
Student Name: Worlanyo Akpatsa
Student ID: 101590287
Term: Winter 2025

Lab Activity 2: Managing Microsoft 365 Compliance and Security

Objective: To learn how to configure and manage compliance and security settings in Microsoft 365.

Tasks:

1. **Set Up Data Loss Prevention (DLP) Policies**
    - Access the Microsoft 365 compliance center.
    - Create a new DLP policy to protect sensitive information (e.g., credit card numbers).
    - Configure the policy to notify users when sensitive information is detected.
    - Test the policy by attempting to send an email containing sensitive information.
2. **Implement Retention Policies**
    - Navigate to the Data life cycle management section in the compliance center.
    - Create a new retention policy for emails and documents.
    - Apply the policy to a specific group of users.
    - Verify the policy is working by checking the retention status of emails and documents.
3. **Configure and Monitor Security Alerts**
    - Access the Security center (MS Defender)
    - Set up security alerts (Medium severity) if the users created a mail forward/redirect rule.
    - Configure alert notifications to be sent to an administrator.
    - Simulate suspicious activity and verify that an alert is triggered.
4. **Review and Manage Audit Logs**
    - Enable auditing in the Microsoft 365 compliance center.
    - Search the audit log for specific activities (e.g., file deletions).
    - Export audit log data for further analysis.
    - Review the exported data to identify any unusual activities.

~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

~~~~~~~
Paste your screenshots here

STARTS ON NEXT PAGE
~~~~~~~

~~~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287

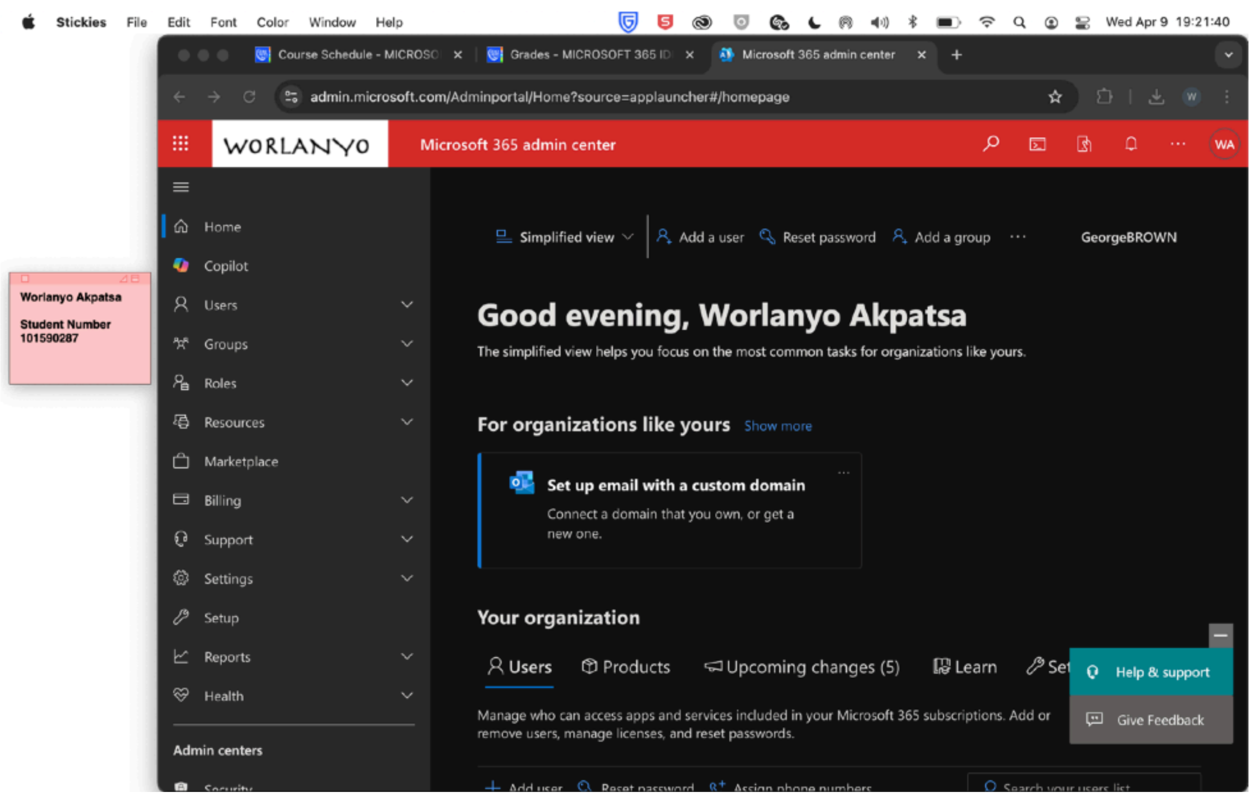
Term: Winter 2025

~~~~~~

TASK 1: SET UP DATA LOSS PREVENTION (DLP) POLICIES

1.1: Access the Microsoft 365 Compliance Center

A: Navigate to Microsoft 365 Admin Center Homepage

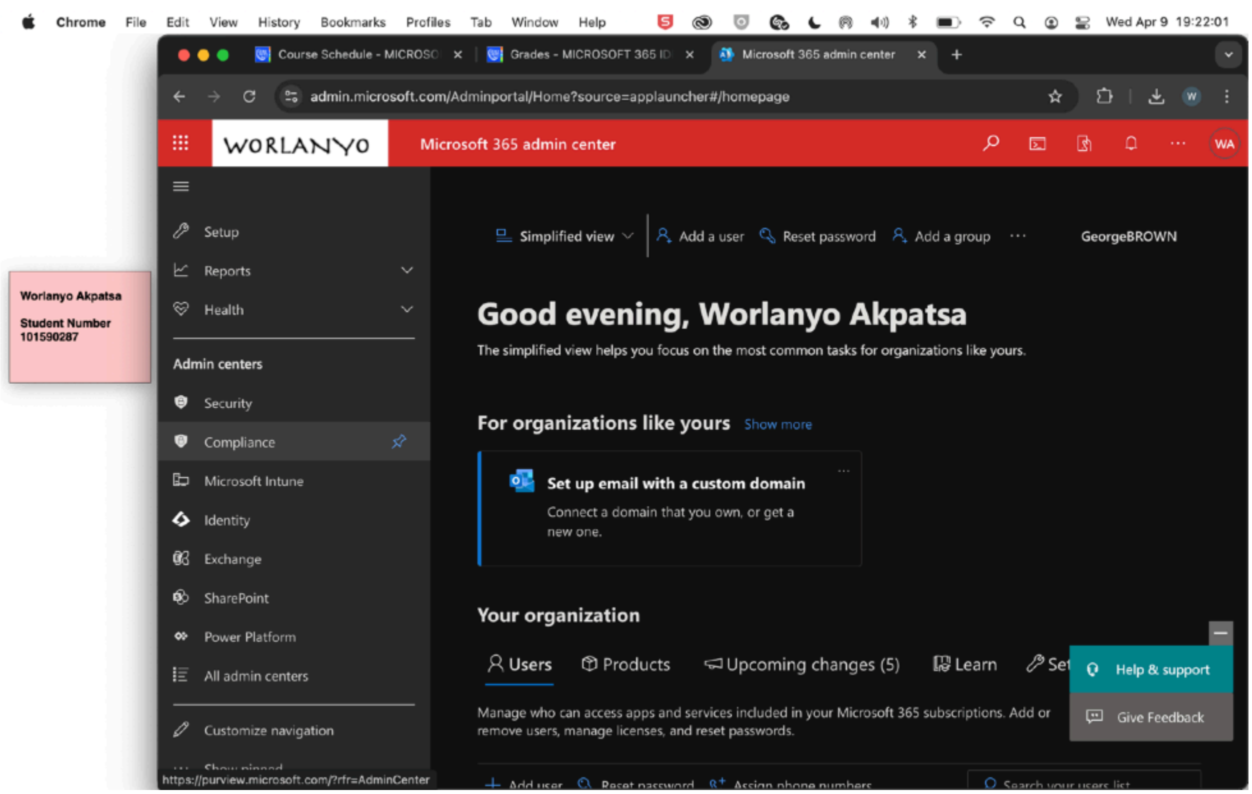


~~~~~~

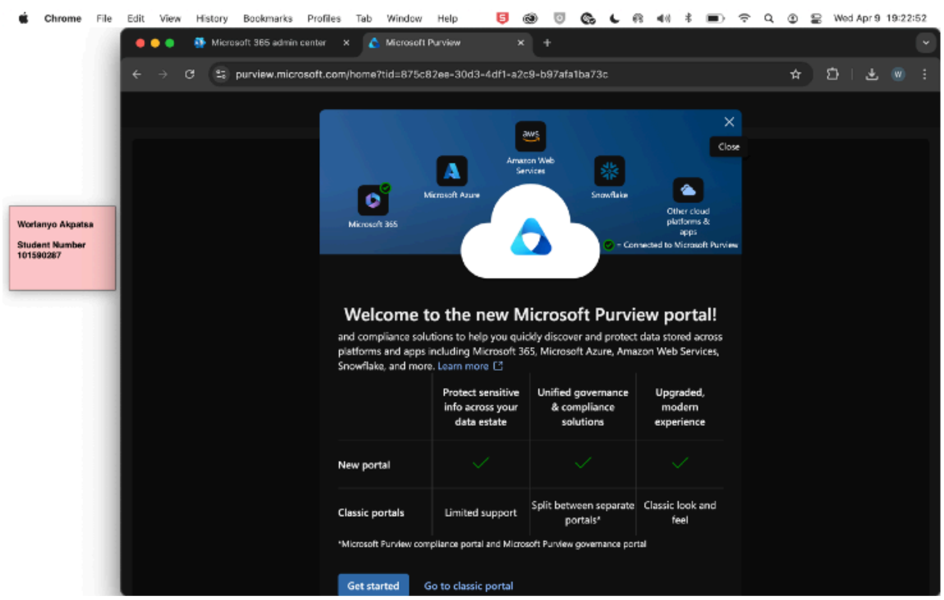
Student Name: Worlanyo Akpatsa | Term: Winter 2025
Student ID: 101590287

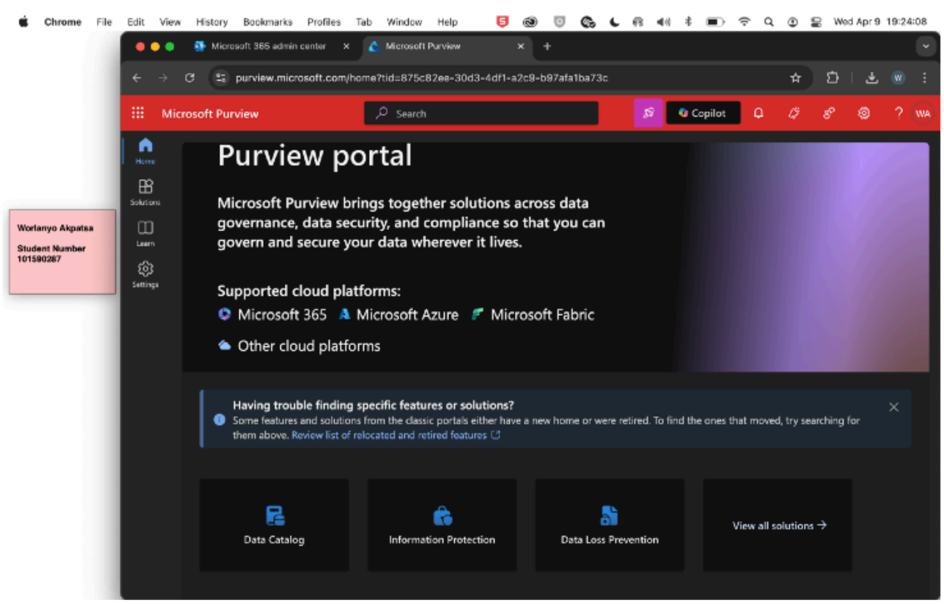
~~~~~~

