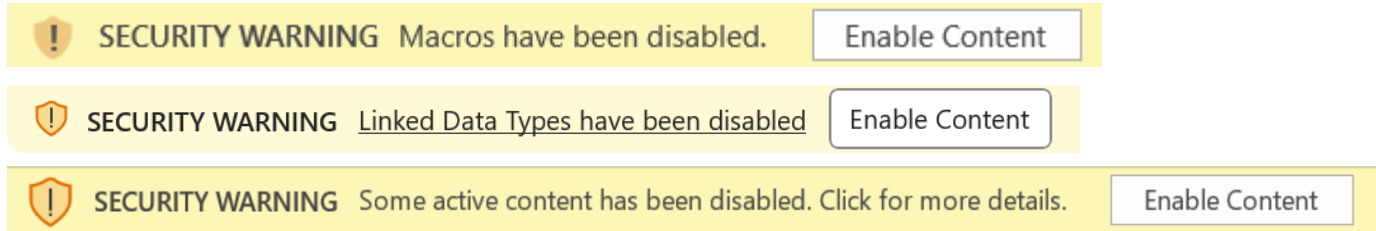


How to Ensure that Macros are Enabled

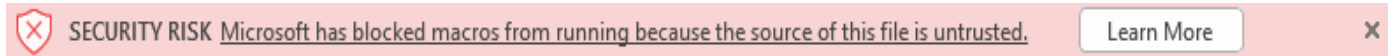
When you first open the RFA application workbook, you may see one of the following messages.

Security Warnings



If you see one of these security warnings (in yellow), click the button to Enable Content.

Security Risk



If you see this security risk warning (in pink), read the following and perform the actions indicated.

Externally Sourced Excel Files

In summer, 2022, Microsoft began blocking the macros for any files that Microsoft believes came from the Internet. For example, if someone emails you an Excel workbook or you download an Excel workbook from the Internet or you store your workbook on cloud storage. If you attempt to open a file that has the characteristics just described, upon opening, you may see a message that Microsoft has disabled macros. VBA macros are a common way for malicious actors to gain access to deploy malware and ransomware. Therefore, to help improve security in Office, Microsoft changed the default behavior of Office applications to block macros in files from the internet.

You can read more about this change that Microsoft made here ...

<https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked>

Microsoft's Security Recommendation for Macro-Enabled Files

Microsoft recommends deploying a public code-signing certificate for the trusted publisher to your users as this helps prevent your users from adding trusted publishers themselves. This method is not employed for the RFA application for several reasons:

- Higher costs
- Overkill for simple needs
- Rollout and configuration can be complex
- Possibility of slower response times and recurring application errors,

Trusted Location Method to Allow VBA Macros to Run

The simplest way to allow macros to run is by designating a *Trusted Location* on your PC's hard drive. A Trusted Location is a folder that Microsoft Office treats as secure, allowing any file stored there to run macros without being blocked. The limitation is that this protection applies only to files already inside that folder — if a file is opened from anywhere else, the Trusted Location settings will not take effect.

The steps to create a secure location are:

1. Open Excel. A blank workbook is fine.
2. On the file menu, select Options → Trust Center → Trust Center Settings

3. Select File
4. Choose Options
5. Click Trust Center
6. Select Trust Center Settings...
7. Click Trusted Locations in the left pane and review the existing trusted folders
8. Add a new Trusted Location
9. Click, "Browse" and select or create a folder on your PC. You can optionally also check that subfolders of this location are also trusted.
10. Click OK to save.
11. Confirm Security Settings
 - a. Only trust folders you fully control
 - b. Ensure files placed here come from known, safe sources
12. Using MS File Explorer, move or copy the file(s) to the new trusted location.
13. Close the Office app (Excel, Word, etc.) and reopen it selecting the file you want to run and ensure that the macro-enabled file runs as expected.

