CIS Center for Internet Security®

CIS Benchmarks™

CIS Microsoft Office System 2016 STIG Benchmark

v1.0.0 - 08-27-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

Microsoft Office System 2016 Secure Technical Implementation Guide (STIG)

Version: 2 Release: 4 Benchmark

Date: 30 Jan 2025

Intended Audience

This benchmark 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 System 2016 and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Microsoft Office System 2016

Recommendations

1 STIG RULES

Microsoft Office 2016

Microsoft Office System 2016 Secure Technical Implementation Guide (STIG)

Version: 2 Release: 4 Benchmark

Date: 30 Jan 2025

CLASSIFICATION unclassified

1.1 DTOO182 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Help Improve Proofing Tools feature for Office must be configured.

```
GROUP ID: V-238024
RULE ID: SV-238024r961863
```

Rationale:

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. If you enable this policy setting, 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. If you disable this policy setting, the Help Improve Proofing Tools feature does not collect proofing tool usage information and transmit it to Microsoft. If you do not configure this policy setting, the behavior is the equivalent of setting the policy to "Enabled".

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Tools \ Options \ Spelling -> Proofing Data Collection "Improve Proofing Tools" is set to "Disabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\common\ptwatson

Criteria: If the value PTWOptIn is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Tools \ Options \ Spelling -> Proofing Data Collection "Improve Proofing Tools" to "Disabled".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.2 DTOO186 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Trust Bar notifications for Security messages must be enforced.

```
GROUP ID: V-238025
RULE ID: SV-238025r961086
```

Rationale:

This policy setting controls whether Office 2016 applications notify users when potentially unsafe features or content are detected, or whether such features or content are silently disabled without notification. The Message Bar in Office 2016 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. If you enable this policy setting, Office 2016 applications do not display information in the Message Bar about potentially unsafe content that has been detected or has automatically been blocked. If you disable this policy setting, Office 2016 applications display information in the Message Bar about content that has automatically been blocked. If you do not configure this policy setting, if an Office 2016 application detects a security issue, the Message Bar is displayed. However, this configuration can be modified by users in the Trust Center.

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "Disable all Trust Bar notifications for security issues" is set to "Disabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\common\trustcenter

Criteria: If the value TrustBar is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "Disable all Trust Bar notifications for security issues" to "Disabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.3 DTOO187 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Rights managed Office Open XML files must be protected.

```
GROUP ID: V-238026
RULE ID: SV-238026r961602
```

Rationale:

This policy setting determines whether metadata is encrypted in Office Open XML files that are protected by Information Rights Management (IRM). If you enable this policy setting, Excel, PowerPoint, and Word encrypt metadata stored in rights-managed Office Open XML files and override any configuration changes on users' computers. If you disable this policy setting, Office 2016 applications cannot encrypt metadata in rights-managed Office Open XML files, which can reduce security. If you do not configure this policy setting, 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.

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "Protect document metadata for rights managed Office Open XML Files" is set to "Enabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\common\security

Criteria: If the value DRMEncryptProperty is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "Protect document metadata for rights managed Office Open XML Files" to "Enabled".

Additional Information:

CCI-002476 Implement cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4::SC-28 (1)
- NIST SP 800-53 Revision 5::SC-28 (1)

1.4 DTOO188 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Document metadata for password protected files must be protected.

```
GROUP ID: V-238027
RULE ID: SV-238027r961128
```

Rationale:

This policy setting determines whether metadata is encrypted when an Office Open XML file is password protected. If you enable this policy setting, Excel 2016, PowerPoint 2016, and Word 2016 encrypt metadata stored in password-protected Office Open XML files and override any configuration changes on users' computers. If you disable this policy setting, Office 2016 applications cannot encrypt metadata in password-protected Office Open XML files, which can reduce security. If you do not configure this policy setting, 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:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "Protect document metadata for password protected files" is set to "Enabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\common\security

Criteria: If the value OpenXMLEncryptProperty is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "Protect document metadata for password protected files" to "Enabled".

Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

1.5 DTOO189 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The encryption type for password protected Open XML files must be set.

```
GROUP ID: V-238028
RULE ID: SV-238028r961128
```

Rationale:

This policy setting allows you to specify an encryption type for Office Open XML files. If you enable this policy setting, you can specify the type of encryption that Office applications use to encrypt password-protected files in the Office Open XML file formats used by Excel, PowerPoint, and Word. The chosen encryption type must have a corresponding cryptographic service provider (CSP) installed on the computer that encrypts the file. See the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\ registry key for a list of CSPs installed on the local computer. Specify the encryption type to use by entering it in the provided text box in the following form:<Encryption Provider>,<Encryption Algorithm>,<Encryption Key Length>For example: Microsoft Enhanced Cryptographic Provider v1.0,RC4,128. If you disable or do not configure this policy setting, the default CSP is used. The default cryptographic service provider (CSP) is Microsoft Enhanced RSA and AES Cryptographic Provider, AES-128, 128-bit.Note: This policy setting does not take effect unless the registry key HKEY_CURRENT_USER\Software\Microsoft\Office\16.0<office application name>\Security\Crypto\CompatMode is set to 0. By default the CompatMode registry key is set to 1.

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "Encryption type for password protected Office Open XML files" is set to "Enabled (Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256)".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\common\security

Criteria: If the value OpenXMLEncryption is REG_SZ = "Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256", this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "Encryption type for password protected Office Open XML files" to "Enabled (Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256)".

Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

1.6 DTOO190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The encryption type for password protected Office 97 thru Office 2003 must be set.

```
GROUP ID: V-238029
RULE ID: SV-238029r961128
```

Rationale:

This policy setting enables you to specify an encryption type for password-protected Office 97-2003 files. If you enable this policy setting, you can specify the type of encryption that Office applications will use to encrypt password-protected files in the older Office 97-2003 file formats. The chosen encryption type must have a corresponding cryptographic service provider (CSP) installed on the computer that encrypts the file. See the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\ registry key for a list of CSPs installed on the local computer. Specify the encryption type to use by entering it in the provided text box in the following form:<Encryption Provider>,<Encryption Algorithm>,<Encryption Key Length>.For example, Microsoft Enhanced Cryptographic Provider v1.0,RC4,128. If you do not configure this policy setting, Excel, PowerPoint, and Word use Office 97/2000 Compatible encryption, a proprietary encryption method, to encrypt password-protected Office 97-2003 files.

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "Encryption type for password protected Office 97-2003 files" is set to "Enabled (Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256)".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\common\security

Criteria: If the value DefaultEncryption12 is REG_SZ = "Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256", this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "Encryption type for password protected Office 97-2003 files" to "Enabled (Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256)".

Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

1.7 DTOO191 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

ActiveX control initialization must be disabled.

```
GROUP ID: V-238030
RULE ID: SV-238030r961779
```

Rationale:

This policy setting specifies the Microsoft ActiveX« initialization security level for all Microsoft Office applications. ActiveX controls can adversely affect a computer directly. 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. If a control is not marked SFI, it is possible that the control could adversely affect a computer--or it could mean that the developers did not test the control in all situations and are not sure whether it might be compromised in the future. If you enable this policy setting, you can set the ActiveX security level to a number between 1 and 6. These security levels are as follows: 1 - Regardless of how the control is marked, load it and use the persisted values (if any). This setting does not prompt the user. 2 - If SFI, load the control in safe mode and use persisted values (if any). If not SFI, load in unsafe mode with persisted values (if any), or use the default (first-time initialization) settings. This level is similar to the default configuration, but does not prompt the user. 3 - If SFI, load the control in unsafe mode and use persisted values (if any). If not SFI, prompt the user and advise them that it is marked unsafe. If the user chooses No at the prompt, do not load the control. Otherwise, load it with default (first-time initialization) settings. 4 - If SFI, load the control in safe mode and use persisted values (if any). If not SFI, prompt the user and advise them that it is marked unsafe. If the user chooses No at the prompt, do not load the control. Otherwise, load it with default (first-time initialization) settings. 5 - If SFI, load the control in unsafe mode and use persisted values (if any). If not SFI, prompt the user and advise them that it is marked unsafe. If the user chooses No at the prompt, do not load the control. Otherwise, load it with persisted values. 6 - If SFI, load the control in safe mode and use persisted values (if any). If not SFI, prompt the user and advise them that it is marked unsafe. If the user chooses No at the prompt, do not load the control. Otherwise, load it with persisted values. If you disable or do not configure this policy setting, if a control is marked SFI, the application loads the control in safe mode and uses persisted values (if any). If the control is not marked SFI, the application loads the control in unsafe mode with persisted values (if any), or uses the default (first-time initialization) settings. In both situations, the Message Bar informs users that the controls have been disabled and prompts them to respond. 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. 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.

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "ActiveX Control Initialization" is set to "Disabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\Common\Security

Criteria: If the value UFIControls exists, this is a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "ActiveX Control Initialization" to "Disabled".

Additional Information:

CCI-002460 Enforce organization-defined actions prior to executing mobile code.

- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.8 DTOO192 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Load controls in forms3 must be disabled from loading.

```
GROUP ID: V-238031
RULE ID: SV-238031r961086
```

Rationale:

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). 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. If you enable this policy setting, you can choose from four options for loading controls in UserForms: 1- For a UFI or SFI signed control that supports safe and unsafe mode, load the control in unsafe mode. For an SFI signed control that only supports a safe mode configuration, load the control in safe mode. This option enforces the default configuration. 2 - Users are prompted to determine how UserForm forms will load. The prompt only displays once per session within an application. When users respond to the prompt, loading continues based on whether the control is UFI or SFI: - For a UFI signed control, if users respond Yes to the prompt, load the control in unsafe mode. If users respond No, load the control using the default properties. - For an SFI signed control that supports both safe and unsafe modes, if users respond Yes to the prompt, load the control in unsafe mode. If users respond No, load the control using safe mode. If the SFI control can only support safe mode, load the control in safe mode. This option is the default configuration in the Microsoft Office 2016 release. 3 - Users are prompted to determine how UserForm forms will load. The prompt only displays once per session within an application. When users respond to the prompt, loading continues based on whether the control is UFI or SFI: - For a UFI signed control, if users respond Yes to the prompt, load the control in unsafe mode. If users respond No, load the control with its default properties. - For an SFI signed control, load in safe mode. 4 - For a UFI signed control, load with the default properties of the control. For an SFI signed control, load in safe mode (considered to be the safest mode). If you disable or do not configure this policy setting, the behavior is as if you enable this policy setting and then select option 1.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings "Load Controls in Forms3" is set to Enabled and 1 from drop-down menu.

(For a UFI or SFI signed control that supports safe and unsafe mode, load the control in unsafe mode. For an SFI signed control that only supports a safe mode configuration, load the control in safe mode. This option enforces the default configuration.) Setting "Load Controls in Forms3" to disabled is also acceptable.

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\vba\security

If the value for "LoadControlsInForms3" does not exist or if the value for "LoadControlsInForms" is REG_DWORD=1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings "Load Controls in Forms3" to "Enabled" and 1 from the drop-down menu, or set it to "Disabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.9 DTOO193 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Automation Security to enforce macro level security in Office documents must be configured.

```
GROUP ID: V-238032
RULE ID: SV-238032r961092
```

Rationale:

This policy setting controls whether macros can run in an Office 2016 application that is opened programmatically by another application. If you enable this policy setting, you can choose from three options for controlling macro behavior in Excel, PowerPoint, and Word when the application is opened programmatically: - Disable macros by default - All macros are disabled in the programmatically opened application. - Macros enabled (default) - Macros can run in the programmatically opened application. This option enforces the default configuration in Excel, PowerPoint, and Word. - User application macro security level - Macro functionality is determined by the setting in the "Macro Settings" section of the Trust Center. If you disable or do not configure this policy setting, when a separate program is used to launch Microsoft Excel, PowerPoint, or Word programmatically, any macros can run in the programmatically opened application without being blocked.

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "Automation Security" is set to "Enabled (Use application macro security level)".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\Common\Security

Criteria: If the value AutomationSecurity is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "Automation Security" to "Enabled (Use application macro security level)".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.10 DTOO196 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A mix of policy and user locations for Office Products must be disallowed.

```
GROUP ID: V-238033
RULE ID: SV-238033r961863
```

Rationale:

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. If you enable this policy setting, 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. If you disable this policy setting, all trusted locations that are not created by Group Policy are disabled and users cannot create new trusted locations in the Trust Center. If you do not configure this policy setting, the behavior is the equivalent of setting the policy to Enabled. Note - InfoPath 2016 and Outlook 2016 do not recognize trusted locations, and therefore are unaffected by this policy setting.

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings -> Trust Center "Allow mix of policy and user locations" is set to "Disabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\common\security\trusted locations

Criteria: If the value Allow User Locations is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings -> Trust Center "Allow mix of policy and user locations" to "Disabled".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.11 DTOO197 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Smart Documents use of Manifests in Office must be disallowed.

```
GROUP ID: V-238034
RULE ID: SV-238034r961863
```

Rationale:

This policy setting controls whether Office 2016 applications can load an XML expansion pack manifest file with a Smart Document. 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 2016 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. If you enable this policy setting, Office 2016 applications cannot load XML expansion packs with Smart Documents. If you disable or do not configure this policy setting, Office 2016 applications can load an XML expansion pack manifest file with a Smart Document.

