Australian Government
Australian Signals Directorate

Restricting Microsoft Office Macros

First published: November 2012
Last updated: October 2021

Introduction

This publication has been developed to discuss different approaches that organisations can use to protect their systems and data from malicious Microsoft Office macros. By understanding the business requirements for the use of macros, and applying the recommendations in this publication, organisations can effectively manage the risk of allowing macros in their environments.

The names and locations of Group Policy settings used in this publication are taken from Microsoft Office 2016 and are equally applicable to Microsoft 365, Office 2021 and Office 2019.

Macros explained

What are macros?

Microsoft Office files can contain embedded code, known as a macro, that is written in the Visual Basic for Applications (VBA) programming language. These macros can contain a series of commands that have been coded or recorded and are able to be replayed at a later time in order to automate repetitive tasks. Macros are powerful tools that can be easily created by users to greatly improve their productivity, however, malicious actors can also create macros to perform a variety of malicious activities, such as assisting in the compromise of systems in order to exfiltrate or deny access to sensitive data.

How are macros verified and trusted?

Microsoft Office allows users to provide information about themselves by digitally signing their macros. Digital signing certificates for macros can be self-generated by users, obtained from a commercial Certificate Authority or obtained from an organisation's own Certificate Authority.

Alternatively, Microsoft Office offers 'trusted document' and 'trusted location' functionality. Once trusted documents or trusted locations are defined, macros within trusted documents, or macros within Microsoft Office files opened from trusted locations, will automatically execute. While the use of trusted documents is discouraged, trusted locations, when implemented in a secure manner, can allow organisations to balance both their business and security requirements.

How can I determine which macros to trust?

To securely manage the use of macros within an organisation, all macros should be checked by assessors, that are independent of macro developers, to ensure that they are safe before being digitally signed or placed within trusted locations.

When assessing whether macros are safe, assessors should ask themselves the following questions:

- Is there a business requirement for this particular macro?
- Has the macro been developed or provided by a trusted party?
- Is the macro free of signs of malicious code or malicious functionality?

Approaches to macro security

The following table displays the security benefit, business impact and implementation difficulty of different approaches to managing macros in Microsoft Office files.

Approach	Security Benefit	Potential Business Friction	Implementation Difficulty
All macros are disabled	Very High	High	Low
Macros digitally signed by trusted publishers are enabled	High	Medium	High
Macros from trusted locations are enabled	High	High	High
Users decide which macros to enable on a case-by-case basis (with additional security measures)	Medium	Medium	Medium
Users decide which macros to enable on a case-by-case basis (with no additional security measures)	Low	Low	None
All macros are enabled	None	None	Low

All macros are disabled

Support for macro use should be disabled across the entire Microsoft Office suite. In addition, to prevent users or malicious actors from bypassing macro security measures, support for trusted documents and trusted locations should be disabled.

This approach should be the default approach implemented for users that do not have a demonstrated business requirement for macro use.

Macros digitally signed by trusted publishers are enabled

If users have a demonstrated business requirement for macro use, approved macros in Microsoft Office files that have been digitally signed by a trusted publisher can be allowed to execute. However, to prevent users or malicious actors from bypassing macro security measures, support for trusted documents and trusted locations should be disabled (unless trusted locations are also used in which case they should also be secured).

To further reduce the likelihood of malicious actors signing a malicious macro and it being executed by users, the ability to enable macros signed by an untrusted publisher, or add additional trusted publishers, should be disabled for users. This includes via the Message Bar, Backstage View, Internet Options control panel applet and any certificate management tools. In addition, ideally the list of trusted publishers should be limited to only signing certificates that an organisation controls themselves (thereby limiting the risk of third-party signing certificates being targeted and compromised as part of a cyber supply chain attack by a malicious actor).

Macros from trusted locations are enabled

If users have a demonstrated business requirement for macro use, approved macros in Microsoft Office files from trusted locations can be allowed to execute. However, to prevent users or malicious actors from bypassing macro security measures, support for trusted documents and trusted publishers should be disabled (unless trusted publishers are also used in which case they should also be secured).