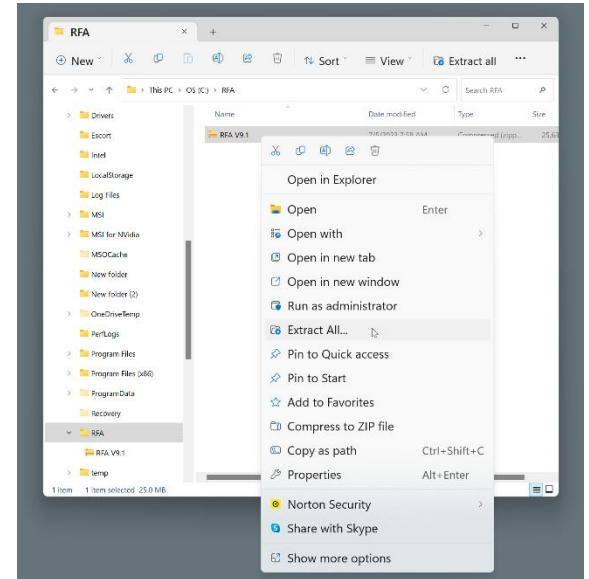


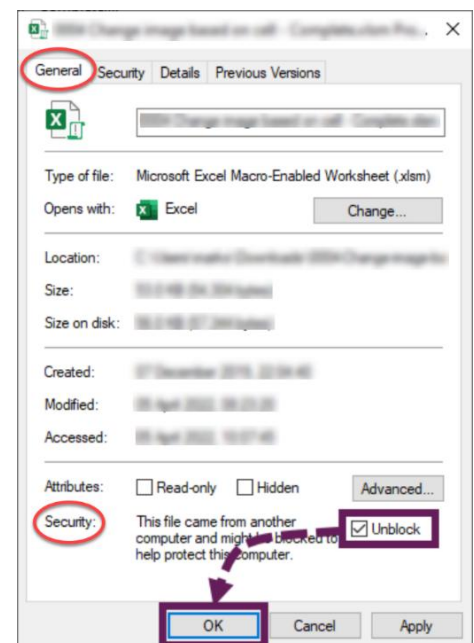
Figure 1: File Explorer Right Click Window

Trusted Document Method to Allow VBA Macros to Run

This method allows you to trust a single file that you manually approve. Once trusted, Office will remember that specific file and allow its macros to run without further prompts. Use this option carefully — only when you are confident the file is safe — so you do not inadvertently grant trust to a document that should remain restricted.

The following steps assume that you are using Microsoft's File Explorer and Windows 11. If you are not familiar with File Explorer, click the Windows Start button and perform a search for File Explorer. Refer to [Figure 1: File Explorer Right Click Window](#). You should be presented with an option to select and start.

1. The RFA is distributed as a self-extracting ZIP file. When you purchased the RFA, you received a link to download the application. Once you have downloaded the file, run the file and it will unzip the contents to your hard drive and it will create a new folder on your C: drive.
2. Once you have installed the application, you can then navigate to the newly created folder on your C: drive. Look for a folder with the format C:\RFA_Vxx.x. This folder, and the sub-folders, will contain all application related files associated with the RFA application. In the top directory you should find an Excel file with the name "RFA Vx.x" with the extension of *xlsb*, which indicates it is a binary file format used by Microsoft Excel.
3. Right click the file and select "Properties" from the menu. Refer to [Figure 2: Properties Window Using File Explorer](#), for an example of File Explorer. If you see a security message that the file came from another computer and it is blocked to protect this computer, check the **Unblock** box, then click OK. If you do not see this message, move to the next step.
4. Start Microsoft Excel. A blank copy of Excel is fine.



5. In Excel, click File, Options, Add-ins
 - a. Under the add-ins, look over the active add-ins and make sure the active ones are ones you recognize and use. To make any changes to the add-ins, click manage Excel Add-ins Go button and disable any Excel add-ins that you do not need. Click OK when done.
 - b. Repeat steps 1 and 2, but this time select "COM Add-ins" from the drop-down menu. Remove or uncheck COM add-ins that are not used. Click OK.

