March 2016

Microsoft Office Macro Security

Introduction

1. Microsoft Office applications can execute macros to automate routine tasks. However, macros can contain malicious code resulting in unauthorised access to sensitive information as part of a targeted cyber intrusion.
2. This document has been developed by the Australian Signals Directorate (ASD) to introduce approaches that can be applied by organisations to secure systems against malicious macros while balancing both their business and security requirements. The names and locations of group policy settings used in this document are taken from Microsoft Office 2013; some slight differences may exist for earlier or later versions of Microsoft Office.

Background

3. The Australian Cyber Security Centre (ACSC) has seen an increasing number of attempts to compromise organisations using malicious macros.
4. Adversaries have been observed using social engineering techniques to entice users into executing malicious macros in Microsoft Office files. The purpose of these malicious macros can range from cybercrime to more sophisticated exploitation attempts.
5. By understanding the business requirements for the use of macros, and applying the recommendations in this document, organisations can effectively manage the risk of allowing macros in their environments.

Macros explained

What are macros?

6. Microsoft Office files can contain embedded code (known as a macro) written in the Visual Basic for Applications (VBA) programming language.
7. A macro can contain a series of commands that can be coded or recorded, and replayed at a later time to automate repetitive tasks. Macros are powerful tools that can be easily created by novice users to greatly improve their productivity. However, adversaries can also create macros to perform a variety of malicious activities, such as compromising workstations in order to exfiltrate sensitive information.

How are macros verified and trusted?

8. Microsoft Office has both trusted document and trusted location functions. Once trusted documents or trusted locations are defined, macros in trusted documents or macros in Microsoft Office files stored in trusted locations automatically execute when the Microsoft Office files are opened. While the use of trusted documents is discouraged, trusted locations when

implemented in a controlled manner can allow organisations to appropriately balance both their business and security requirements.

9. Microsoft Authenticode allows developers to include information about themselves and their macro code by digitally signing their macros. The certificate that is used to create a signed macro confirms that the macro originated from the signatory, while the signature itself confirms that the macro has not been altered. Digital certificates can be obtained from a commercial Certificate Authority (CA) or from an organisation's security administrator if they operate their own CA service. It is important to note that macro code, either legitimate or malicious, can be self-signed or signed using a commercial CA.

10. By defining trusted publishers in Microsoft Windows, organisations can allow authorised signed macros to execute without users receiving a security warning. However, unauthorised signed macros can still be executed by users if they enable the macro from the Trust Bar or Info page in the Microsoft Office application's backstage view.

How to determine which macros to trust

11. When determining whether to trust macros, organisations should ask themselves the following questions:

    a. Is there a business requirement for a particular macro?

    b. Has the macro been validated by a trustworthy and technically skilled party?

    c. Has the macro been signed by a trusted publisher and an approved CA?

Approaches to securing systems against malicious macros

12. The following table displays the security, business impact and implementation difficulty of different approaches to securing systems against malicious macros.

Approach	Security	Business Impact	Implementation Difficulty	Recommended
Disable all macros and trusted locations	Very high	High	Low	Yes
Disable all macros but allow controlled trusted locations	High	Medium	Medium	Yes
Disable all macros, except digitally signed macros, and disable trusted locations	Medium	Medium	High	No
Let users decide which macros to enable on a case-by-case basis	Low	Low	Low	No
Enable all macros	None	None	Low	No

13. To protect against malicious macros, organisations should balance both their business and security requirements. Ideally, this should be the *very high* or *high* security approaches in the table above. Further information on specific group policy settings relating to *very high* and *high* security approaches can be found in paragraphs 15 to 21, and **Appendix A**.

14. In addition to applying the group policy settings in **Appendix A**, organisations should:

    a. implement application whitelisting to mitigate a malicious macro running unauthorised programs

    b. implement email and web content filtering to inspect incoming Microsoft Office files for macros, and block or quarantine them as appropriate

c. implement macro execution logging to verify only authorised macros are used in their environment e.g. by logging the execution of known file extensions such as dotm, docm, xlsm, pptm and ppsm

d. ensure privileged users assigned to assessing macro code have appropriate VBA training.

Approaches to securing systems against malicious macros explained

Very high security approach – Disable all macros and trusted locations

15. If organisations do not have a business requirement for macro use, support for their use should be disabled across the Microsoft Office suite.

16. To prevent users or adversaries from bypassing macro security controls, all support for trusted documents and trusted locations should be disabled.

