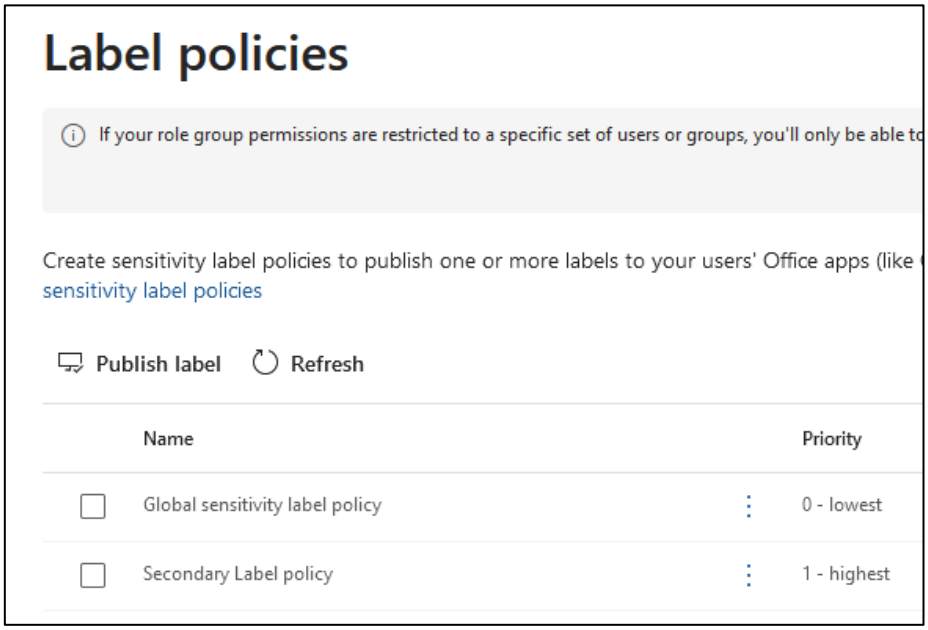
Excluding Security Mailbox-Enabled Group from Global Sensitivity Label Policy Using PowerShell

---

In this situation, two **Sensitivity Label Policies** exist:

1. **Global Sensitivity Label Policy**:
    - Contains **9 labels**, including **sub-labels**.
2. **Secondary Label Policy**:
    - Contains **4 labels** (no sub-labels).



The goal of this scenario is to **simplify the labeling experience** for a small set of users, such as a **Pilot User Group**, who should only see a specific subset of labels. These users were provided a new label set from the **Secondary Label Policy**, which includes only 4 labels for a more streamlined experience.

The Problem:

Although the Secondary Label Policy has fewer labels and is targeted for the Pilot User Group, the **Global Sensitivity Label Policy** is still applied to these users. Because there is **no label conflict** between the two policies (i.e., the labels in the Global Sensitivity Label Policy are not overridden by the Secondary Label Policy), the Pilot users continue to see **all 9 labels** from the Global Sensitivity Label Policy.

The Solution:

To resolve this, you need to **exclude the Pilot User Group** from the **Global Sensitivity Label Policy**. By excluding these users, they will no longer receive the 9 labels from the Global policy. As a result, the users will only see the **4 labels** from the Secondary Label Policy, which simplifies their labeling experience and ensures they interact only with the desired labels.

Since this configuration option is not available using the Microsoft Purview GUI, we will need to use **Powershell.**

Most of the items below came from: https://learn.microsoft.com/en-us/powershell/module/exchange/set-labelpolicy?view=exchange-ps

---

Prerequisites:

Before running the PowerShell script, ensure the following:

1. **Local Admin Access**:
    - You need to run PowerShell as an **Administrator** on your machine to install the required modules and run commands.
    - **Step**: Right-click the **Start** menu, select **Windows PowerShell (Admin)** or **Windows Terminal (Admin)**.
2. **Microsoft 365 Security Administrator Access**:
    - The person running the script must be a **Security Administrator** or have permissions to manage **Sensitivity Labels** and policies in the Microsoft 365 Compliance Center.
    - Ensure you log in with an account that has the necessary permissions (e.g., Security Admin or Global Admin).
3. **Modules**:
    - You need the **ExchangeOnlineManagement** and **Security & Compliance Center** PowerShell modules installed. Instructions on installing and connecting are included below.