B: In the left pane, scroll down to “Admin Centers” and select “Compliance”



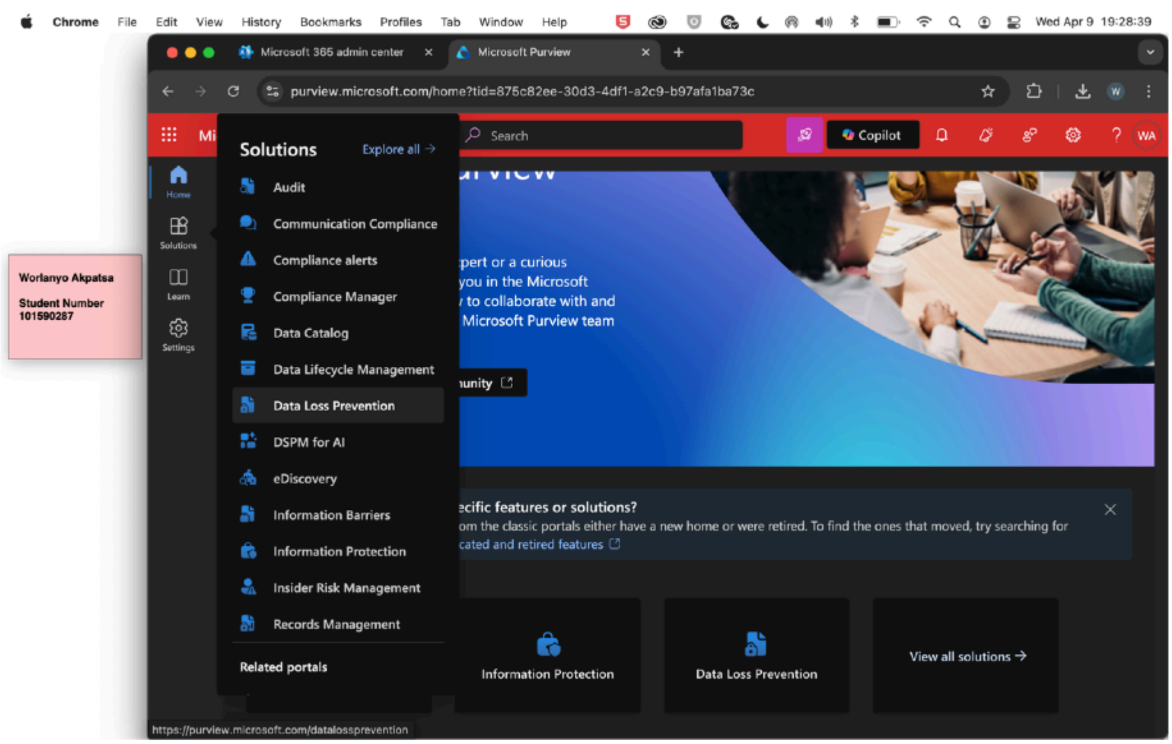
C: Microsoft Purview Compliance Portal Welcome and Homepage