17. To ensure users cannot knowingly or unintentionally alter macro security controls via a Microsoft Office application's Trust Center interface, organisations should apply macro security controls using group policy settings.

High security approach – Disable all macros but allow controlled trusted locations

18. If organisations have a business requirement for macro use, only approved macros in Microsoft Office files stored in trusted locations should be allowed to execute. Further, only specific Microsoft Office applications for which there is a business requirement for macro use should be allowed to execute approved macros. All other Microsoft Office applications should have support for macros, trusted documents and trusted locations disabled.

19. To prevent users or adversaries from bypassing macro security controls, support for trusted documents should be disabled while trusted locations should prevent all users, except for approved privileged users, from adding or modifying macros in Microsoft Office files stored in these locations. Using an appropriately secured network path as a trusted location can assist in the centralised management and control of macros in Microsoft Office files.

20. To manage the development and use of macros, organisations should create appropriate user groups that include macro developers, macro approvers and macro users. All macros created by an organisation's macro developers, or third parties, that macro users have a business requirement to execute should be reviewed by a macro approver and assessed to be safe before being approved. This should not be done with an administrator account but a macro approver account that is only used for checking macros and adding or modifying macros in Microsoft Office files stored in trusted locations. Macro users should be limited to only those users that are required to execute macros.

21. To ensure users cannot knowingly or unintentionally alter macro security controls via a Microsoft Office application's Trust Center interface, organisations should apply macro security controls using group policy settings.

Understanding macro settings

22. There are several group policy settings associated with Microsoft Office that organisations should configure to protect themselves from malicious macros.

VBA Macro Notification Settings

23. The *VBA Macro Notification Settings* policy controls how specific Microsoft Office applications warn users when macros are present in Microsoft Office files.

Office Application	Group Policy	Policy Value	Policy Description	Recommended

Access, Excel, PowerPoint, Project, Publisher, Visio and Word	VBA Macro Notification Settings	Enabled – Disable all without notification	All macros are disabled. Users are not notified of macros in Microsoft Office files.	**Yes** – Helps prevent users from knowingly or unintentionally executing malicious macros in Microsoft Office files by removing their ability to make security decisions.
		Enabled – Disable all except digitally signed macros	Macros are allowed to execute if they have been digitally signed by a trusted publisher. If a macro has been digitally signed by a publisher that is not trusted, users are prompted via the Trust Bar to enable the macro. If the user selects enable, the publisher will become recognised as trusted, thereby allowing the macro to execute.	**No** – Users should not be relied upon to make correct security decisions.
		Enabled – Disable all with notification	**Default behaviour** – Macros are disabled by default. However, users are prompted via the Trust Bar to enable macros on a case-by-case basis.	**No** – Users should not be relied upon to make correct security decisions.
		Disabled	Macro security will be determined by the policy value selected by users in each Microsoft Office application's Trust Center interface.	**No** – Users should not be relied upon to make correct security decisions.
		Enabled – Enable all macros	All macros are enabled. Users are not notified of macros in Microsoft Office files.	**No** – There is nothing stopping malicious macros in Microsoft Office files from executing.

Disable all trusted locations

24. Trusted locations are used to store macros in Microsoft Office files that have been assessed by a macro approver to be safe. The *Disable all trusted locations* policy controls whether specific Microsoft Office applications are able to use trusted locations.

Office Application	Group Policy	Policy Value	Policy Description	Recommended
Access, Excel, InfoPath, PowerPoint, Project, Visio and Word	Disable all trusted locations	Enabled	Microsoft Office applications won't use trusted locations. As such, Microsoft Office files will be subject to any specified macro security controls when opened by users.	**Yes (very high security approach)** – Helps prevent users from knowingly or unintentionally executing malicious macros in Microsoft Office files by removing their ability to use or specify trusted locations to open Microsoft Office files from, thereby

				bypassing macro security controls. **No (high security approach)** – Preventing the management and control of macros in Microsoft Office files by organisations.
		Disabled	**Default behaviour** – Microsoft Office applications will automatically execute macros in Microsoft Office files stored in trusted locations.	**No (very high security approach)** – Users may be able to knowingly or unintentionally execute malicious macros in Microsoft Office files if they have write access to any specified trusted locations or they are able to specify their own trusted locations. **Yes (high security approach)** – Using an appropriately secured path as a trusted location can assist organisations in the management and control of macros in Microsoft Office files.