Steps for First-Time Setup and Script Execution:

Step 1: Install Exchange Online Management Module

Run the following command in **PowerShell (Admin)** to install the necessary modules:

```
# Install the Exchange Online Management module

Install-Module -Name ExchangeOnlineManagement -Force -AllowClobber
```

If prompted for permission to install from an untrusted repository, type Y to proceed.

If you get this error, then follow the item in the next box

```
PS C:\WINDOWS\system32> # Import the Exchange Online Management module
>> Import-Module ExchangeOnlineManagement
>>
Import-Module : File C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.4.8.1\PackageManagement.psm1
cannot be loaded because running scripts is disabled on this system. For more information, see
about_Execution_Policies at https:/go.microsoft.com/fwlink/?LinkID=135170.
At line:2 char:1
+ Import-Module ExchangeOnlineManagement
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [Import-Module], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess,Microsoft.PowerShell.Commands.ImportModuleCommand
PS C:\WINDOWS\system32>
```

Important. You may need to change the Execution policy TEMPORARILY in your computer to run the following scripts. To set it to **Bypass**, do the following:

Temporarily Change for the Current Session:

If you only want to change the execution policy for the current session:

```
# Change execution policy for the current session (no admin required)

Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
```

Select **Y**

Important: This Bypass will only be open during this session. The moment you close the session/ powershell. This permission is removed.

Step 2: Import the Module

After installing, import the module using the following command:

```
# Import the Exchange Online Management module

Import-Module ExchangeOnlineManagement
```

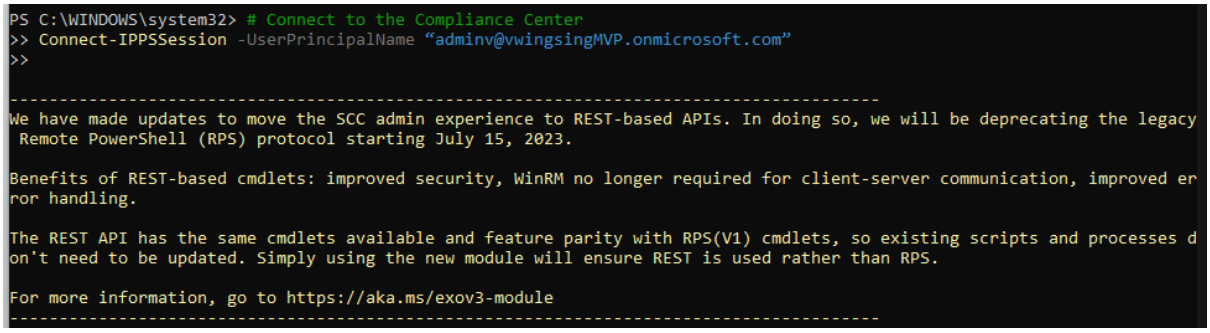
Step 3: Connect to Microsoft 365 Compliance Center

Once the module is installed and imported, connect to the **Microsoft 365 Compliance Center** using your administrator credentials:

```
# Connect to the Compliance Center

Connect-IPPSSession -UserPrincipalName "<YourAdminAccount@domain.com>"
```

Important: Replace <YourAdminAccount@domain.com> with your Security Administrator email.