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Smart Documents (Word, Excel) "Disable Smart Document's use of manifests" is set to "Enabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\Common\Smart Tag

Criteria: If the value NeverLoadManifests is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Smart Documents (Word, Excel) "Disable Smart Document's use of manifests" to "Enabled".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.12 DTOO201 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Connection verification of permissions must be enforced.

```
GROUP ID: V-238035
RULE ID: SV-238035r961353
```

Rationale:

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. If you enable this policy setting, users are required to connect to verify permissions. This policy setting will only affect protected files created on machines where the policy is enabled. If you disable or do not configure this policy setting, users are not required to connect to the network to verify permissions.

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Manage Restricted Permissions "Always require users to connect to verify permission" is set to "Enabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\common\drm

Criteria: If the value RequireConnection is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Manage Restricted Permissions "Always require users to connect to verify permission" to "Enabled".

Additional Information:

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (10)
- NIST SP 800-53 Revision 5::AC-6 (10)

1.13 DTOO206 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Inclusion of document properties for PDF and XPS output must be disallowed.

```
GROUP ID: V-238036
RULE ID: SV-238036r961863
```

Rationale:

This policy setting controls whether document metadata can be saved in PDF and XPS documents. If you enable this policy setting, document properties metadata is not exported to PDF and XPS files. If you disable this policy setting, document properties metadata will always be saved with PDF and XPS files, and users will not be able to override this configuration. If you do not configure this policy setting, if the Microsoft Save as PDF or XPS Add-in for Microsoft Office Programs add-in is installed, document properties are saved as metadata when users save files using the PDF or XPS or Publish as PDF or XPS commands in Access, Excel, InfoPath, PowerPoint, and Word, unless the "Document properties" option is unchecked in the Options dialog.

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Microsoft Save As PDF and XPS add-ins "Disable inclusion of document properties in PDF and XPS output" is set to "Enabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\common\fixedformat

Criteria: If the value DisableFixedFormatDocProperties is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Microsoft Save As PDF and XPS add-ins "Disable inclusion of document properties in PDF and XPS output" to "Enabled".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.14 DTOO321 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Encrypt document properties must be configured for OLE documents.

```
GROUP ID: V-238037
RULE ID: SV-238037r961602
```

Rationale:

This policy setting allows you configure if the document properties are encrypted. This applies to OLE documents (Office 97-2003 compatible) if the application is configured for CAPI RC4. If you enable this policy setting, the document properties will be encrypted. If you disable or do not configure this policy setting, the document properties will not be encrypted.

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "Encrypt document properties" is set to "Enabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\common\security

Criteria: If the value EncryptDocProps is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings "Encrypt document properties" to "Enabled".

Additional Information:

CCI-002476 Implement cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4::SC-28 (1)
- NIST SP 800-53 Revision 5::SC-28 (1)

1.15 DTOO408 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Office Presentation Service must be removed as an option for presenting PowerPoint and Word online.

```
GROUP ID: V-238038
RULE ID: SV-238038r960963
```

Rationale:

This policy setting allows you to remove Office Presentation Service from the list of online presentation services in PowerPoint and Word. This list appears when a user selects Present Online from the Share tab in Backstage view and in the ribbon in PowerPoint. If you enable this policy setting, Office Presentation Service is not shown as an option for presenting online. If you disable or do not configure this policy setting, users can select Office Presentation Service to present their PowerPoint or Word file to other users online.

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Present Online -> "Remove Office Presentation Service from the list of online presentation services in PowerPoint and Word" is set to "Enabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\Microsoft\office\16.0\common\broadcast

Criteria: If the value disabledefaultservice is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Present Online -> "Remove Office Presentation Service from the list of online presentation services in PowerPoint and Word" to "Enabled".

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.16 DTOO409 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The ability to create an online presentation programmatically must be disabled.

```
GROUP ID: V-238039
RULE ID: SV-238039r961092
```

Rationale:

This policy setting allows you to restrict the ability to create an online presentation programmatically in PowerPoint and Word. If you enable this policy setting, an online presentation cannot be created programmatically. If you disable or do not configure this policy setting, an online presentation can be created programmatically.

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Present Online -> "Restrict programmatic access for creating online presentations in PowerPoint and Word" is set to "Enabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\Microsoft\office\16.0\common\broadcast

Criteria: If the value disableprogrammaticaccess is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Present Online -> "Restrict programmatic access for creating online presentations in PowerPoint and Word" to "Enabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.17 DTOO410 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

When using the Office Feedback tool, the ability to include a screenshot must be disabled.

```
GROUP ID: V-238040
RULE ID: SV-238040r961863
```

Rationale:

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. If you enable this policy setting, the Office Feedback Tool will allow the user to send a screenshot of their desktop with their feedback to Microsoft. 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. If you do not configure this policy setting, the behavior is the equivalent of setting the policy to "Enabled".