Allow Trusted Locations on the network

25. Once trusted locations are enabled, the *Allow Trusted Locations on the network* policy controls the use of network paths as trusted locations by specific Microsoft Office applications.

Office Application	Group Policy	Policy Value	Policy Description	Recommended
Access, Excel, PowerPoint, Project, Visio and Word	Allow Trusted Locations on the network	Disabled	**Default behaviour** – Microsoft Office applications won't use trusted locations on the network. As such, Microsoft Office files will be subject to any specified macro security controls when opened by users.	**Yes (very high security approach)** – Helps prevent users from knowingly or unintentionally executing malicious macros in Microsoft Office files by removing their ability to use or specify trusted locations on the network to open Microsoft Office files from, thereby bypassing macro security controls. **No (high security approach)** – Prevents the centralised management and control of macros in Microsoft Office files by organisations.
		Enabled	Microsoft Office applications will automatically execute macros in Microsoft Office files stored in trusted locations on the network.	**No (very high security approach)** – Users may be able to knowingly or unintentionally execute malicious macros in Microsoft Office files if they have write access to any specified

				trusted locations on the network or they are able to specify their own trusted locations on the network. **Yes (high security approach)** – Using an appropriately secured network path as a trusted location can assist organisations in the centralised management and control of macros in Microsoft Office files.

Allow mix of policy and user locations

26. The *Allow mix of policy and user locations* policy controls whether trusted locations can be specified only through group policy settings or through a mix of group policy settings and user specified settings.

Office Application	Group Policy	Policy Value	Policy Description	Recommended
All	Allow mix of policy and user locations	Disabled	Only trusted locations that are specified in group policy settings are used.	**Yes** – If trusted locations are enabled, this helps prevent users from knowingly or unintentionally executing malicious macros in Microsoft Office files by removing their ability to specify trusted locations to open Microsoft Office files from, thereby bypassing macro security controls.
		Enabled	**Default behaviour** – In addition to trusted locations specified in group policy settings, users can specify trusted locations via a Microsoft Office application's Trust Center interface.	**No** – If trusted locations are enabled, users can knowingly or unintentionally execute malicious macros in Microsoft Office files by specifying trusted locations to open Microsoft Office files from, thereby bypassing macro security controls.

Turn off trusted documents

27. Trusted documents are Microsoft Office files that are assessed by a user to be safe. The *Turn off trusted documents* policy controls whether specific Microsoft Office applications are able to execute macros in trusted documents.

Office Application	Group Policy	Policy Value	Policy Description	Recommended
Access, Excel, PowerPoint, Visio and Word	Turn off trusted documents	Enabled	Users won't be able to specify any trusted documents. As such, Microsoft Office files will be subject to any specified macro security controls when opened by users.	**Yes** – Helps prevent users from knowingly or unintentionally executing malicious macros in Microsoft Office files by preventing them from either specifying Microsoft Office files as trusted documents or by

				adding or modifying macros in existing Microsoft Office documents which have already been trusted by other users.
		Disabled	**Default behaviour** – Users can specify whether macros and other types of active content in Microsoft Office files are safe. Subsequently, even if changes are made to the macros or other active content, the Microsoft Office file will be treated as safe and automatically execute macros and other active content when opened by users.	**No** – Users can knowingly or unintentionally execute malicious macros in Microsoft Office files by either specifying Microsoft Office files as trusted documents or by adding or modifying macros in existing Microsoft Office documents which have already been trusted by other users.

Turn off Trusted Documents on the network

28. Once trusted documents are enabled, the *Turn off Trusted Documents on the network* policy controls the use of trusted documents from network paths by specific Microsoft Office applications.

Office Application	Group Policy	Policy Value	Policy Description	Recommended
Access, Excel, PowerPoint, Visio and Word	Turn off Trusted Documents on the network	Enabled	Users won't be able to specify any trusted documents from network paths. As such, Microsoft Office files will be subject to any specified macro security controls when opened by users.	**Yes** – Helps prevent users from knowingly or unintentionally executing malicious macros in Microsoft Office files from network paths by preventing them from either specifying Microsoft Office files as trusted documents or by adding or modifying macros in existing Microsoft Office documents which have already been trusted by other users.
		Disabled	**Default behaviour** – Users can specify whether macros and other types of active content in Microsoft Office files from network paths are safe. Subsequently, even if changes are made to the macros or other active content, the Microsoft Office file will be treated as safe and automatically execute macros and other active content when opened by users.	**No** – Users can knowingly or unintentionally execute malicious macros in Microsoft Office files from network paths by either specifying Microsoft Office files as trusted documents or by adding or modifying macros in existing Microsoft Office documents which have already been trusted by other users. This security risk is especially high for Microsoft Office files stored in network paths that all users have access to and have an ongoing requirement to access e.g. letter or brief templates.