You will be prompted to log in and authenticate. You will see this window



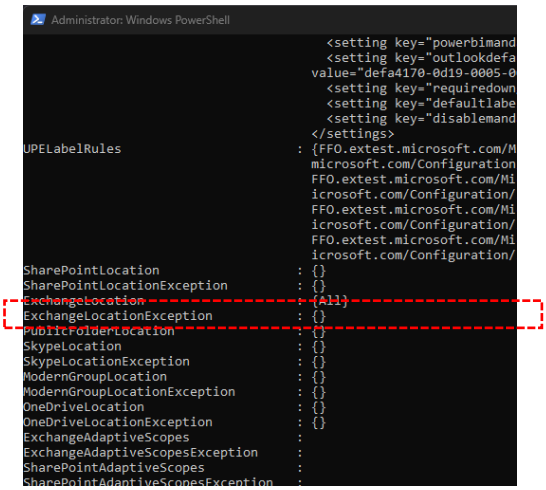
Step 4: Retrieve the Global Sensitivity Label Policy

Now, retrieve the Global Sensitivity Label Policy to confirm you are modifying the correct policy:

```
# Get all label policies

$labelPolicies = Get-LabelPolicy


# Filter for the Global Sensitivity Label Policy

$globalPolicy = $labelPolicies | Where-Object { $_.Name -eq "Global sensitivity label policy" }


# Display the details of the Global Sensitivity Label Policy

$globalPolicy | Format-List
```

This will display the Global Sensitivity Label Policy for review. (example below)

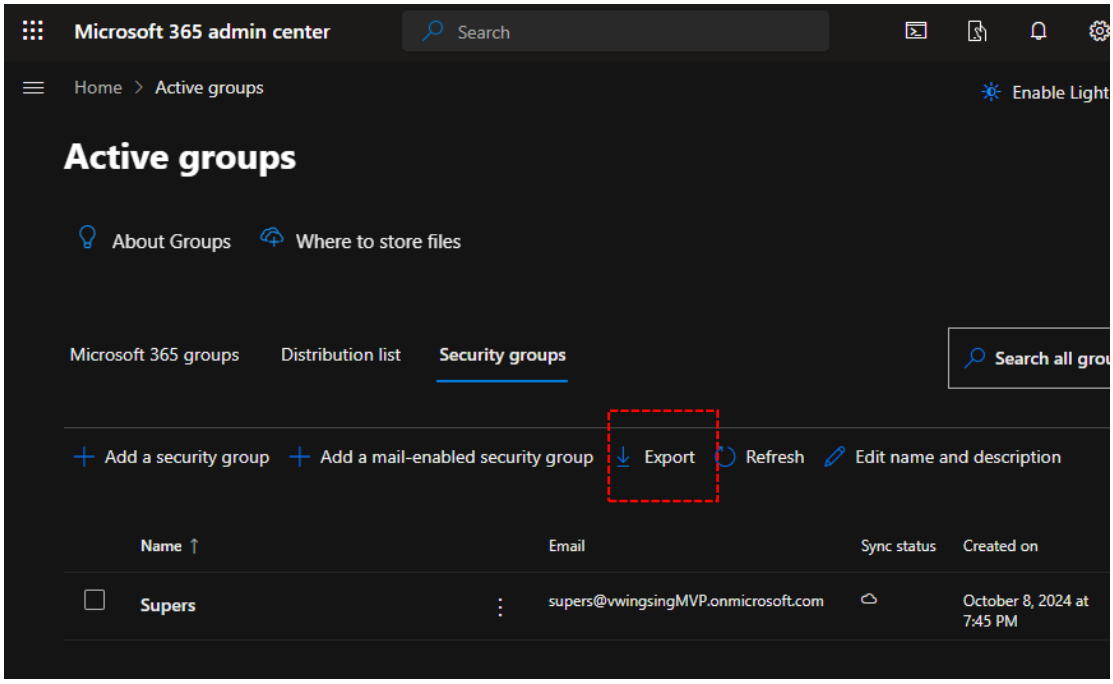
You will notice that there are currently nothing inside of the **ExchangeLocationException**



Step 5: Export the Group members in a CSV file and save it in a local folder.