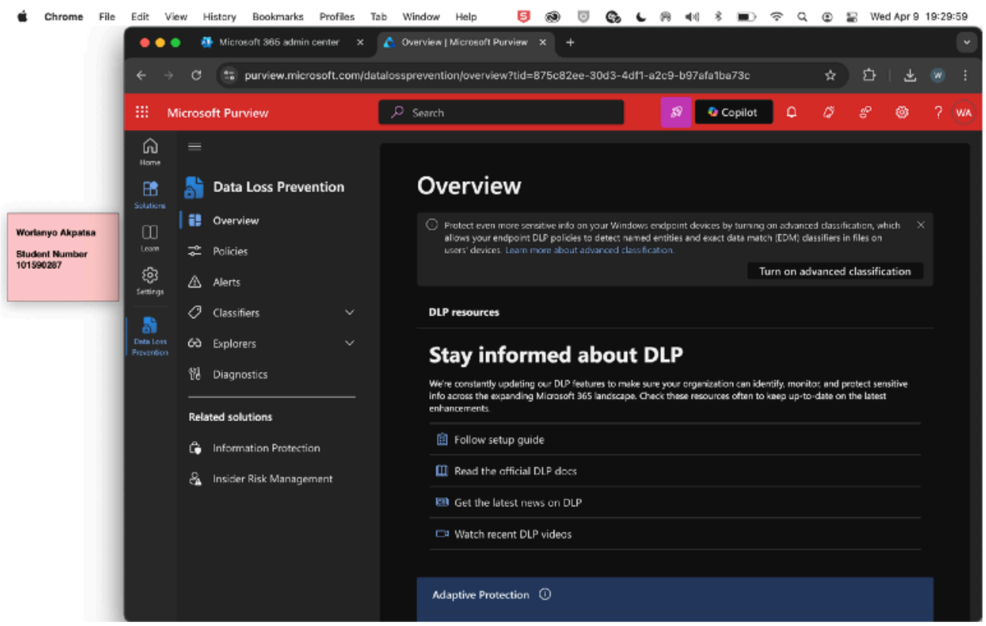


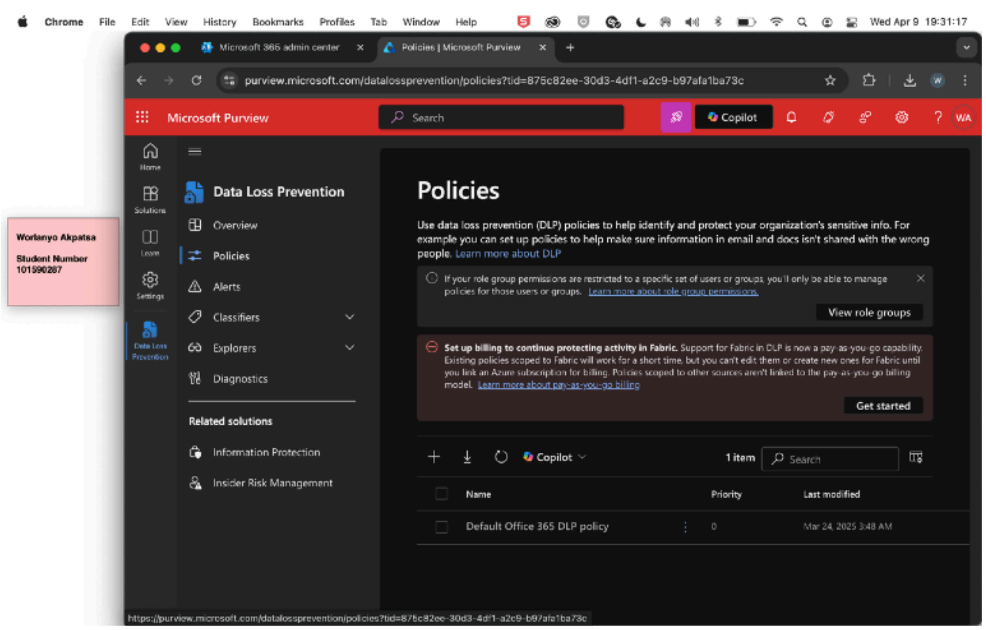
1.2: Create a new DLP policy to protect sensitive information

A: Click on "Solutions" in the left pane and select "Data Loss Prevention"