Disable all Trust Bar notifications for security issues

29. The *Disable all Trust Bar notifications for security issues* policy controls whether the Trust Bar is displayed in Microsoft Office applications. The Trust Bar notifies users via a security warning that macros have been disabled. Users can then select to enable the macro allowing it to execute.

Office Application	Group Policy	Policy Value	Policy Description	Recommended
All	Disable all Trust Bar notifications for security issues	Enabled	The Trust Bar is not displayed in Microsoft Office applications.	**Yes** – Helps prevent users from knowingly or unintentionally executing malicious macros in Microsoft Office files by preventing them from interactively allowing macros to execute. Note, this policy setting won't prevent users from allowing macros via the Info page in the Microsoft Office application's backstage view.
		Disabled	**Default behaviour** – The Trust Bar is displayed in Microsoft Office applications.	**No** – Users can knowingly or unintentionally execute malicious macros in Microsoft Office files by interactively allowing macros to execute when prompted by the Trust Bar upon opening a Microsoft Office file.

Automation Security

30. The *Automation Security* policy controls macro behaviour for Microsoft Excel, Microsoft PowerPoint and Microsoft Word files when launched programmatically by another application.

Office Application	Group Policy	Policy Value	Policy Description	Recommended
All	Automation Security	Enabled – Disable macros by default	Macros are disabled in Microsoft Office files launched by another application, even if macros are normally enabled for the Microsoft Office application being launched.	**Yes (very high security approach)** – Helps prevent users from knowingly or unintentionally executing malicious macros in Microsoft Office files.
		Enabled – Use application macro security level	Macros in Microsoft Office files launched by another application are enabled or disabled based on the group policy settings of the Microsoft Office application being launched.	**Yes (high security approach)** – Can be used to control macro execution on a per-Microsoft Office application basis.
		Enabled – Macros enabled (default)	**Default behaviour** – Macros in Microsoft Office files launched by another application are enabled, even if macros are	**No** – There is nothing stopping malicious macros in Microsoft Office files from executing.

			normally disabled for the Microsoft Office application being launched.	
		Disabled	Macros in Microsoft Office files launched by another application are enabled, even if macros are normally disabled for the Microsoft Office application being launched.	**No** – There is nothing stopping malicious macros in Microsoft Office files from executing.

Trust access to Visual Basic Project

31. The *Trust access to Visual Basic Project* policy controls whether automation clients can access the VBA project system in specific Microsoft Office applications.

Office Application	Group Policy	Policy Value	Policy Description	Recommended
Excel, PowerPoint and Word	Trust access to Visual Basic Project	Disabled	**Default behaviour** – Automation clients will not have programmatic access to VBA projects.	**Yes** – Helps prevent malicious applications from building self-replicating functionality.
		Enabled	Automation clients will have programmatic access to VBA projects.	**No** – Malicious applications will have full programmatic access to Visual Basic objects, methods and properties.

Security setting for macros

32. The *Security setting for macros* policy applies to Microsoft Outlook only. This policy controls the ability to execute macros in Microsoft Outlook.

Office Application	Group Policy	Policy Value	Policy Description	Recommended
Outlook	Security settings for macros	Enabled – Never warn, disable all	Macros in Microsoft Outlook are disabled.	**Yes** – Helps prevent users from knowingly or unintentionally executing malicious macros in Microsoft Outlook.
		Enabled – Warning for signed, disable unsigned	**Default behaviour** – Macros in Microsoft Outlook are allowed to execute if they have been digitally signed by a trusted publisher. If a macro has been digitally signed by a publisher that is not trusted, users are prompted to enable the macro. If the user selects enable, the publisher will become recognised as trusted, thereby allowing the macro to execute.	**No** – Users should not be relied upon to make correct security decisions.

		Enabled – Always warn	Macros in Microsoft Outlook are disabled by default. However, users are prompted to enable macros on a case-by-case basis.	**No** – Users should not be relied upon to make correct security decisions.
		Disabled	Macro security will be determined by the policy value selected by users in Microsoft Outlook's Trust Center interface.	**No** – Users should not be relied upon to make correct security decisions.
		Enabled – No security check	All macros are enabled. Users are not notified of the presence of macros in Microsoft Outlook.	**No** – There is nothing stopping malicious macros in Microsoft Outlook from executing.

