denote them as Safe For Initialization (SFI). SFI indicates that a control is safe to open and run, and that it is not capable of causing a problem for any computer, regardless of whether it has persisted data values or not.

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\common\security\uficontrols
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security
Settings\ActiveX Control Initialization
```

Impact:

This setting only increases security for ActiveX controls that are accurately marked as SFI. In situations that involve malicious or poorly designed code, an ActiveX control might be inaccurately marked as SFI.

Important Some ActiveX controls do not respect the safe mode registry setting, and therefore might load persisted data even though you configure this setting to instruct the control to use safe mode.

Default Value:

Not Configured

2.26 Server Settings

This section contains settings to configure Server Settings.

2.26.1 SharePoint Server

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

2.26.2 (L1) Ensure 'Disable The Office Client From Polling The SharePoint Server For Published Links' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Office applications can poll Office servers to retrieve lists of published links.

Note - This policy setting applies to Microsoft SharePoint Server specifically. It does not apply to Microsoft SharePoint Foundation.

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

Rationale:

By default, users of Office applications can see and use links to Microsoft Office SharePoint Server sites from those applications. Administrators configure published links to Office applications during initial deployment, and can add or change links as part of regular operations. These links appear on the My SharePoint Sites tab of the Open, Save, and Save As dialog boxes when opening and saving documents from these applications. Links can be targeted so that they only appear to users who are members of particular audiences.

If a malicious person gains access to the list of published links, they could modify the links to point to unapproved sites, which could make sensitive data vulnerable to exposure.

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\common\portal\linkpublishingdisabled
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Server
Settings\Disable The Office Client From Polling The SharePoint Server For Published
Links
```

Impact:

If this setting is Enabled, users will not be able to use the list of published links to open and save files directly from within Office applications, which could hinder the use of SharePoint Server for document collaboration.

Note This setting applies to Microsoft Office SharePoint Server specifically. It does not apply to Windows SharePoint Services (WSS).

Default Value:

Not Configured

2.27 Services

This section contains settings to configure Services.

2.27.1 Fax

This section configures settings to configure Fax options.

2.27.1.1 (L1) Ensure 'Disable Internet Fax Feature' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether users can access the Internet Fax feature in Office applications.

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

Rationale:

Excel, PowerPoint, and Word users can use the Internet Fax feature to send documents to fax recipients through an Internet fax service provider. If your organization has policies that govern the time, place, or manner in which faxes are sent, this feature could help users evade those policies.

By default, Office users can use the Internet Fax feature.

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\common\services\fax\nofax
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Services\Fax\Disable
Internet Fax Feature
```

Impact:

If the Internet Fax feature is used by your organization to send faxes, enabling this setting will cause users to lose this functionality. In such situations, you will need to ensure that users who need to send faxes have some other mechanism for doing so.

Default Value:

Not Configured

2.28 Shared Paths

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

2.29 Signing

This section contains settings for configuring Signing options.

2.29.1 (L1) Ensure 'Suppress External Signature Service' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook displays the "Add Signature Services" menu item.

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

Rationale:

By default, users can select Add Signature Services (from the Signature Line drop-down menu on the Insert tab of the Ribbon in Excel, PowerPoint, and Word) to see a list of signature service providers on the Microsoft Office Web site. If your organization has policies that govern the use of external resources such as signature providers or Office Marketplace, allowing users to access the Add Signature Services menu item might enable them to violate those policies.

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\common\signatures\suppressext
signingsvcs
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Signing\Suppress
External Signature Service
```

Impact:

Enabling this setting prevents users from adding a signature service from Microsoft Office.com, but should not otherwise cause significant usability issues for most users.

Default Value:

Not Configured

2.29.2 (L1) Ensure 'Legacy Format Signatures' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether users can apply binary format digital signatures to Office 97-2003 documents.

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

Rationale:

By default, Office applications use the XML-based XMLDSIG format to attach digital signatures to documents, including Office 97-2003 binary documents. XMLDSIG signatures are not recognized by Office 2003 applications or previous versions. If an Office 2003 user opens an Excel, PowerPoint, or Word binary document with an XMLDSIG signature attached, the signature will be lost.