B: Click on “Policies” Subheader





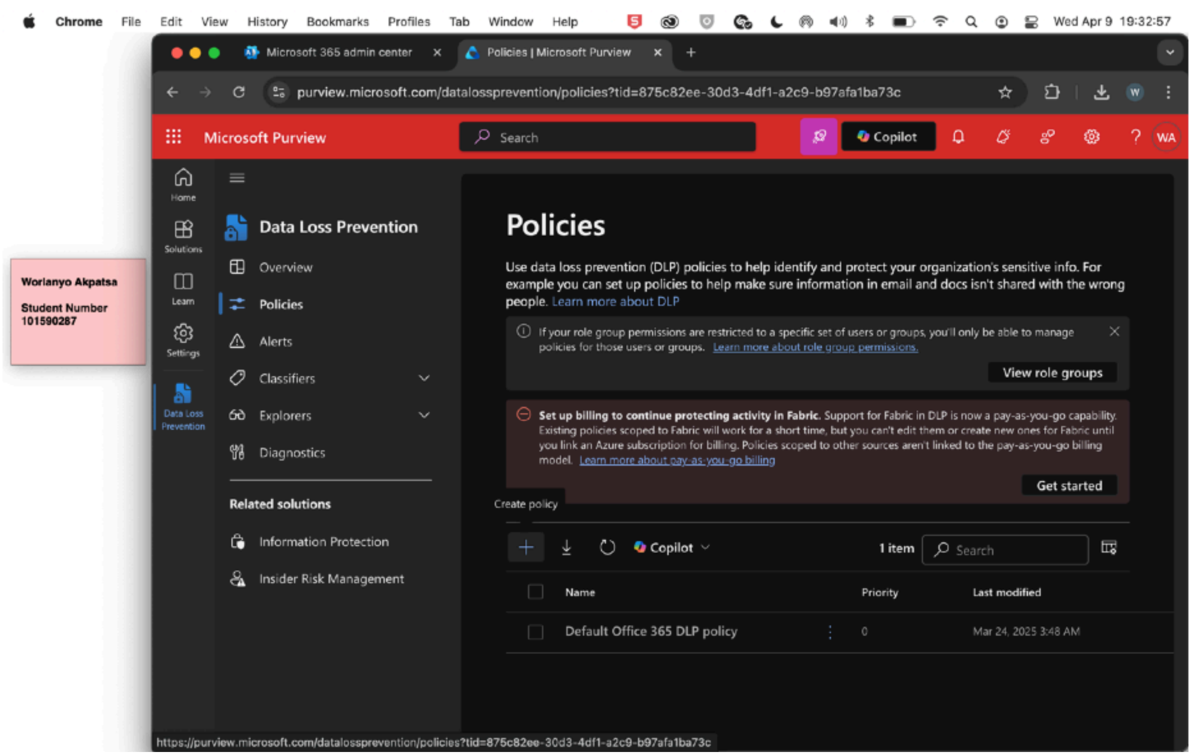
~~~~~~

~~~~

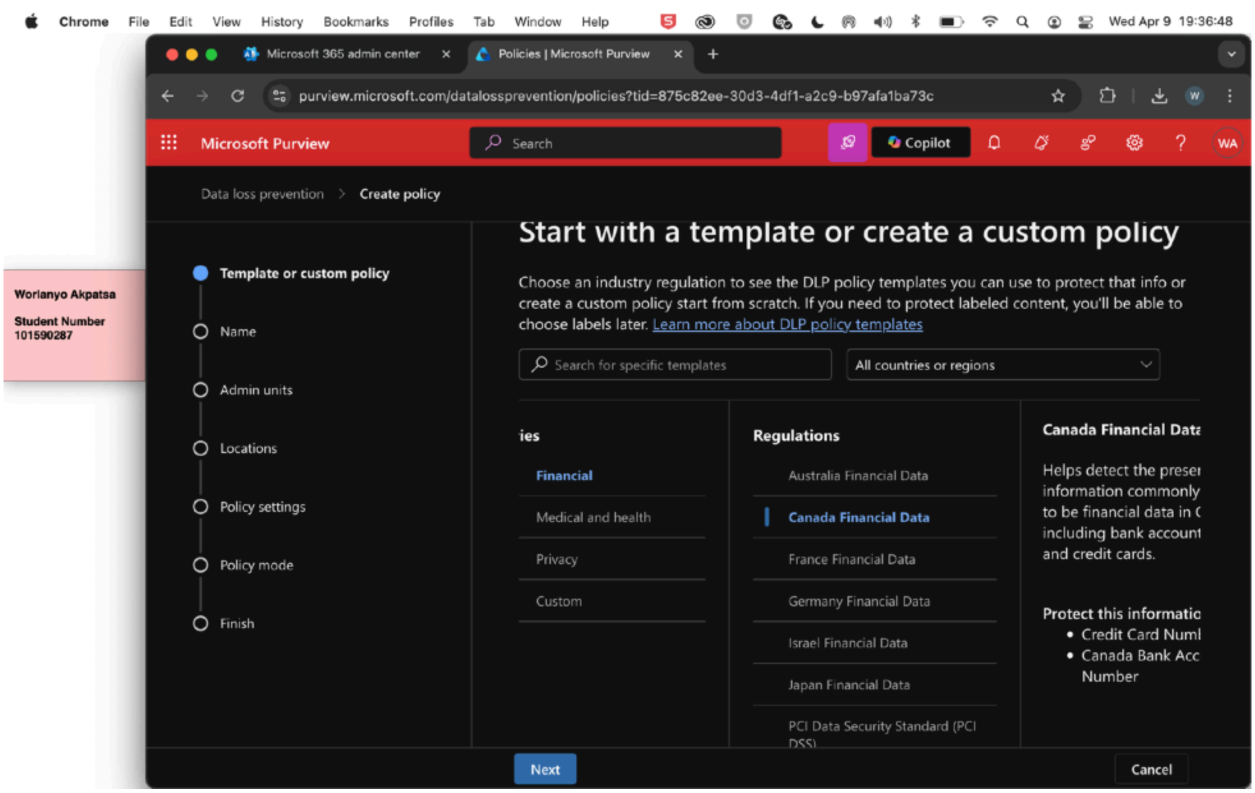
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~
~~~~

C: Click on the "+" to Create Policy

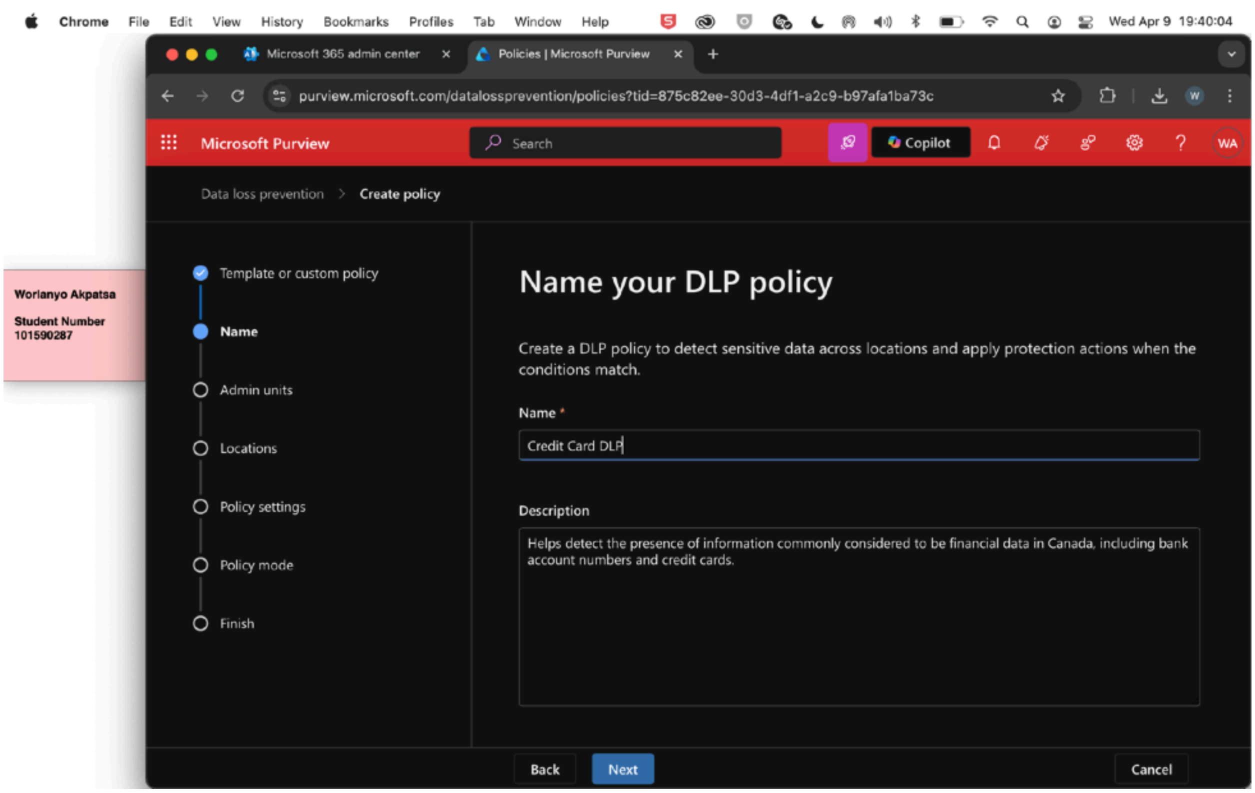


D: Policy Creation (Selecting Template = Financial)



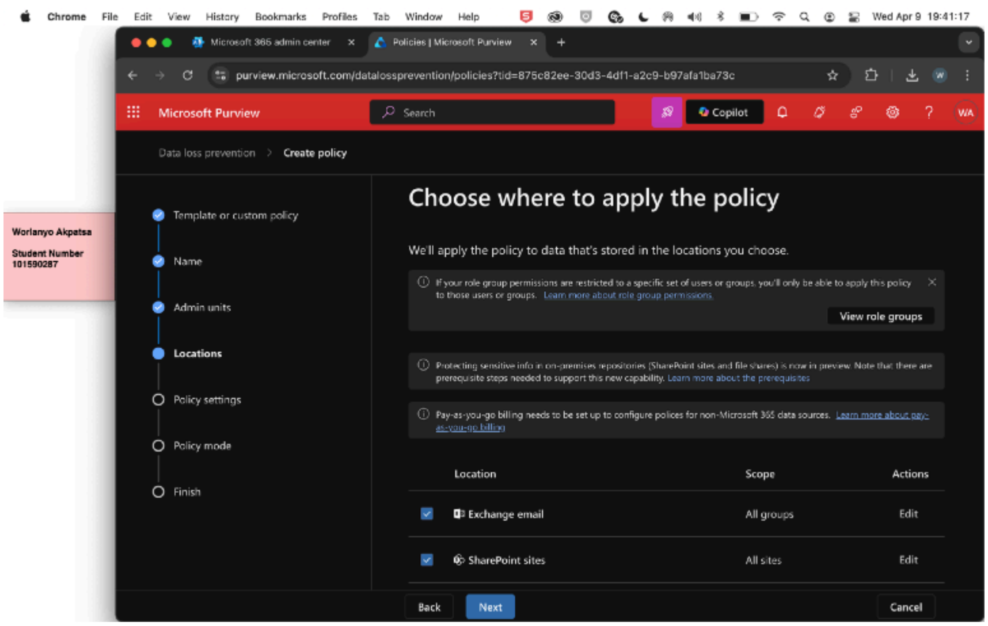