Log in to Entra or Microsoft 365 admin center. Go to Security groups then Select the target group <pilotusergroup@example.com>

create an export of the target group as a CSV file



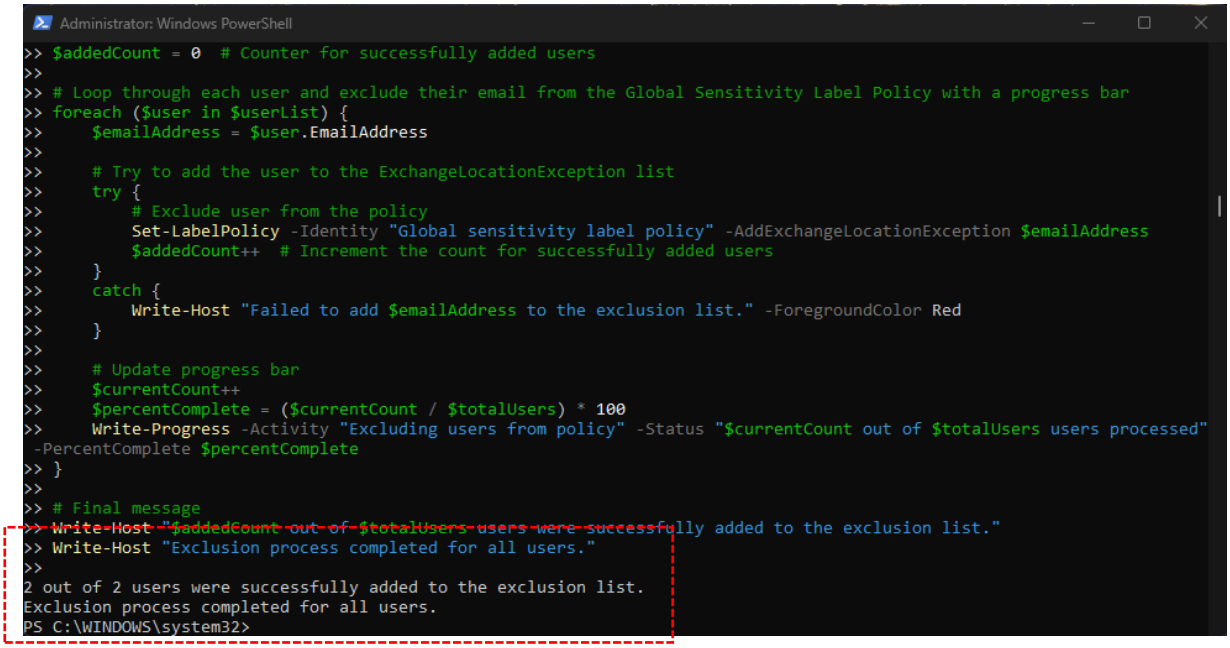
Step 6: Exclude the Group from the Policy

This step will use the exported CSV, and add them to the Exclusions

Important: Please replace the csv path with the path to your own file.

```
# Import the CSV file containing the user list
$userList = Import-Csv -Path "C:\Users\victo\OneDrive\Desktop\Members_Supers_10082024_210304.csv"

# Get the total number of users in the CSV file
$totalUsers = $userList.Count
$currentCount = 0
$addedCount = 0  # Counter for successfully added users

# Loop through each user and exclude their email from the Global Sensitivity Label Policy with a progress bar
foreach ($user in $userList) {
    $emailAddress = $user.EmailAddress

    # Try to add the user to the ExchangeLocationException list
    try {
        # Exclude user from the policy
        Set-LabelPolicy -Identity "Global sensitivity label policy" -AddExchangeLocationException $emailAddress
        $addedCount++  # Increment the count for successfully added users
    }
    catch {
        Write-Host "Failed to add $emailAddress to the exclusion list." -ForegroundColor Red
    }
    # Update progress bar
    $currentCount++
    $percentComplete = ($currentCount / $totalUsers) * 100
    Write-Progress -Activity "Excluding users from policy" -Status "$currentCount out of $totalUsers users processed" -
PercentComplete $percentComplete
}
# Final message
Write-Host "$addedCount out of $totalUsers users were successfully added to the exclusion list."
Write-Host "Exclusion process completed for all users."
```