Furthermore, trusted locations should prevent all users, except for a limited number of approved users, from adding or modifying macros in Microsoft Office files in these locations. Using an appropriately secured network path as a trusted location can assist in the centralised management and control of approved macros. Note, however, this approach is limited in that users will not be able to reuse macros once they save files outside of trusted locations (which they will be forced to do the first time they save a file as all files opened from trusted locations will initially be read-only).

Users decide which macros to enable on a case-by-case basis (with additional security measures)

If users have a demonstrated business requirement for macro use, they can approve the execution of macros on a case-by-case basis. However, as relying on users to make correct security decisions every time is not realistic, additional security measures should be implemented, such as blocking macros in Microsoft Office files originating from internet, using macro antivirus scanning and preventing macros from making Win32 API calls.

Users decide which macros to enable on a case-by-case basis (with no additional security measures)

If users have a demonstrated business requirement for macro use, they can approve the execution of macros on a case-by-case basis. However, as relying on users to make correct security decisions every time is not realistic, and in the absence of additional security measures or safeguards, this presents a significant risk and is not recommended.

All macros are enabled

Allowing unrestricted execution of macros presents a serious risk for organisations and should never be implemented.

Securing systems against malicious macros

Recommended approaches to macro security

To protect themselves against malicious macros, organisations should implement one of, or a combination of, the following approaches (in order of preference):

- all macros are disabled
- macros digitally signed by trusted publishers are enabled
- macros from trusted locations are enabled
- users decide which macros to enable on a case-by-case basis (with additional security measures).

Additional security measures

In addition to the recommended approaches above, organisations should:

- implement an application control solution to mitigate malicious macros running unapproved applications
- implement email and web content filtering rules (where supported) to inspect incoming Microsoft Office files for macros, and block or quarantine them as appropriate
- implement macro execution logging to verify only approved macros are used
- ensure users assigned to assessing the safety of macros have appropriate VBA training in order to be able to identify signs of malicious code or malicious functionality
- prevent users from changing macro security settings within Microsoft Office applications.

Recommended Group Policy settings

The following Group Policy settings should be implemented depending on an organisation's desired approach to managing macros in Microsoft Office files.

Microsoft Windows

Group Policy Setting	All Macros Disabled	Macros from Trusted Locations	Macros Digitally Signed by Trusted Publishers	Users Decide (With Additional Security)
Computer Configuration\Policies\Administration Templates\Windows Components\Internet Explorer\Internet Control Panel				
Disable the Content page	N/A	N/A	Enabled	N/A
User Configuration\Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins				
Certificates	N/A	N/A	Disabled	N/A

Microsoft Office 2016

Group Policy Setting	All Macros Disabled	Macros from Trusted Locations	Macros Digitally Signed by Trusted Publishers	Users Decide (With Additional Security)
User Configuration\Policies\Administration Templates\Microsoft Office 2016\Security Settings				
Automation Security	Enabled Set the Automation Security level: Disable macros by default	Enabled Set the Automation Security level: Use application macro security level	Enabled Set the Automation Security level: Use application macro security level	Enabled Set the Automation Security level: Use application macro security level
Disable all Trust Bar notifications for security issues	N/A	N/A	Enabled	Disabled
Disable VBA for Office applications	Enabled	Disabled	Disabled	Disabled
Macro Runtime Scan Scope	N/A	Enable for all documents	Enable for all documents	Enable for all documents
User Configuration\Policies\Administration Templates\Microsoft Office 2016\Security Settings\Trust Center				
Allow mix of policy and user locations	Disabled	Disabled	Disabled	Disabled

Microsoft Access 2016

Group Policy Setting	All Macros Disabled	Macros from Trusted Locations	Macros Digitally Signed by Trusted Publishers	Users Decide (With Additional Security)
User Configuration\Policies\Administration Templates\Microsoft Access 2016\Application Settings\Security\Trust Center				
Block macros from running in Office files from the Internet	N/A	Enabled	Enabled	Enabled
Turn off trusted documents	Enabled	Enabled	Enabled	Enabled
Turn off Trusted Documents on the network	Enabled	Enabled	Enabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification	Enabled Disable all except digitally signed macros	Enabled Disable all with notification
User Configuration\Policies\Administration Templates\Microsoft Access 2016\Application Settings\Security\Trust Center\Trusted Locations				
Allow Trusted Locations on the network	Disabled	Enabled	Disabled	Disabled
Disable all trusted locations	Enabled	Disabled	Enabled	Enabled
User Configuration\Policies\Administration Templates\Microsoft Access 2016\Disable Items in User Interface\Custom				
Disable commands	N/A	N/A	Enabled Enter a command bar ID to disable: 19092	N/A