1.3: Configure the policy to notify users when sensitive information is detected

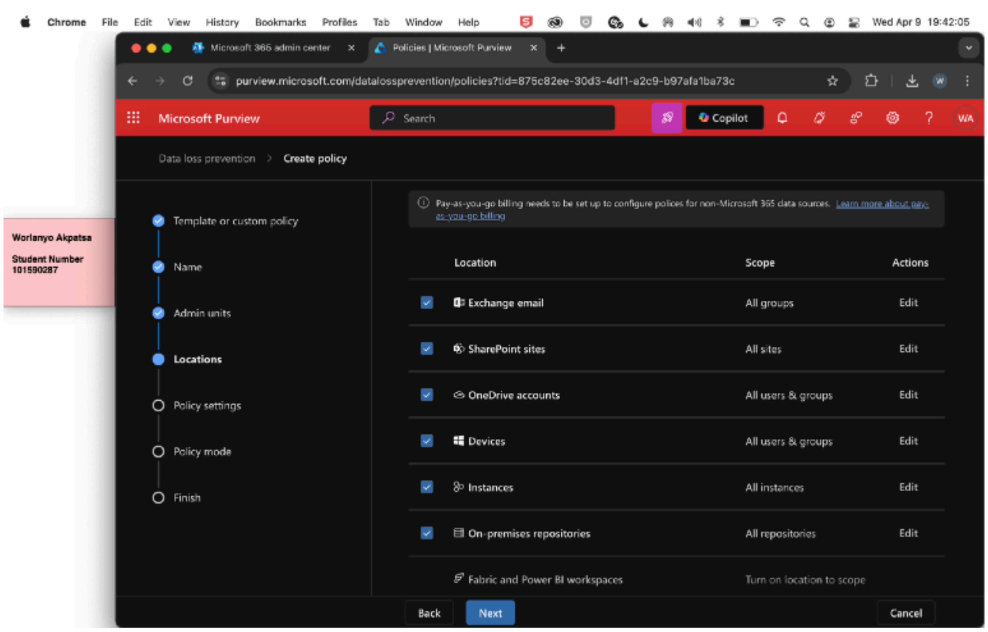
A: Policy Creation (Naming and Describing Policy)



Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

B: Policy Creation (Choosing where to apply the policy (location))



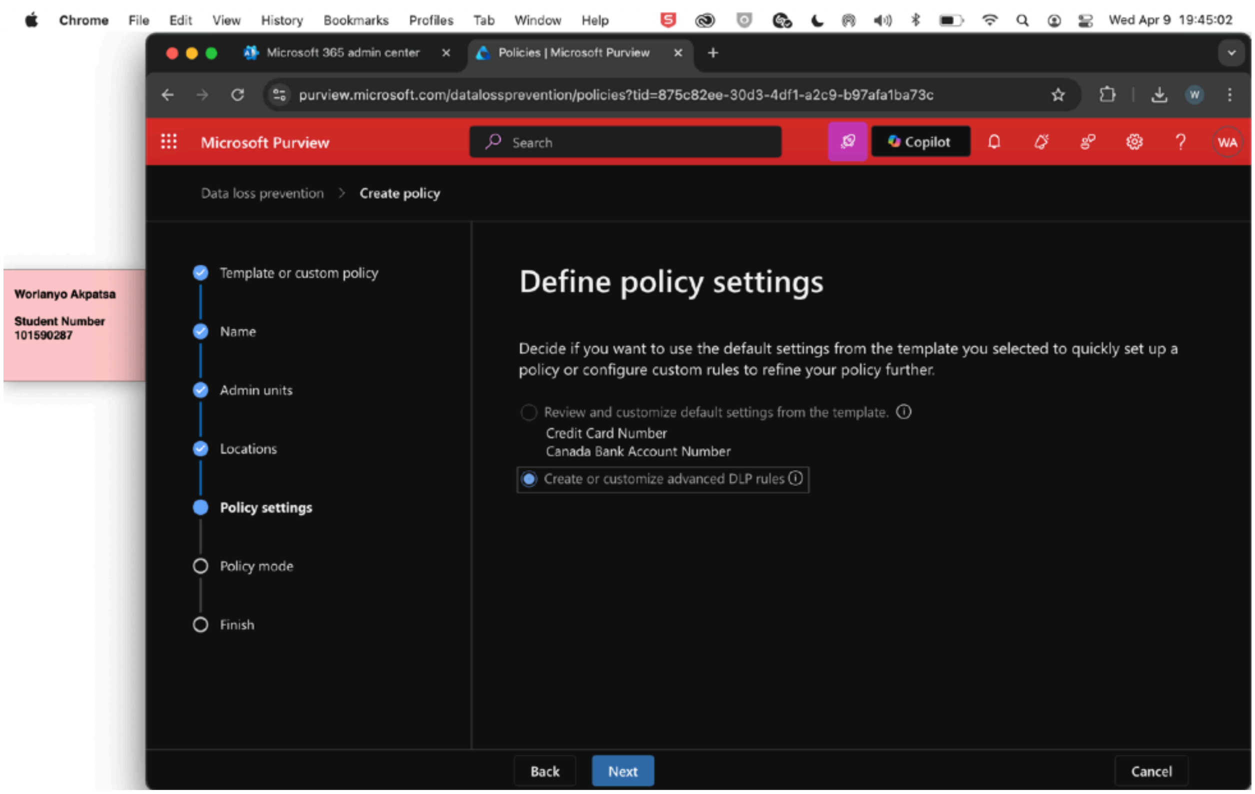