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\common\signatures\enablecreat
ionofweakxpsignatures
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Signing\Legacy
Format Signatures
```

Impact:

Enabling this setting is not likely to cause significant usability issues for most Office users.

Default Value:

Not Configured

2.30 Smart Documents (Word, Excel)

This section contains settings to configure Smart Documents.

2.30.1 (L1) Ensure 'Disable Smart Document's Use of Manifests' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Office applications can load an XML expansion pack manifest file with a Smart Document.

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

Rationale:

An XML expansion pack is the group of files that constitutes a Smart Document in Excel and Word. You package one or more components that provide the logic needed for a Smart Document by using an XML expansion pack. These components can include any type of file, including XML schemas, Extensible Stylesheet Language Transforms (XSLTs), dynamic-link libraries (DLLs), and image files, as well as additional XML files, HTML files, Word files, Excel files, and text files.

The key component to building an XML expansion pack is creating an XML expansion pack manifest file. By creating this file, you specify the locations of all files that make up the XML expansion pack, as well as information that instructs Office how to set up the files for your Smart Document. The XML expansion pack can also contain information about how to set up some files, such as how to install and register a COM object required by the XML expansion pack.

XML expansion packs can be used to initialize and load malicious code, which might affect the stability of a computer and lead to data loss.

By default, Office applications can load an XML expansion pack manifest file with a Smart 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\common\smart
tag\neverloadmanifests
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Smart Documents
(Word, Excel)\Disable Smart Document's Use of Manifests
```

Impact:

Enabling this setting prevents users from working with Smart Documents. It might not be feasible to enable this setting.

Default Value:

Not Configured

2.31 Subscription Activation

This section contains settings to configure Subscription Activation.

2.32 Telemetry Dashboard

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

2.33 Tools | AutoCorrect Options... (Excel, PowerPoint and Access)

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

2.33.1 Additional Actions

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

2.34 Tools | Options | General | Service Options...

This section contains settings to configure Office options.

2.34.1 Conversion Service

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

2.34.2 Online Content

This section contains settings to configure Online Content.

2.34.2.1 (L1) Ensure 'Online Content Options' is set to Enabled (Allow Office to connect to the internet) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls users' access to the online features of Office.

The recommended state for this setting is: `Enabled. (Allow Office to connect to the internet)`

Rationale:

By default, the Office Help system automatically searches Microsoft Office.com for content when a computer is connected to the Internet. Users can change this default by clearing the Search Microsoft Office.com for Help content when I'm connected to the Internet check box in the Privacy Options section of the Trust Center. If your organization has policies that govern the use of external resources such as Office.com, allowing the Help system to download content might cause users to violate these policies.

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\common\internet\useonlinecont
ent
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Tools | Options |
General | Service Options...\Online Content\Online Content Options
```

Impact:

Configuring this setting to "Never show online content or entry points" will cause disruptions for users who are accustomed to receiving content from Microsoft Office.com within Office applications. These users will have to access Microsoft Office.com using their Web browsers to obtain this content, if permitted.

Default Value:

Not Configured

2.34.3 PowerPoint Designer

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

2.35 Tools | Options | General | Web Options...

This section contains settings to configure Office options.

2.35.1 Browsers

This section contains settings to configure Browser options.

2.35.1.1 (L1) Ensure 'Allow PNG As an Output Format' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether Office applications can output graphics in Portable Network Graphics (PNG) format when documents are saved as Web pages.

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

Rationale:

Excel, PowerPoint, and Word can save graphic files in Portable Network Graphics (PNG) format to improve the quality of the graphics when documents are saved as Web pages. The PNG graphic file format (.png) is used for a wide range of graphics, from small images (such as bullets and banners) to complex images (such as photographs), and can offer better image fidelity and smaller file sizes than some other formats. However, PNG graphics cannot be displayed by many earlier Web browsers, such as Microsoft Internet Explorer® version 5 or earlier.

By default, Office applications do not save graphics in the PNG format. To change this functionality, users can open the application's Options dialog box, click Advanced, click Web Options, and then select the Allow PNG as a graphics format check box.

This setting can be used to guard against theoretical future zero-day attacks that might target PNG files.

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\common\internet\allowpng
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Tools | Options |
General | Web Options...\Browsers\Allow PING As an Output Format
```

Impact:

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

Default Value:

Not Configured

2.35.2 Encoding

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

2.35.3 Files

This section contains settings to configure Files options.

2.35.3.1 (L1) Ensure 'Open Office Documents as Read/Write While Browsing' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether users can edit and save Office documents on Web servers that they have opened using Internet Explorer.