Apply macro security settings to macros, add-ins and additional actions

33. The *Apply macro security settings to macros, add-ins and additional actions* policy applies to Microsoft Outlook only. If macros are not disabled for Microsoft Outlook, this policy controls whether Microsoft Outlook also applies the macro security settings to installed Component Object Model (COM) add-ins and additional actions.

Office Application	Group Policy	Policy Value	Policy Description	Recommended
Outlook	Apply macro security settings to macros, add-ins and additional actions	Enabled	Macro security settings for Microsoft Outlook will also be applied to add-ins and additional actions.	**Yes** – Malicious macros will be prevented from executing in Microsoft Outlook add-ins.
		Disabled	**Default behaviour** – Microsoft Outlook will not use macro security settings to determine whether to execute macros, install COM add-ins and additional actions.	**No** – There is nothing stopping malicious macros in Microsoft Outlook add-ins from executing.

Enable Microsoft Visual Basic for Applications project creation

34. The *Enable Microsoft Visual Basic for Applications project creation* policy applies to Microsoft Visio only. This policy controls the creation of VBA projects when opening or creating a Microsoft Visio file that does not already contain a VBA project.

Office Application	Group Policy	Policy Value	Policy Description	Recommended
Visio	Enable Microsoft Visual Basic for Applications project creation	Disabled	Users won't be able to create a macro in a Microsoft Visio file that does not already contain a VBA project.	**Yes** – Users won't be able to create malicious macros in Microsoft Visio files.
		Enabled	**Default behaviour** – Users will be able to create a macro in a Microsoft Visio file that does not already contain a VBA project.	**No** – Users will be able to create malicious macros in Microsoft Visio files.

Load Microsoft Visual Basic for Applications projects from text

35. The *Load Microsoft Visual Basic for Applications projects from text* policy applies to Microsoft Visio only. This policy enables any macro code in a Microsoft Visio file to be automatically compiled and executed with the file is opened.

Office Application	Group Policy	Policy Value	Policy Description	Recommended
Visio	Load Microsoft Visual Basic for Applications projects from text	Disabled	VBA projects are not compiled automatically when Microsoft Visio files are opened.	**Yes** – Helps prevent users from knowingly or unintentionally executing malicious macros in Microsoft Visio files by preventing the automatic compilation and execution of malicious macro code when opening Microsoft Visio files.
		Enabled	**Default behaviour** – VBA projects will be compiled automatically when Microsoft Visio files are opened	**No** – Users can knowingly or unintentionally execute malicious macros in Microsoft Visio files by automatically compiling and executing malicious macro code when opening Microsoft Visio files.

Further information

36. The *Australian Government Information Security Manual* (ISM) assists in the protection of official government information that is processed, stored or communicated by Australian Government systems. It can be found at: http://www.asd.gov.au/infosec/ism/.

37. ASD's *Strategies to Mitigate Targeted Cyber Intrusions* complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at: http://www.asd.gov.au/infosec/mitigationstrategies.htm.

Contact details

38. Australian government customers with questions regarding this advice should contact ASD Advice and Assistance by emailing asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

39. Australian businesses or other private sector organisations with questions regarding this advice should contact CERT Australia by emailing info@cert.gov.au or by calling 1300 172 499.

Appendix A: Group policy settings for Microsoft Office applications

The following group policy settings can be used to control the use of macros for Microsoft Office applications and are located in *User Configuration\Policies\Administration Template*\.

Microsoft Office

Group Policy	Policy Value (Disabled Macros)	Policy Value (Trusted Macros)
\Microsoft Office 2013\Security Settings		
Automation Security	Enabled Disable macros by default	Enabled Use application macro security level
Disable all Trust Bar notifications for security issues	Enabled	Enabled
\Microsoft Office 2013\Security Settings\Trust Center		
Allow mix of policy and user locations	Disabled	Disabled

Microsoft Access

Group Policy	Policy Value (Disabled Macros)	Policy Value (Trusted Macros)
\Microsoft Access 2013\Application Settings\Security\Trust Center		
Turn off trusted documents	Enabled	Enabled
Turn off Trusted Documents on the network	Enabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification
\Microsoft Access 2013\Application Settings\Security\Trust Center\Trusted Locations		
Allow Trusted Locations on the network	Disabled	Enabled
Disable all trusted locations	Enabled	Disabled
Trusted Location #1	N\A	Enabled Path: Path to a secure location using Universal Naming Convention (UNC). e.g. \\server\share\macros