~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

C: Defining policy settings (creating/customizing advanced DLP rules)



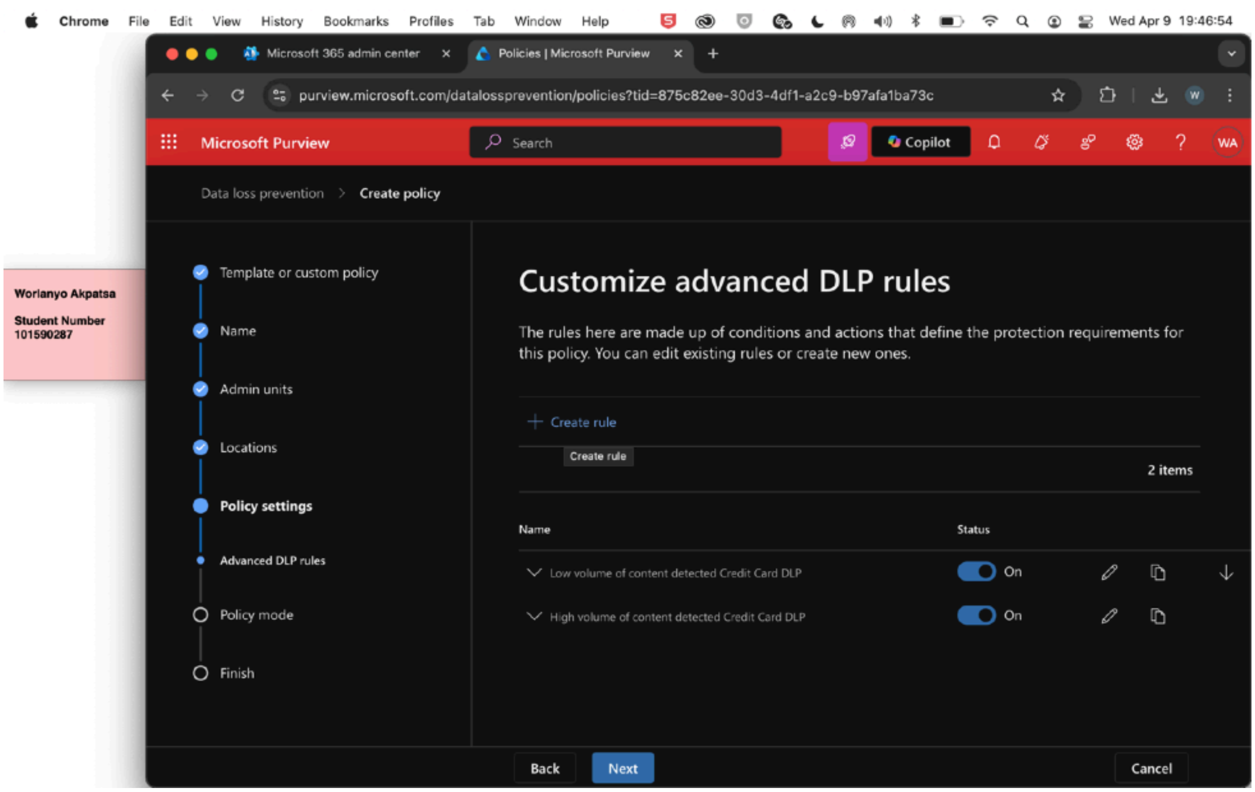
~~~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

~~~~~~

D: Creating custom DLP rules (click create rule)

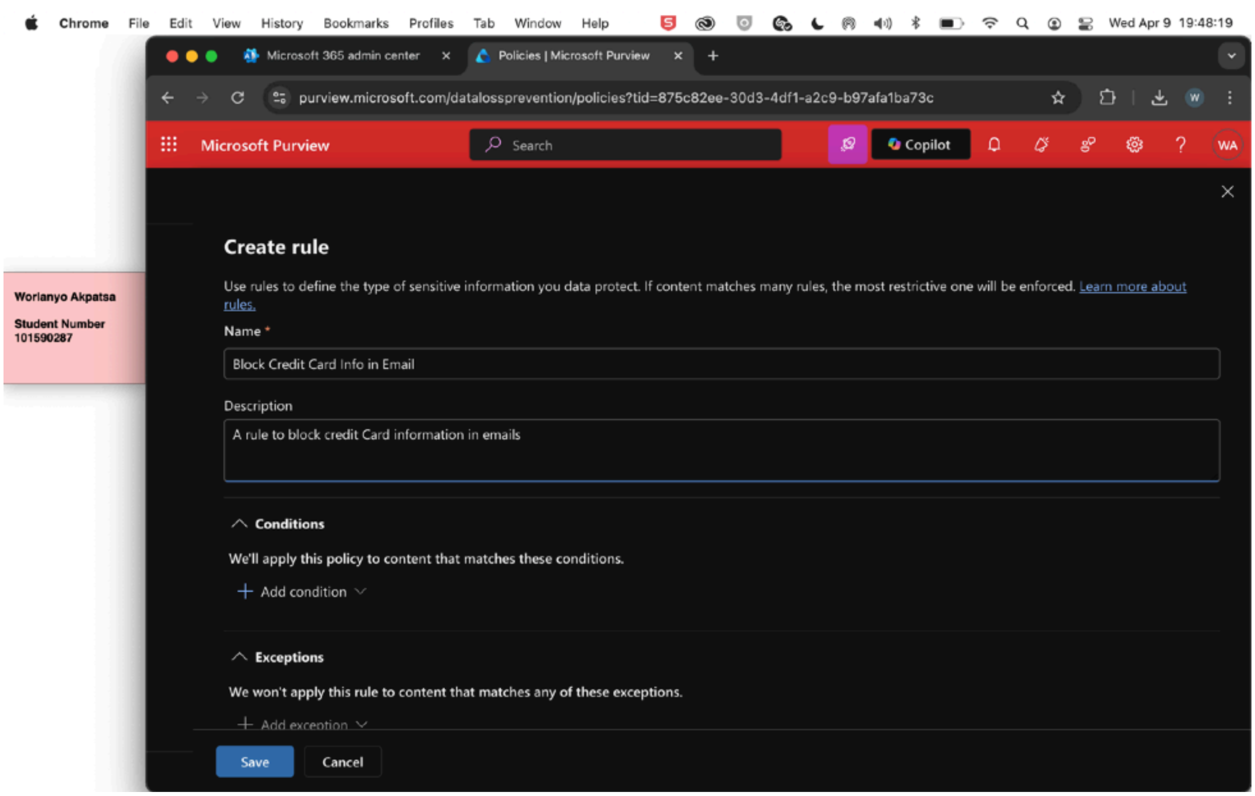


\~~~~~~

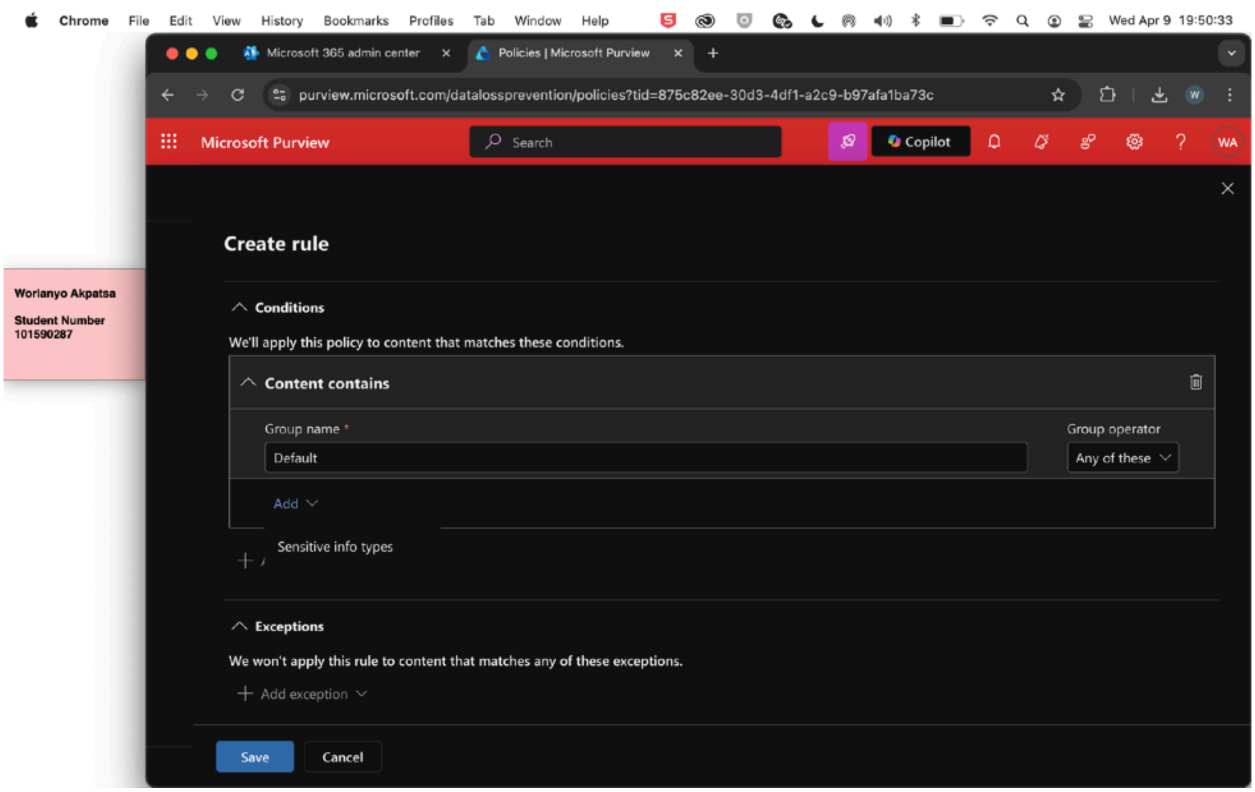