6. Again, in Excel, click File, Options, Trust Center

7. In the Trust Center window, click "Trust Center Settings" button.

You will see several options available for you.

- a. You should not need to make any changes in **Trusted Publishers**
- b. Select **Trusted Locations**. Although not a Microsoft recommendation, you may check the box for "Allow Trusted Locations on my network" if you are placing the RFA on your internal network. Otherwise leave this unchecked (recommended).

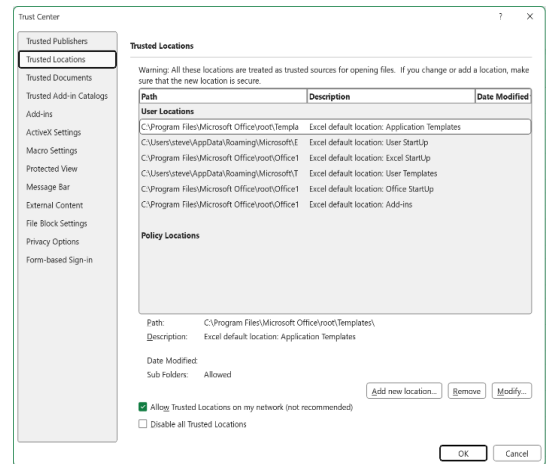


Figure 2: Properties Window Using File Explorer

You can also add a folder to the list of trusted locations. Adding a new folder will treat the location as a trusted location for any files placed in that directory ... refer to *Microsoft's Security Recommendation for Macro-Enabled Files*

- c. *Microsoft recommends deploying a public code-signing certificate for the trusted publisher to your users as this helps prevent your users from adding trusted publishers themselves. This method is not employed for the RFA application for several reasons:*
 - Higher costs
 - Overkill for simple needs
 - Rollout and configuration can be complex
 - Possibility of slower response times and recurring application errors,
- d. Trusted Location Method to Allow VBA Macros to Run.
- e. Select **Trusted Documents**. Check the box "Allow documents on a network to be trusted" if you are storing the document on a local network. Otherwise, you can leave this unchecked. If you do check this option, any files received and placed on your local network will be trusted. Microsoft discourages this.
- f. Select **Trusted Add-in Catalogs**. Uncheck all boxes.
- g. Select **Add-ins**. Uncheck all boxes on the "Add-ins" section. *Note: This section of Add-ins is under the Trust Center window, not the main options window.*
- h. Select **ActiveX Settings**. Select radio button for "Prompt me before enabling Unsafe for initialization (UFI) ..."
- i. Select **Macro Settings** option, select the radio button for "Disable VBA macros with notification" or "Enable VBA macros ...". Also, check the box for "Enable Excel 4.0 macros when VBA macros are enabled" and check the box for "Trust access to the VBA project object model".
- j. Select **Protected View**. You may choose to check or uncheck any or all of the top three boxes ...
 - Enable Protected View for files originating ...

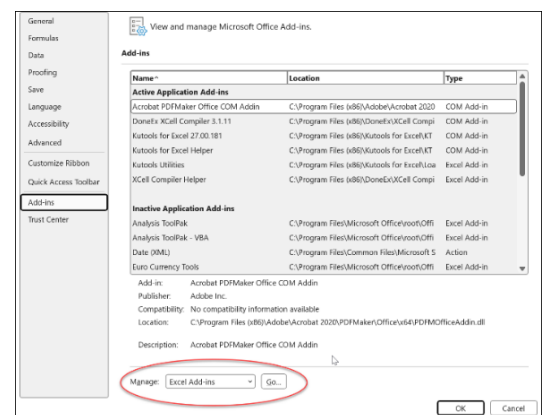


Figure 4: Excel Add-ins Option Window

- Enable Protected View for files located ...
- Enable Protected View for Outlook ...

Uncheck the two boxes ...