This will display the following:

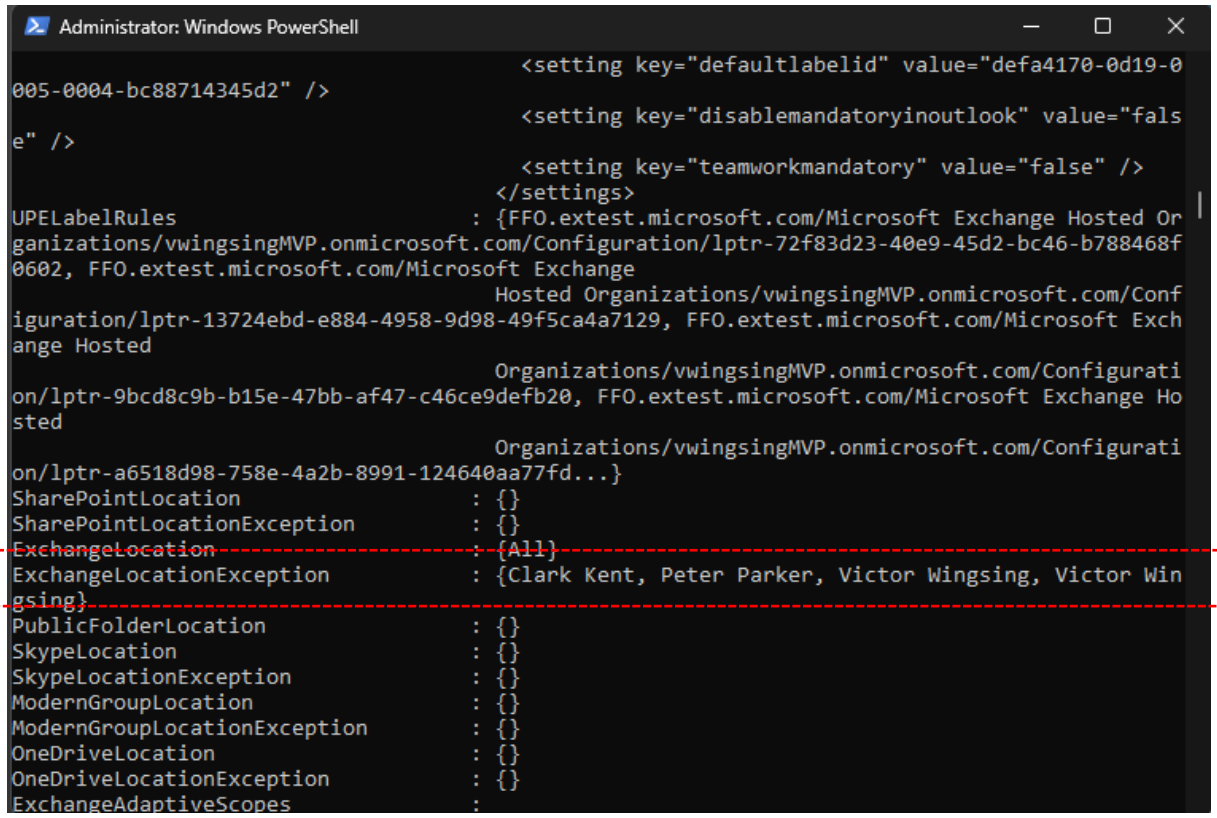


Step 6: Verify the Exclusion

After excluding the group, verify that the exclusion has been applied correctly:

```
# Verify the exclusion from the Global Sensitivity Label Policy

Get-LabelPolicy "Global sensitivity label policy"
```

Check that the group is listed under the excluded users/groups.