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

Rationale:

By default, when users browse to an Office document on a Web server using Internet Explorer, the appropriate application opens the file in read-only mode. However, if the default configuration is changed, the document is opened as read/write. Users could potentially make changes to documents and resave them in situations where the Web server security is not configured to prevent such changes.

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\common\internet\opendocuments
readwritewhilebrowsing
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Tools | Options |
General | Web Options...\Files\Open Office Documents as Read/Write While Browsing
```

Impact:

This setting enforces the Office default configuration and therefore should have minimal impact on users.

Default Value:

Not Configured

2.35.4 General

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

2.36 Tools | Options | Spelling

This sections contains settings to configure Office Options.

2.36.1 Proofing Data Collection

This section contains settings to configure Proofing Data Collection.

2.36.1.1 (L1) Ensure 'Improve Proofing Tools' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether the Help Improve Proofing Tools feature sends usage data to Microsoft. The Help Improve Proofing Tools feature collects data about use of the Proofing Tools, such as additions to the custom dictionary, and sends it to Microsoft. After about six months, the feature stops sending data to Microsoft and deletes the data collection file from the user's computer.

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

Rationale:

The Help Improve Proofing Tools feature collects data about use of the Proofing Tools, such as additions to the custom dictionary, and sends it to Microsoft. After about six months, the feature stops sending data to Microsoft and deletes the data collection file from the user's computer. Although this feature does not intentionally collect personal information, some of the content that is sent could include items that were marked as spelling or grammar errors, such as proper names and account numbers. However, any numbers such as account numbers, street addresses, and phone numbers are converted to zeroes when the data is collected. Microsoft uses this information solely to improve the effectiveness of the Office Proofing Tools, not to identify users.

By default, this feature is enabled if users choose to participate in the Customer Experience Improvement Program (CEIP). If your organization has policies that govern the use of external resources such as the CEIP, allowing the use of the Help Improve Proofing Tools feature might cause them to violate these policies.

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\\common\ptwatson\ptwoptin
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Office 2016\Tools | Options |
Spelling\Proofing Data Collection\Improve Proofing Tools
```

Impact:

The Customer Experience Improvement Program sends proofing tool data to Microsoft silently and without affecting application usage, so disabling the collection and transmission of proofing tool data is unlikely to cause usability issues for most users.

Default Value:

Not Configured

2.37 Web Archives

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

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Computer Configuration**		
1.1	**Miscellaneous**		
1.2	**Security Settings**		
1.2.1	**IE Security**		
1.2.1.1	(L1) Ensure 'Protection From Zone Elevation' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)	☐	☐
1.2.1.2	(L1) Ensure 'Mime Sniffing Safety Feature' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)	☐	☐
1.2.1.3	(L1) Ensure 'Information Bar' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)	☐	☐
1.2.1.4	(L1) Ensure 'Bind to Object' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)	☐	☐
1.2.1.5	(L1) Ensure 'Restrict File Download' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)	☐	☐
1.2.1.6	(L1) Ensure 'Saved from URL' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)	☐	☐
1.2.1.7	(L1) Ensure 'Disable User Name and Password' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)	☐	☐
1.2.1.8	(L1) Ensure 'Scripted Window Security Restrictions' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe,	☐	☐

	onent.exe, mse7.exe) (Scored)		
1.2.1.9	(L1) Ensure 'Local Machine Zone Lockdown Security' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)	☐	☐
1.2.1.10	(L1) Ensure 'Object Caching Protection' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)	☐	☐
1.2.1.11	(L1) Ensure 'Consistent Mime Handling' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)	☐	☐
1.2.1.12	(L1) Ensure 'Add-on Management' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)	☐	☐
1.2.1.13	(L1) Ensure 'Navigate URL' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)	☐	☐
1.2.1.14	(L1) Ensure 'Restrict ActiveX Install' is set to Enabled (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe) (Scored)	☐	☐
1.3	**Updates**		
1.3.1	(L1) Ensure 'Enable Automatic Updates' is set to Enabled (Scored)	☐	☐
1.3.2	(L1) Ensure 'Hide Option to Enable or Disable Updates' is set to Enabled (Scored)	☐	☐
1.4	**Volume Activation**		
2	**User Configuration**		
2.1	**Business Data**		
2.1.1	**Database**		
2.1.2	**Synchronization**		
2.1.3	**Web Service**		
2.2	**Collaboration Settings**		
2.2.1	**Co-Authoring**		
2.2.2	**Default Message Text for a reply...**		
2.2.3	**Default Message Text for a Review Request...**		
2.3	**Contact Card**		
2.3.1	**Contact Card**		
2.4	**Customizable Error Messages**		

