How to access the documents in the APQP4Wind Toolbox despite security issues with macros?

出现宏安全问题，如何访问APQP4Wind工具箱中的文档？

Please be aware that some users of the **APQP4Wind Workbook** and **APQP4Wind Analysis Tool** are met with a warning regarding Microsoft security issues with macros. This is because the APQP4Wind Workbook and APQP4Wind Analysis Tool are Microsoft Excel files containing macros, which are now being blocked by default. To learn more about why **macros are being blocked by default in Office**, we recommend you visit Microsoft's website: https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked

请注意，部分用户在访问**APQP4Wind工作手册与APQP4Wind分析工具**时，遇到了有关Microsoft 宏安全问题的警告。这是因为APQP4Wind工作手册与APQP4Wind分析工具为Microsoft Excel文档，其中包含默认被阻拦的宏。如果您想进一步了解为什么**宏会在Office程序中默认被阻拦**，可参阅Microsoft网站：
https://learn.microsoft.com/zh-cn/deployoffice/security/internet-macros-blocked

What are Macros?
宏是什么？

A macro is a small program/code, often written to automate repetitive tasks in Microsoft Office applications, such as inserting the current date and time, auto-process inserted data, etc. **Macros are often created for legitimate reasons, and this is also the case for macros in the APQP4Wind Workbook and APQP4Wind Analysis Tool.**

宏是一种小程序/代码，通常用于自动执行 Microsoft Office程序中的重复性任务，例如插入当前日期和时间、自动处理插入的数据等等。**通常，宏的创立都是出于正当理由， APQP4Wind 工作手册与APQP4Wind分析工具中的宏便隶属此类。**

However, macros can also be written by attackers to gain access to or harm a system. Malicious macros can do almost anything that other malware can do to your system, including emulating ransomware, stealing data, and emailing itself out to your contacts. In fact, exploitation of these malicious macros is one of the top ways that organizations are compromised today because malicious macros are often hidden in an attached Excel Sheet in an email or downloaded content that the end-user opens and executes.

但是，攻击者也可以创建宏以访问或者破坏系统。恶意宏几乎可以对您的系统执行其他恶意软件能执行的任何操作，包括模拟勒索软件、窃取数据以及通过邮箱给您的联系人发送邮件。 事实上，恶意宏是当今组织受到伤害的主要途径之一，因为它们通常隐藏在邮件附加的 Excel 工作表中，或者终端用户可打开并执行的下载内容里。

The APQP4Wind Secretariat is aware that the use of macros in the APQP4Wind Toolbox raises some concerns for our users, and it is therefore important to emphasize that there are no malicious macros enabled in the APQP4Wind Workbook or APQP4Wind Analysis Tool. Consequently, we are in the process of finding a more suitable solution in the future.

contact@apqp4wind.org
www.apqp4wind.org
APQP4Wind

APQP4Wind
Lysbrohøjen 24
8600 Silkeborg
Denmark

APQPWind秘书处意识到APQP4Wind工具箱中宏的使用给用户带来了一些困扰，因此，我们希望在这里强调APQP4Wind工作手册与APQP4Wind分析工具当中并不包含恶意宏。目前，我们正在寻找未来更合适的解决方案。

How to access the APQP4Wind Workbook or APQP4Wind Analysis Tool documents?
如何访问 APQP4Wind 工作手册或 APQP4Wind 分析工具文档？

Until a suitable solution has been found, there are two ways to gain access to the documents:
在我们找到更佳解决方案之前，有两种访问文档的方法：

1. Save the APQP4Wind Workbook or APQP4Wind Analysis Tool locally on your computer and follow this guide: https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked#remove-mark-of-the-web-from-a-file
   or
2. Add https://apqp4wind.org as a trusted site by following this guide: https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked#files-centrally-located-on-a-network-share-or-trusted-website

1. 将APQP4Wind工作手册或APQP4Wind分析工具下载到您的电脑上，之后按照本指南进行操作：https://learn.microsoft.com/zh-cn/deployoffice/security/internet-macros-blocked#remove-mark-of-the-web-from-a-file
   或者
2. 按照本指南将 https://apqp4wind.org 添加为信任网点: https://learn.microsoft.com/zh-cn/deployoffice/security/internet-macros-blocked#files-centrally-located-on-a-network-share-or-trusted-website

APQP4Wind is dedicated to providing an APQP4Wind Toolbox that is secure for all of our users, and we apologize for any inconvenience this may have caused you. If you have any questions or concerns, please do not hesitate to contact us.

APQP4Wind致力于为所有用户提供安全的APQP4Wind工具箱，对于当前版本给您带来的任何不便，我们深表歉意。 如果您有任何问题或疑虑，请随时与我们联系。

contact@apqp4wind.org
www.apqp4wind.org
APQP4Wind

APQP4Wind
Lysbrohøjen 24
8600 Silkeborg
Denmark