Microsoft Excel 2016

Group Policy Setting	All Macros Disabled	Macros from Trusted Locations	Macros Digitally Signed by Trusted Publishers	Users Decide (With Additional Security)
User Configuration\Policies\Administration Templates\Microsoft Excel 2016\Disable Items in User Interface\Custom				
Disable commands	N/A	N/A	Enabled Enter a command bar ID to disable: 19092	N/A
User Configuration\Policies\Administration Templates\Microsoft Excel 2016\Excel Options\Security				
Scan encrypted macros in Excel Open XML workbooks	N/A	Scan encrypted macros (default)	Scan encrypted macros (default)	Scan encrypted macros (default)
User Configuration\Policies\Administration Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center				
Block macros from running in Office files from the Internet	N/A	Enabled	Enabled	Enabled
Trust access to Visual Basic Project	Disabled	Disabled	Disabled	Disabled
Turn off trusted documents	Enabled	Enabled	Enabled	Enabled
Turn off Trusted Documents on the network	Enabled	Enabled	Enabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification	Enabled Disable all except digitally signed macros	Enabled Disable all with notification
User Configuration\Policies\Administration Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center\Trusted Locations				
Allow Trusted Locations on the network	Disabled	Enabled	Disabled	Disabled
Disable all trusted locations	Enabled	Disabled	Enabled	Enabled

Microsoft Outlook 2016

Group Policy Setting	All Macros Disabled	Macros from Trusted Locations	Macros Digitally Signed by Trusted Publishers	Users Decide (With Additional Security)
User Configuration\Policies\Administration Templates\Microsoft Outlook 2016\Disable Items in User Interface\Custom				
Disable commands	N/A	N/A	Enabled Enter a command bar ID to disable: 19092	N/A
User Configuration\Policies\Administration Templates\Microsoft Outlook 2016\Security\Trust Center				
Apply macro security settings to macros, add-ins and additional actions	Enabled	Enabled	Enabled	Enabled
Security settings for macros	Enabled Security Level: Never warn, disable all	Enabled Security Level: Never warn, disable all	Enabled Security Level: Warn for signed, disable unsigned	Enabled Security Level: Always warn

Microsoft PowerPoint 2016

Group Policy Setting	All Macros Disabled	Macros from Trusted Locations	Macros Digitally Signed by Trusted Publishers	Users Decide (With Additional Security)
User Configuration\Policies\Administration Templates\Microsoft PowerPoint 2016\Disable Items in User Interface\Custom				
Disable commands	N/A	N/A	Enabled Enter a command bar ID to disable: 19092	N/A
User Configuration\Policies\Administration Templates\Microsoft PowerPoint 2016\PowerPoint Options\Security				
Scan encrypted macros in PowerPoint Open XML presentations	N/A	Scan encrypted macros (default)	Scan encrypted macros (default)	Scan encrypted macros (default)
User Configuration\Policies\Administration Templates\Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center				

Block macros from running in Office files from the Internet	N/A	Enabled	Enabled	Enabled
Trust access to Visual Basic Project	Disabled	Disabled	Disabled	Disabled
Turn off trusted documents	Enabled	Enabled	Enabled	Enabled
Turn off Trusted Documents on the network	Enabled	Enabled	Enabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification	Enabled Disable all except digitally signed macros	Enabled Disable all with notification
User Configuration\Policies\Administration Templates\Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\Trusted Locations				
Allow Trusted Locations on the network	Disabled	Enabled	Disabled	Disabled
Disable all trusted locations	Enabled	Disabled	Enabled	Enabled

Microsoft Project 2016

Group Policy Setting	All Macros Disabled	Macros from Trusted Locations	Macros Digitally Signed by Trusted Publishers	Users Decide (With Additional Security)
User Configuration\Policies\Administration Templates\Microsoft Project 2016\Project Options\Security\Trust Center				
Allow Trusted Locations on the network	Disabled	Enabled	Disabled	Disabled
Disable all trusted locations	Enabled	Disabled	Enabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification	Enabled Disable all except digitally signed macros	Enabled Disable all with notification