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Privacy >> Trust Center >> "Allow users to include screenshots and attachments when they submit feedback to Microsoft" is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\Microsoft\office\16.0\common\feedback

If the value "includescreenshot" is "REG_DWORD = 0", this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Privacy >> Trust Center >> "Allow users to include screenshots and attachments when they submit feedback to Microsoft" to "Disabled".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.18 DTOO412 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The ability to run unsecure Office web add-ins and Catalogs must be disabled.

```
GROUP ID: V-238041
RULE ID: SV-238041r961863
```

Rationale:

This policy setting allows users to run unsecure web add-in, which are add-ins that have web page or catalog locations that are not SSL-secured (https://), and are not in users' Internet zones. If you enable this policy setting, users can run unsecure apps. To enable specific unsecure web add-ins, you must also configure the Trusted Web add-in Catalog policy settings to trust the catalogs that contains those Add-ins. If you disable or do not configure this policy setting, unsecure web add-ins are not allowed.

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings -> Trust Center -> Trusted Catalogs "Allow Unsecure web add-ins and Catalogs" is set to "Disabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\Microsoft\office\16.0\wef\trustedcatalogs

Criteria: If the value requireserververification is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Security Settings -> Trust Center -> Trusted Catalogs "Allow Unsecure web add-ins and Catalogs" to "Disabled".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.19 DTOO416 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Office Telemetry Agent must be configured to obfuscate the file name, file path, and title of Office documents before uploading telemetry data to the shared folder.

```
GROUP ID: V-238042
RULE ID: SV-238042r1047204
```

Rationale:

This policy setting configures Office Telemetry Agent to disguise, or obfuscate, certain file properties that are reported in telemetry data. If this policy setting is enabled, Office Telemetry Agent obfuscates the file name, file path, and title of Office documents before uploading telemetry data to the shared folder. If this policy setting is disabled or not configured, Office Telemetry Agent uploads telemetry data that shows the full file name, file path, and title of all Office documents.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Telemetry Dashboard >> "Turn on privacy setting in Office Telemetry Agent" is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\Microsoft\office\16.0\osm

If the value "enablefileobfuscation" is "REG_DWORD = 1", this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 .> Telemetry Dashboard >> "Turn on privacy settings in Office Telemetry Agent" to "Enabled".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.20 DTOO601 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The ability to send personal information to Office must be disabled.

```
GROUP ID: V-238043
RULE ID: SV-238043r961863
```

Rationale:

This policy setting controls whether users can send personal information to Office. When users choose to send information Office 2016 applications automatically send information to Office. If you enable this policy setting, users will opt into sending personal information to Office. If your organization has policies that govern the use of external resources, opting users into the program might cause them to violate these policies. If you disable this policy setting, Office 2016 users cannot send personal information to Office. If you do not configure this policy setting, the behavior is the equivalent of setting the policy to "Enabled".

Audit:

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Privacy -> Trust Center -> "Send personal information" is set to "Disabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\Microsoft\office\16.0\common

Criteria: If the value sendcustomerdata is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Office 2016 -> Privacy -> Trust Center -> "Send personal information" to "Disabled".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	DTOO182 (Manual)	☐	☐
1.2	DTOO186 (Manual)	☐	☐
1.3	DTOO187 (Manual)	☐	☐
1.4	DTOO188 (Manual)	☐	☐
1.5	DTOO189 (Manual)	☐	☐
1.6	DTOO190 (Manual)	☐	☐
1.7	DTOO191 (Manual)	☐	☐
1.8	DTOO192 (Manual)	☐	☐
1.9	DTOO193 (Manual)	☐	☐
1.10	DTOO196 (Manual)	☐	☐
1.11	DTOO197 (Manual)	☐	☐
1.12	DTOO201 (Manual)	☐	☐
1.13	DTOO206 (Manual)	☐	☐
1.14	DTOO321 (Manual)	☐	☐
1.15	DTOO408 (Manual)	☐	☐
1.16	DTOO409 (Manual)	☐	☐
1.17	DTOO410 (Manual)	☐	☐
1.18	DTOO412 (Manual)	☐	☐
1.19	DTOO416 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	DTOO601 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 27, 2025	1.0.0	Initial CIS Release