Step 7: Disconnect from the Session

Once the task is completed, disconnect from the session:

```
# Disconnect from Exchange Online

Disconnect-ExchangeOnline -Confirm:$false
```

Important Notes:

- Make sure that your account has the proper admin permissions (Security Admin or Global Admin) to manage Sensitivity Label Policies.
- Always confirm the policy and exclusion before applying changes to ensure you are not affecting unintended groups or users.

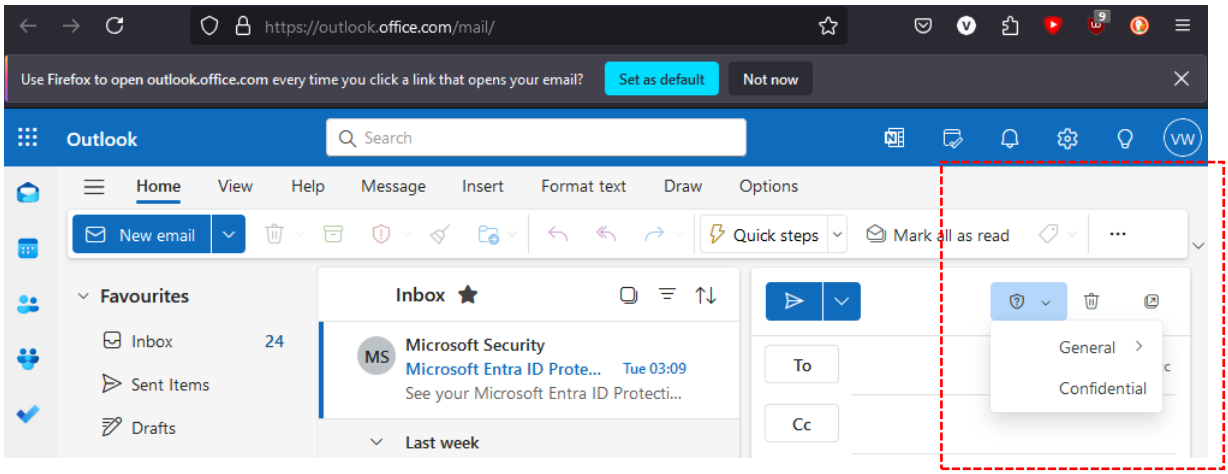
Expected outcome (end-user experience):