Microsoft Publisher 2016

Group Policy Setting	All Macros Disabled	Macros from Trusted Locations	Macros Digitally Signed by Trusted Publishers	Users Decide (With Additional Security)
User Configuration\Policies\Administration Templates\Microsoft Publisher 2016\Disable Items in User Interface\Custom				
Disable commands	N/A	N/A	Enabled Enter a command bar ID to disable: 19092	N/A
User Configuration\Policies\Administration Templates\Microsoft Publisher 2016\Security				
Publisher Automation Security Level	Enabled High (disabled)	Enabled High (disabled)	Enabled By UI (prompted)	Enabled By UI (prompted)
User Configuration\Policies\Administration Templates\Microsoft Publisher 2016\Security\Trust Center				
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification	Enabled Disable all except digitally signed macros	Enabled Disable all with notification

Microsoft Visio 2016

Group Policy Setting	All Macros Disabled	Macros from Trusted Locations	Macros Digitally Signed by Trusted Publishers	Users Decide (With Additional Security)
User Configuration\Policies\Administration Templates\Microsoft Visio 2016\Disable Items in User Interface\Custom				
Disable commands	N/A	N/A	Enabled Enter a command bar ID to disable: 19092	N/A
User Configuration\Policies\Administration Templates\Microsoft Visio 2016\Visio Options\Security\Macro Security				
Enable Microsoft Visual Basic for Applications project creation	Disabled	Disabled	Disabled	Disabled
Load Microsoft Visual Basic for Applications projects from text	Disabled	Disabled	Disabled	Disabled

User Configuration\Policies\Administration Templates\Microsoft Visio 2016\Visio Options\Security\Trust Center				
Allow Trusted Locations on the network	Disabled	Enabled	Disabled	Disabled
Block macros from running in Office files from the Internet	N/A	Enabled	Enabled	Enabled
Disable all trusted locations	Enabled	Disabled	Enabled	Enabled
Turn off trusted documents	Enabled	Enabled	Enabled	Enabled
Turn off Trusted Documents on the network	Enabled	Enabled	Enabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification	Enabled Disable all except digitally signed macros	Enabled Disable all with notification

Microsoft Word 2016

Group Policy Setting	All Macros Disabled	Macros from Trusted Locations	Macros Digitally Signed by Trusted Publishers	Users Decide (With Additional Security)
User Configuration\Policies\Administration Templates\Microsoft Word 2016\Disable Items in User Interface\Custom				
Disable commands	N/A	N/A	Enabled Enter a command bar ID to disable: 19092	N/A
User Configuration\Policies\Administration Templates\Microsoft Word 2016\Word Options\Security				
Scan encrypted macros in Word Open XML documents	N/A	Scan encrypted macros (default)	Scan encrypted macros (default)	Scan encrypted macros (default)
User Configuration\Policies\Administration Templates\Microsoft Word 2016\Word Options\Security\Trust Center				
Block macros from running in Office files from the Internet	N/A	Enabled	Enabled	Enabled

Trust access to Visual Basic Project	Disabled	Disabled	Disabled	Disabled
Turn off trusted documents	Enabled	Enabled	Enabled	Enabled
Turn off Trusted Documents on the network	Enabled	Enabled	Enabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification	Enabled Disable all except digitally signed macros	Enabled Disable all with notification
User Configuration\Policies\Administration Templates\Microsoft Word 2016\Word Options\Security\Trust Center\Trusted Locations				
Allow Trusted Locations on the network	Disabled	Enabled	Disabled	Disabled
Disable all trusted locations	Enabled	Disabled	Enabled	Enabled

Microsoft Defender Antivirus

Group Policy Setting	All Macros Disabled	Macros from Trusted Locations	Macros Digitally Signed by Trusted Publishers	Users Decide (With Additional Security)
Computer Configuration\Policies\Administration Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction				
Configure Attack Surface Reduction rules	N/A	Enabled Set the state for each ASR rule: 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B (1)	Enabled Set the state for each ASR rule: 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B (1)	Enabled Set the state for each ASR rule: 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B (1)

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Contact details

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