2.5	**Disable Items in User Interface**		
2.6	**DLP**		
2.7	**Document Information Panel**		
2.7.1	(L1) Ensure 'Document Information Panel Beaconing UI' is set to Enabled (Always show UI) (Scored)	☐	☐
2.8	**Downloading Framework Components**		
2.9	**File Open/Save Dialog Box**		
2.9.1	**Places Bar Locations**		
2.9.2	**Restricted Browsing**		
2.10	**First Run**		
2.11	**Global Options**		
2.11.1	**Customize**		
2.11.1.1	**Shared Workspace**		
2.11.1.1.1	**Define Shared Workspace URL's**		
2.11.1.2	(L1) Ensure 'Disable UI Extending from Documents and Templates' is set to Enabled (Disallow in Access, Excel, InfoPath, Outlook, PowerPoint, Publisher, Word) (Scored)	☐	☐
2.12	**Graph Settings**		
2.13	**Help**		
2.14	**IME (Japanese)**		
2.15	**Improved Error Reporting**		
2.16	**Language Preferences**		
2.16.1	**Display Language**		
2.16.2	**Editing Languages**		
2.16.2.1	**Enabled Editing Languages**		
2.17	**Manage Restricted Permissions**		
2.17.1	(L1) Ensure 'Prevent Users From Changing Permissions on Rights Managed Content' is set to Disabled (Scored)	☐	☐
2.17.2	(L1) Ensure 'Never Allow Users to Specify Groups When Restricting Permission for Documents' is set to Enabled (Scored)	☐	☐
2.17.3	(L1) Ensure 'Always Require Users to Connect to Verify Permission' is set to Enabled (Scored)	☐	☐
2.17.4	(L1) Ensure 'Always Expand Groups in Office When Restricting Permission for Documents' is set to Enabled (Scored)	☐	☐
2.17.5	(L1) Ensure 'Allow Users With Earlier Versions of Office to Read with Browsers...." is set to Disabled (Scored)	☐	☐
2.18	**Microsoft Office Document Cache**		
2.19	**Microsoft Office SmartArt**		
2.20	**Microsoft Save as PDF and XPS add-ins**		
2.21	**Miscellaneous**		
2.21.1	**Workflow Cache**		

2.21.2	(L1) Ensure 'Control Blogging' is set to Enabled (All Blogging Disabled) (Scored)	☐	☐
2.21.3	(L1) Ensure 'Block Signing into Office' is set to Enabled (None allowed) (Scored)	☐	☐
2.22	**Office Converters**		
2.22.1	(L1) Ensure 'Block Opening of Pre-Release Versions of File Formats New to PowerPoint Through the Compatibility Pack for Office and PowerPoint Converter' is set to Enabled (Scored)	☐	☐
2.22.2	(L1) Ensure 'Block Opening of Pre-release Versions of File Formats New to Excel Through The Compatibility Pack for Office and Excel Converter' is set to Enabled (Scored)	☐	☐
2.23	**Present Online**		
2.23.1	**Presentation Services**		
2.24	**Privacy**		
2.24.1	**Trust Center**		
2.24.1.1	(L1) Ensure 'Disable Opt-in Wizard on First Run' is set to Enabled (Scored)	☐	☐
2.24.1.2	(L1) Ensure 'Enable Customer Experience Improvement Program' is set to Disabled (Scored)	☐	☐
2.24.1.3	(L1) Ensure 'Allow including screenshot with Office Feedback' is set to Disabled (Scored)	☐	☐
2.24.1.4	(L1) Ensure 'Send Office Feedback' is set to Disabled (Scored)	☐	☐
2.24.1.5	(L1) Ensure 'Send personal information' is set to Disabled (Scored)	☐	☐
2.24.1.6	(L1) Ensure Set 'Automatically Receive Small Updates to Improve Reliability' is set to Disabled (Scored)	☐	☐
2.25	**Security Settings**		
2.25.1	**Digital Signatures**		
2.25.2	**Escrow Certificates**		
2.25.3	**Trust Center**		
2.25.3.1	**Protected View**		
2.25.3.2	**Trusted Catalogs**		
2.25.3.3	(L1) Ensure 'Allow Mix of Policy and User Locations' is set to Disabled (Scored)	☐	☐
2.25.4	(L1) Ensure 'Suppress Hyperlink Warnings' is set to Disabled (Scored)	☐	☐
2.25.5	(L1) Ensure 'Protect Document Metadata for Rights Managed Office Open XML Files' is set to Enabled (Scored)	☐	☐
2.25.6	(L1) Ensure 'Protect Document Metadata for Password Protected Files' is set to Enabled (Scored)	☐	☐
2.25.7	(L1) Ensure 'Load Controls in Forms3' is set to Disabled (Scored)	☐	☐
2.25.8	(L1) Ensure 'Encryption Type for Password Protected Office	☐	☐