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

\~~~~~~

D: Creating Custom DLP rule (naming rule)



D: Creating Custom DLP rule (Adding Condition that policy applies to)

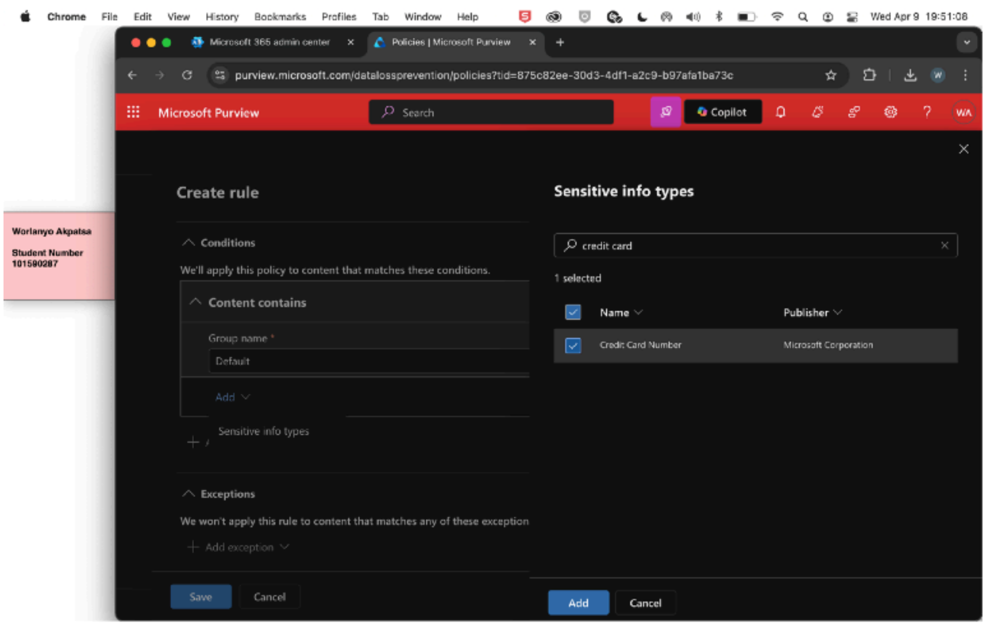


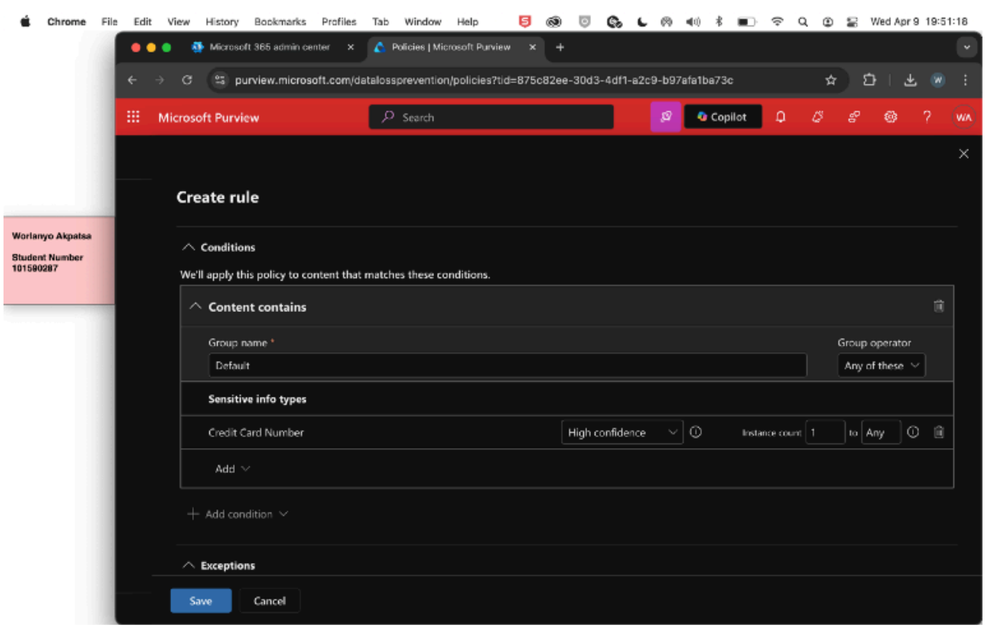
~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

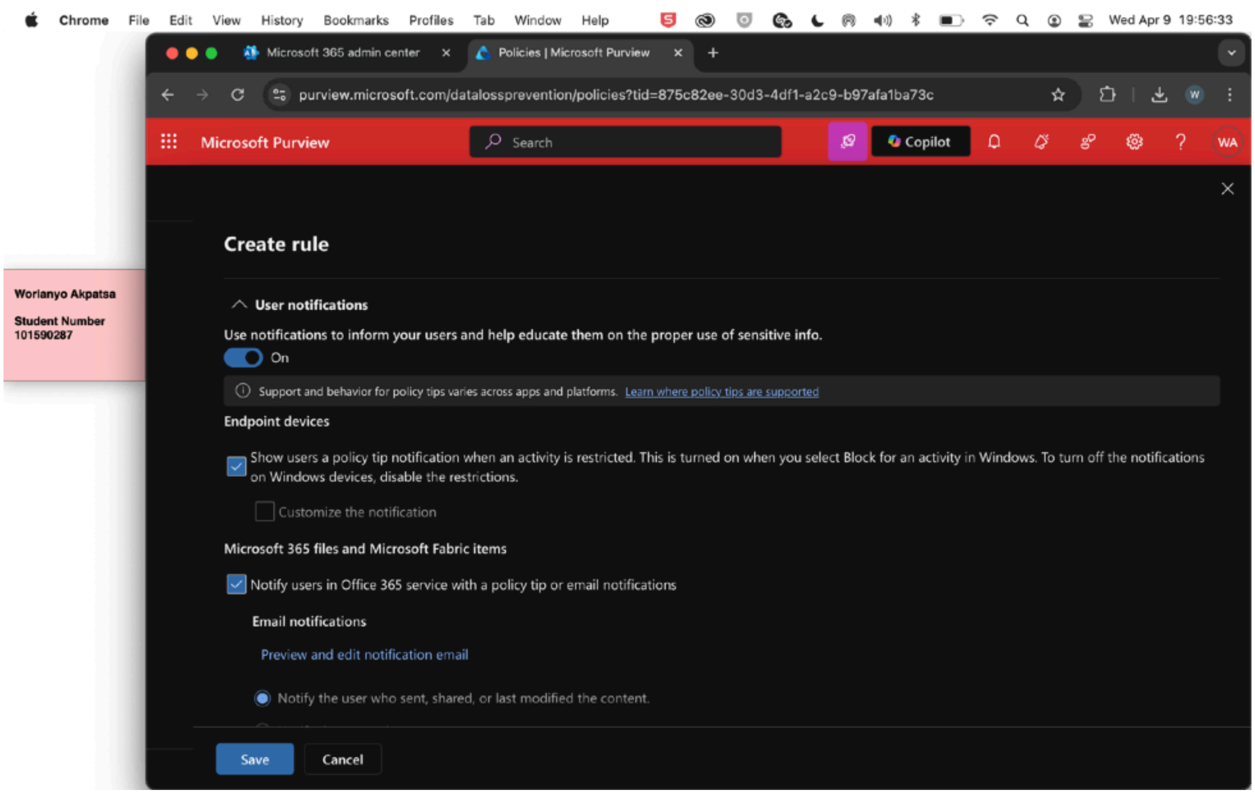
~~~~~~