- i. Always open untrusted Test-Based files
 - ii. Always open untrusted Database files
- k. Select **Message Bar**. Select radio button "Show the Message Bar in all applications ..." and check the box for Policy Tips
- l. Select **External Content**.
- Select the button to Prompt user about Data Connections
 - Select the button to Prompt user on automatic update
 - Select the button to Prompt the user about Linked Data Types
 - Check the box to Enable Dynamic Data Exchange Server Lookup
 - Uncheck the box to Always block the connection of untrusted Microsoft Query files
- m. Select **File Block Settings** option, uncheck all boxes for all file types. And select the radio button, "Open selected file types in Protected View"
- n. You should not need to make any changes in **Privacy Options**.
- o. Select **Form-based Sign-in**. Select the top radio button to Block all sign-in prompts.
- p. Click OK to close the Trust Center Settings window. Click OK again to close the Options window.
8. Close Excel. Your settings will be saved and applied.
9. The above instructions will not reduce the security of your PC as any new files downloaded from the internet will be flagged and Microsoft's security will disable any macros that may be contained within the file. If you do download a new file and observe that macros have been disabled, you will likely have to adjust the properties of the file as explained above.

Setting Defaults for Microsoft Word

In addition to the above, you should ensure that the text wrapping default for Microsoft Word is set up so that when pictures are inserted, they are inserted *In Line with Text*. If you have set the default word wrapping option to other than *In Line with Text*, the reserve study report will not format correctly.

In any instance of Microsoft Word, do the following:

- Click File, Options, Advanced
- In the “Cut, copy and paste” section (you may have to scroll down in the Advanced section), ensure that “In line with text” is selected for the option “Insert/paste pictures as:”

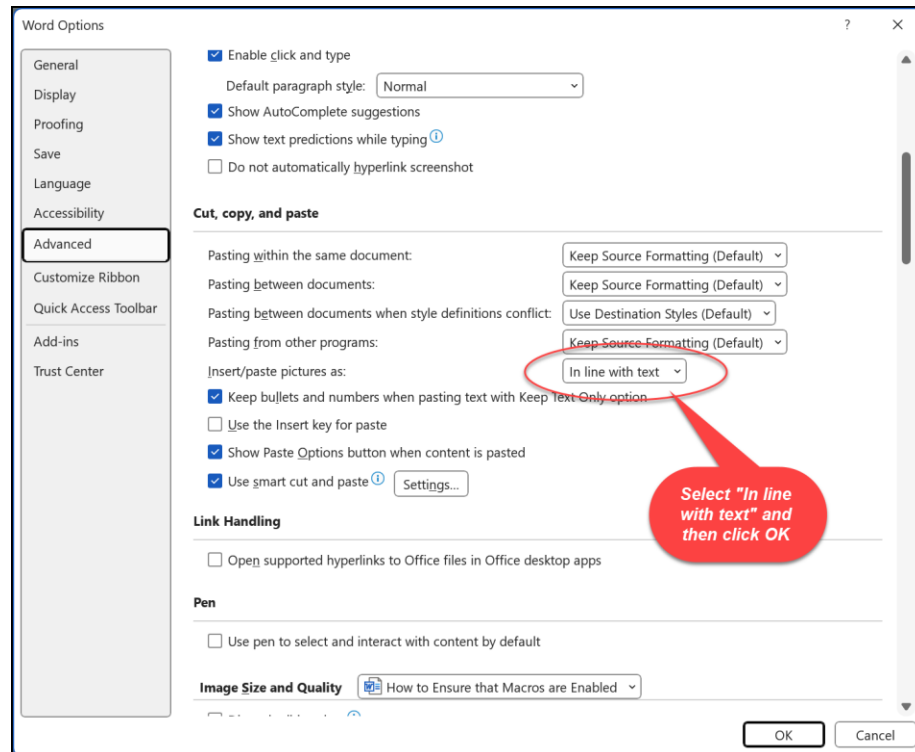


Figure 5: Word Options Advanced Window

- After selecting “OK” in the options dialog, close Word, and any change you have made will be saved.