	Open XML Files' is set to Enabled (Scored)		
2.25.9	(L1) Ensure 'Encryption Type for Password Protected Office 97-2003 files' is set to Enabled (Scored)	☐	☐
2.25.10	(L1) Ensure 'Disable Password to Open UI' is set to Disabled (Scored)	☐	☐
2.25.11	(L1) Ensure 'Disable All Trust Bar Notifications For Security Issues' is set to Disabled (Scored)	☐	☐
2.25.12	(L1) Ensure 'Automation Security' is set to Enabled (Disable Macros by Default) (Scored)	☐	☐
2.25.13	(L1) Ensure 'ActiveX Control Initialization' is set to Disabled (Scored)	☐	☐
2.26	**Server Settings**		
2.26.1	**SharePoint Server**		
2.26.2	(L1) Ensure 'Disable The Office Client From Polling The SharePoint Server For Published Links' is set to Enabled (Scored)	☐	☐
2.27	**Services**		
2.27.1	**Fax**		
2.27.1.1	(L1) Ensure 'Disable Internet Fax Feature' is set to Enabled (Scored)	☐	☐
2.28	**Shared Paths**		
2.29	**Signing**		
2.29.1	(L1) Ensure 'Suppress External Signature Service' is set to Enabled (Scored)	☐	☐
2.29.2	(L1) Ensure 'Legacy Format Signatures' is set to Disabled (Scored)	☐	☐
2.30	**Smart Documents (Word, Excel)**		
2.30.1	(L1) Ensure 'Disable Smart Document's Use of Manifests' is set to Enabled (Scored)	☐	☐
2.31	**Subscription Activation**		
2.32	**Telemetry Dashboard**		
2.33	**Tools | AutoCorrect Options... (Excel, PowerPoint and Access)**		
2.33.1	**Additional Actions**		
2.34	**Tools | Options | General | Service Options...**		
2.34.1	**Conversion Service**		
2.34.2	**Online Content**		
2.34.2.1	(L1) Ensure 'Online Content Options' is set to Enabled (Allow Office to connect to the internet) (Scored)	☐	☐
2.34.3	**PowerPoint Designer**		
2.35	**Tools | Options | General | Web Options...**		
2.35.1	**Browsers**		
2.35.1.1	(L1) Ensure 'Allow PNG As an Output Format' is set to Disabled (Scored)	☐	☐

2.35.2	**Encoding**		
2.35.3	**Files**		
2.35.3.1	(L1) Ensure 'Open Office Documents as Read/Write While Browsing' is set to Disabled (Scored)	☐	☐
2.35.4	**General**		
2.36	**Tools | Options | Spelling**		
2.36.1	**Proofing Data Collection**		
2.36.1.1	(L1) Ensure 'Improve Proofing Tools' is set to Disabled (Scored)	☐	☐
2.37	**Web Archives**		

Appendix: Change History

Date	Version	Changes for this version
1-29-16	1.0.0	Initial Release – Based off of Office 2013 v1.0.0
11/30/16	V1.1.0	Title/Recommendation Clean up
11/30/16	V1.1.0	Add "Ensure 'Send Office Feedback' is set to Disabled" Ticket #14
11/30/16	V1.1.0	Add "Ensure 'Allow including screenshot with Office Feedback' is set to Disabled" Ticket #15
11/30/16	V1.1.0	Modify 2.21.3 (L1) Ensure 'Block Signing into Office' is set to Enabled (Both IDs Allowed) (Scored) Ticket #17
11/30/16	V1.1.0	Add Ensure "Send personal information" to Disabled Ticket #13