The labels are now excluded in Word, Excel, PowerPoint and Outlook

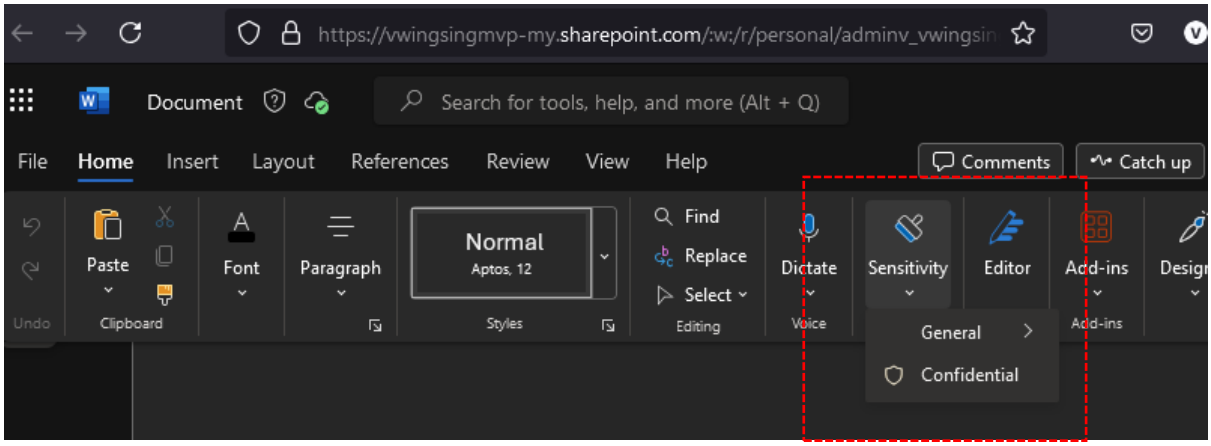
Excluded user experience

Users who have been excluded from the policy will only get a limited set of policy that is available to them.