Microsoft Excel

Group Policy	Policy Value (Disabled Macros)	Policy Value (Trusted Macros)
\Microsoft Excel 2013\Excel Options\Security\Trust Center		
Trust access to Visual Basic Project	Disabled	Disabled
Turn off trusted documents	Enabled	Enabled

Turn off Trusted Documents on the network	Enabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification
\Microsoft Excel 2013\Excel Options\Security\Trust Center\Trusted Locations		
Allow Trusted Locations on the network	Disabled	Enabled
Disable all trusted locations	Enabled	Disabled
Trusted Location #1	N\A	Enabled Path: Path to a secure location using Universal Naming Convention (UNC). e.g. \\server\share\macros

Microsoft InfoPath

Group Policy	Policy Value (Disabled Macros)	Policy Value (Trusted Macros)
\Microsoft InfoPath\Security\Trust Center		
Disable all trusted locations	Enabled	Disabled
\Microsoft InfoPath\Security\Trust Center\Trusted Locations		
Trusted Location #1	N\A	Enabled Path: Path to a secure location using Universal Naming Convention (UNC). e.g. \\server\share\macros

Microsoft Outlook

Group Policy	Policy Value (Disabled Macros)	Policy Value (Trusted Macros)
\Microsoft Outlook 2013\Security\Trust Center		
Apply macro security settings to macros, add-ins and additional actions	Enabled	Enabled
Security setting for macros	Enabled Never warn, disable all	Enabled Never warn, disable all

Microsoft PowerPoint

Group Policy	Policy Value (Disabled Macros)	Policy Value (Trusted Macros)
\Microsoft PowerPoint 2013\PowerPoint Options\Security\Trust Center		
Trust access to Visual Basic Project	Disabled	Disabled
Turn off trusted documents	Enabled	Enabled

Turn off Trusted Documents on the network	Enabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification
\Microsoft PowerPoint 2013\PowerPoint Options\Security\Trust Center\Trusted Locations		
Allow Trusted Locations on the network	Disabled	Enabled
Disable all trusted locations	Enabled	Disabled
Trusted Location #1	N\A	Enabled Path: Path to a secure location using Universal Naming Convention (UNC). e.g. \\server\share\macros

Microsoft Project

Group Policy	Policy Value (Disabled Macros)	Policy Value (Trusted Macros)
\Microsoft Project 2013\Project Options\Security\Trust Center		
Allow Trusted Locations on the network	Disabled	Enabled
Disable all trusted locations	Enabled	Disabled
Trusted Location #1	N\A	Enabled Path: Path to a secure location using Universal Naming Convention (UNC). e.g. \\server\share\macros
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification

Microsoft Publisher

Group Policy	Policy Value (Disabled Macros)	Policy Value (Trusted Macros)
\Microsoft Publisher 2013\Security\Trust Center		
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification

Microsoft Visio

Group Policy	Policy Value (Disabled Macros)	Policy Value (Trusted Macros)
\Microsoft Visio 2013\Visio Options\Security\Trust Center		
Allow Trusted Locations on the network	Disabled	Enabled

Disable all trusted locations	Enabled	Disabled
Turn off trusted documents	Enabled	Enabled
Turn off Trusted Documents on the network	Enabled	Enabled
Trusted Location #1	N\A	Enabled Path: Path to a secure location using Universal Naming Convention (UNC). e.g. \\server\share\macros
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification
\Microsoft Visio 2013\Visio Options\Security\Macro Security		
Enable Microsoft Visual Basic for Applications project creation	Disabled	Disabled
Load Microsoft Visual Basic for Applications projects from text	Disabled	Disabled

Microsoft Word

Group Policy	Policy Value (Disabled Macros)	Policy Value (Trusted Macros)
\Microsoft Word 2013\Word Options\Security\Trust Center		
Trust access to Visual Basic Project	Disabled	Disabled
Turn off trusted documents	Enabled	Enabled
Turn off Trusted Documents on the network	Enabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification
\Microsoft Word 2013\Word Options\Security\Trust Center\Trusted Locations		
Allow Trusted Locations on the network	Disabled	Enabled
Disable all trusted locations	Enabled	Disabled
Trusted Location #1	N\A	Enabled Path: Path to a secure location using Universal Naming Convention (UNC). e.g. \\server\share\macros