Email



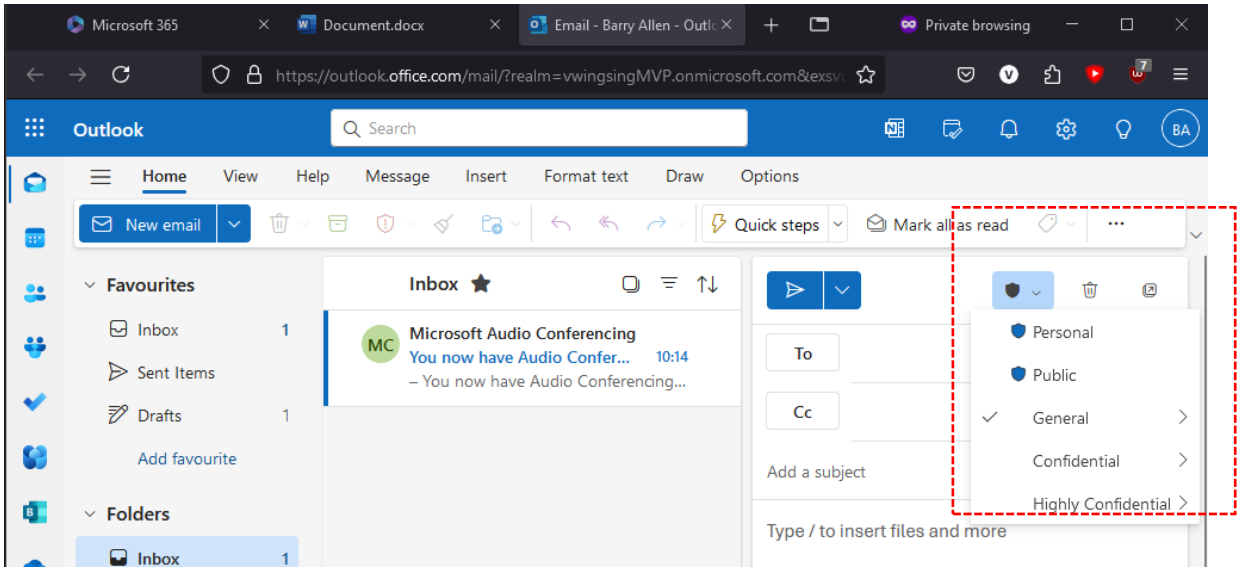
Office Docs



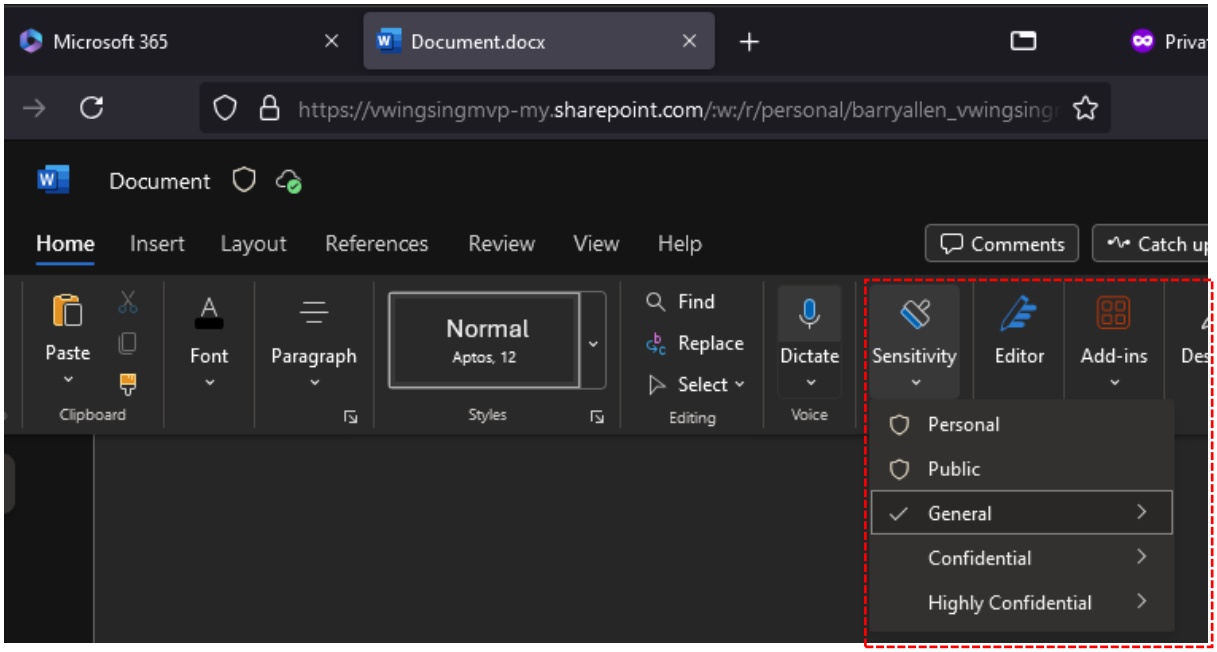
Non-excluded user experience

These users still have all the default policies.

Email



Office docs


Microsoft 365
Document.docx
https://vwingsingmvp-my.sharepoint.com/:w:/r/personal/barryallen_vwingsing
Document
Home
Insert
Layout
References
Review
View
Help
Comments
Catch up
Paste
Clipboard
Font
Paragraph
Normal
Aptos, 12
Styles
Find
Replace
Select
Editing
Dictate
Voice
Sensitivity
Editor
Add-ins
Personal
Public
General
Confidential
Highly Confidential

Removing the Exclusion.

This step will remove ALL the items that are in the Exchange Location exceptions. It will loop until it sees 0 items in the list then ends the script.

Important: Please replace the csv path with the path to your own file.

```
# Import the CSV file containing the user list

$userList = Import-Csv -Path
"C:\Users\victo\OneDrive\Desktop\Members_Supers_10082024_210304.csv"



# Loop through each user and remove their exclusion from the Global Sensitivity Label Policy

foreach ($user in $userList) {

   $emailAddress = $user.EmailAddress



   # Remove the user from the exclusion list

   Set-LabelPolicy -Identity "Global sensitivity label policy" -RemoveExchangeLocationException
$emailAddress

}



# Final message

Write-Host "All users have been removed from the exclusion list and are now back in scope."
```

You will see this screen with the status below:

```
PS C:\WINDOWS\system32> # Import the CSV file containing the user list
>> $userList = Import-Csv -Path "C:\Users\victo\OneDrive\Desktop\Members_Supers_10082024_210304.csv"
>>
>> # Loop through each user and remove their exclusion from the Global Sensitivity Label Policy
>> foreach ($user in $userList) {
>>     $emailAddress = $user.EmailAddress
>>
>>     # Remove the user from the exclusion list
>>     Set-LabelPolicy -Identity "Global sensitivity label policy" -RemoveExchangeLocationException $emailAddress
>> }
>>
>> # Final message
>> Write-Host "All users have been removed from the exclusion list and are now back in scope."
>>
All users have been removed from the exclusion list and are now back in scope.
```