D: Creating Custom DLP rule (Adding Credit card Number as a Sensitive Info Type that Policy will apply to)

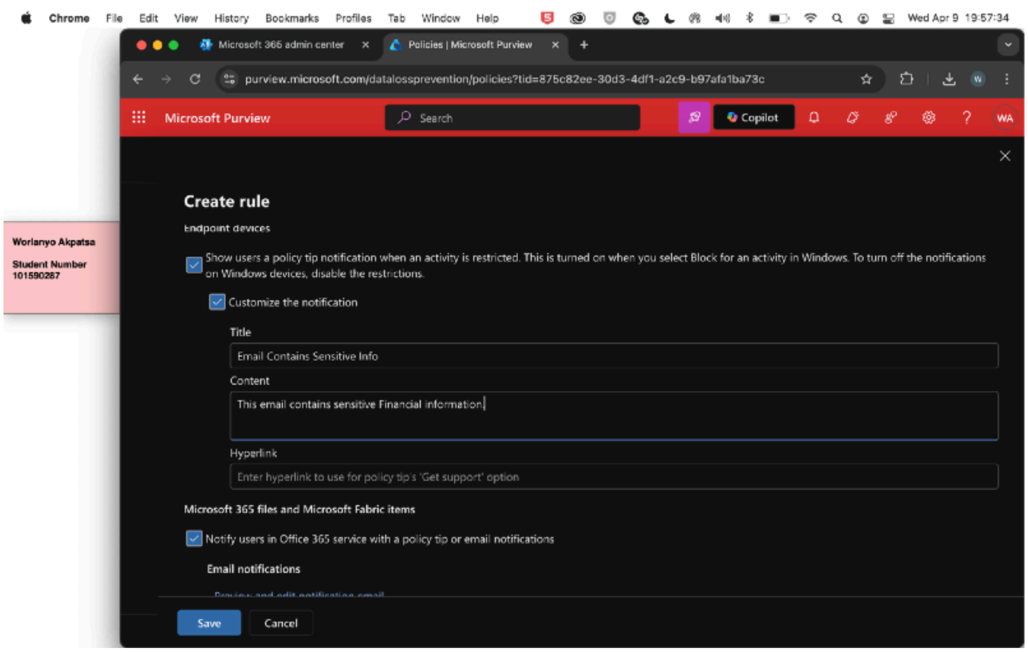


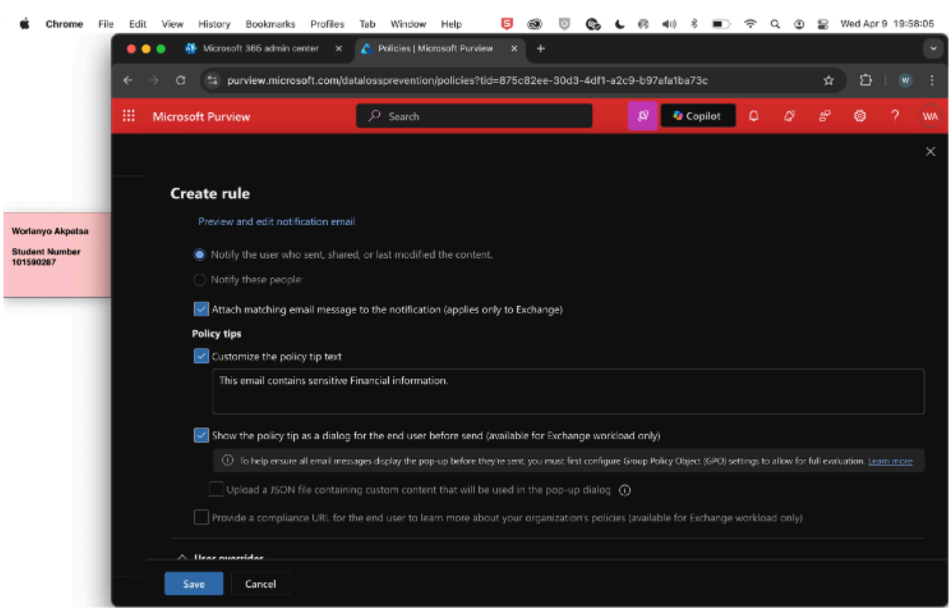


E: Enabling notifications to notify users that sensitive info is being shared



F: Customizing the notification that is sent and the policy tip



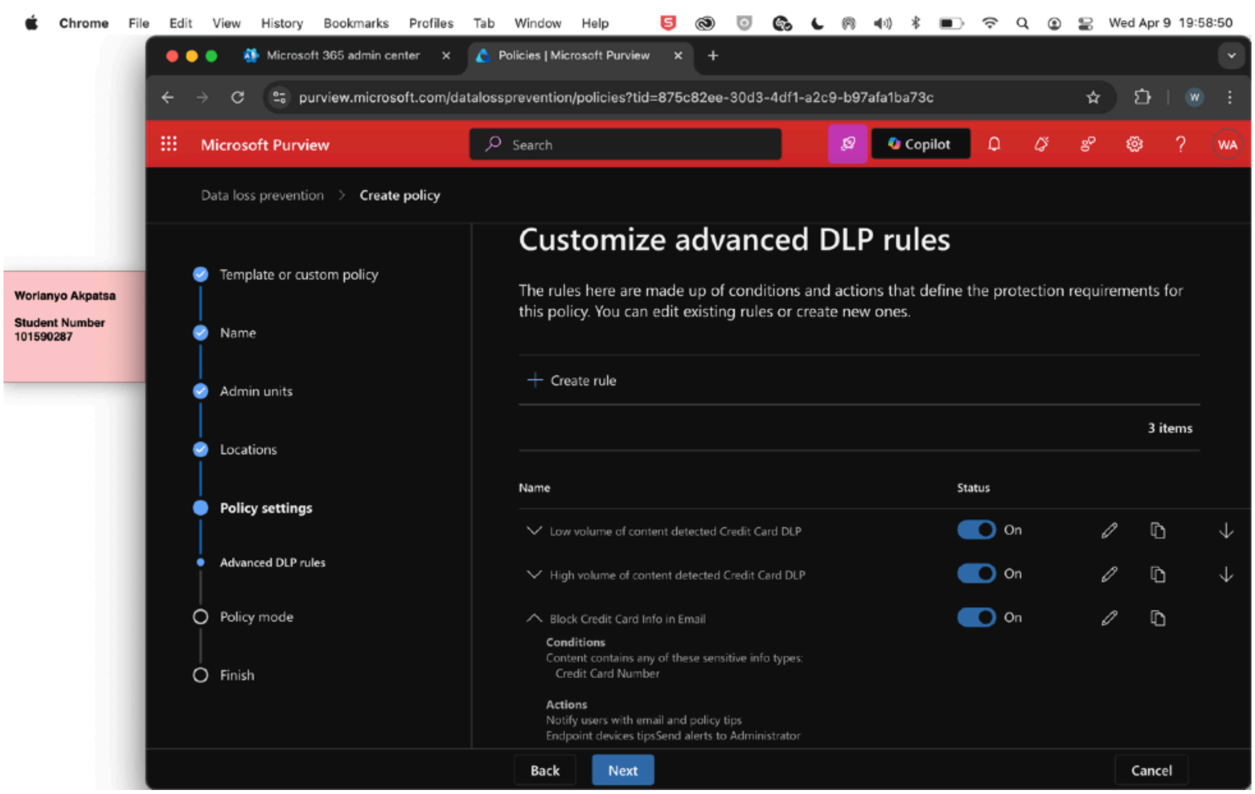


~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

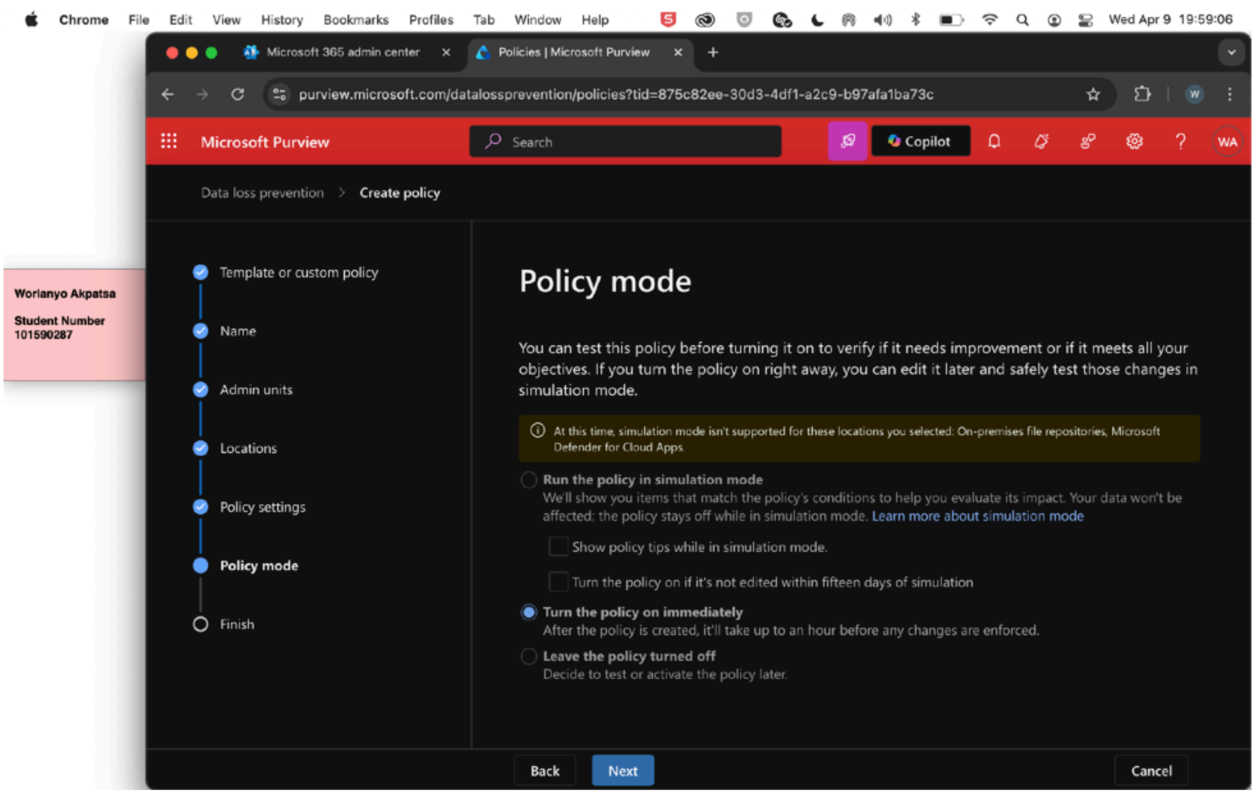
~~~~~~

G: Advanced DLP rule created

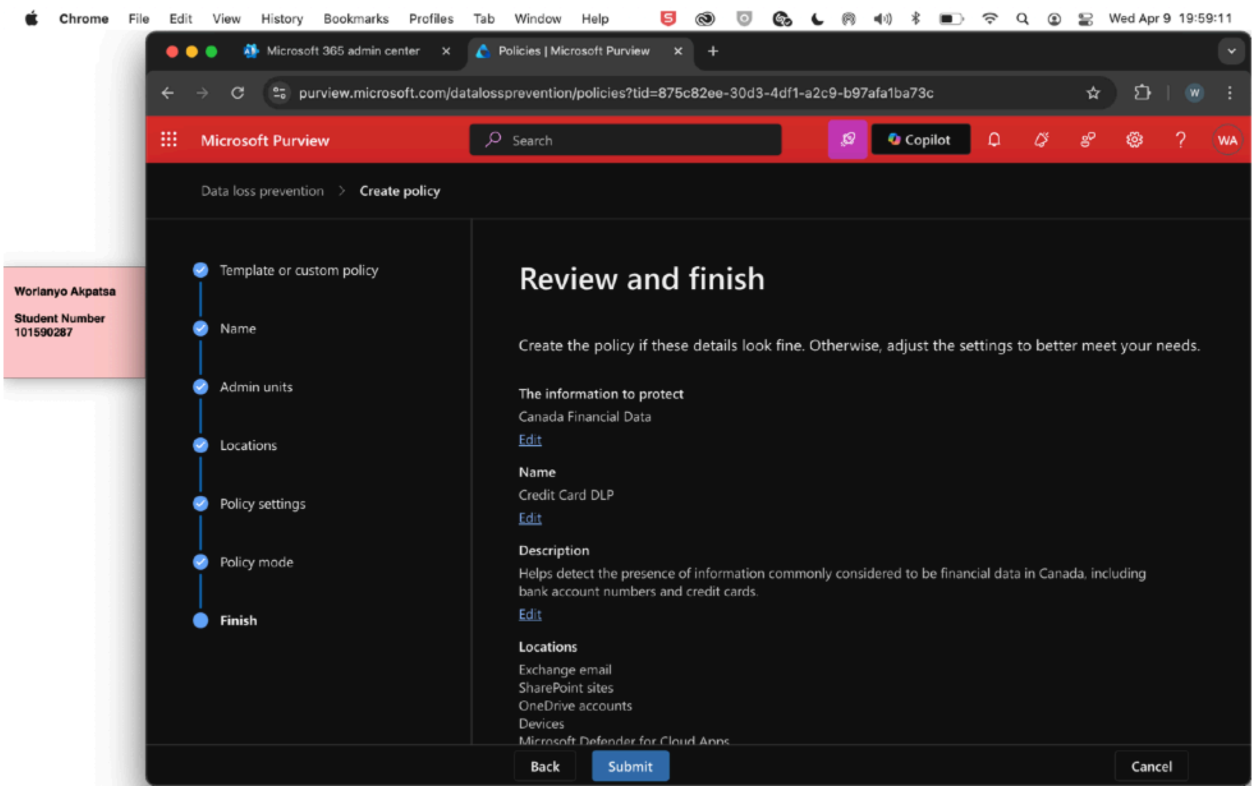


Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

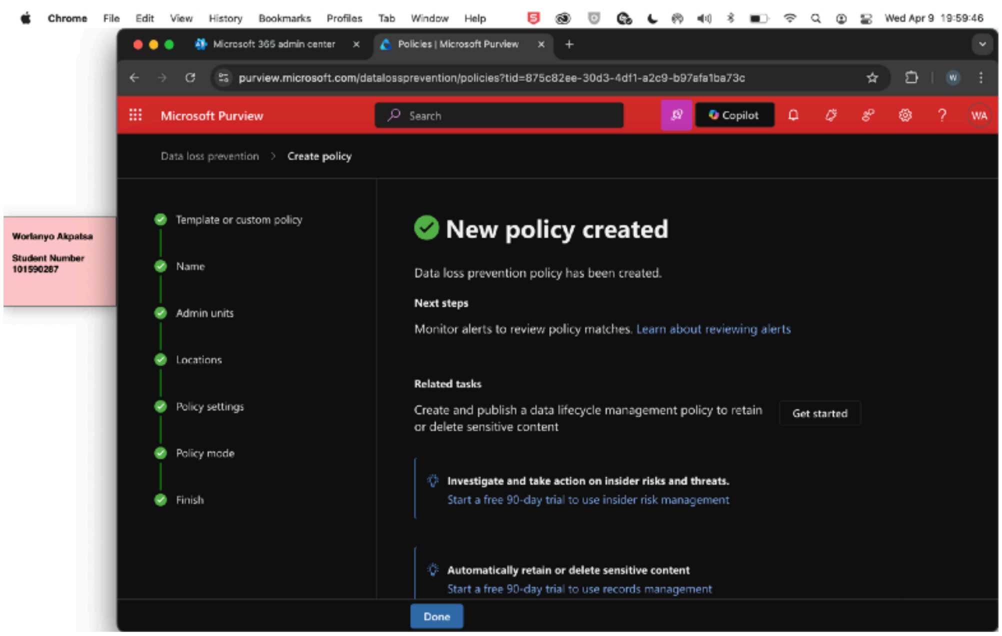
H: Turning Policy on immediately

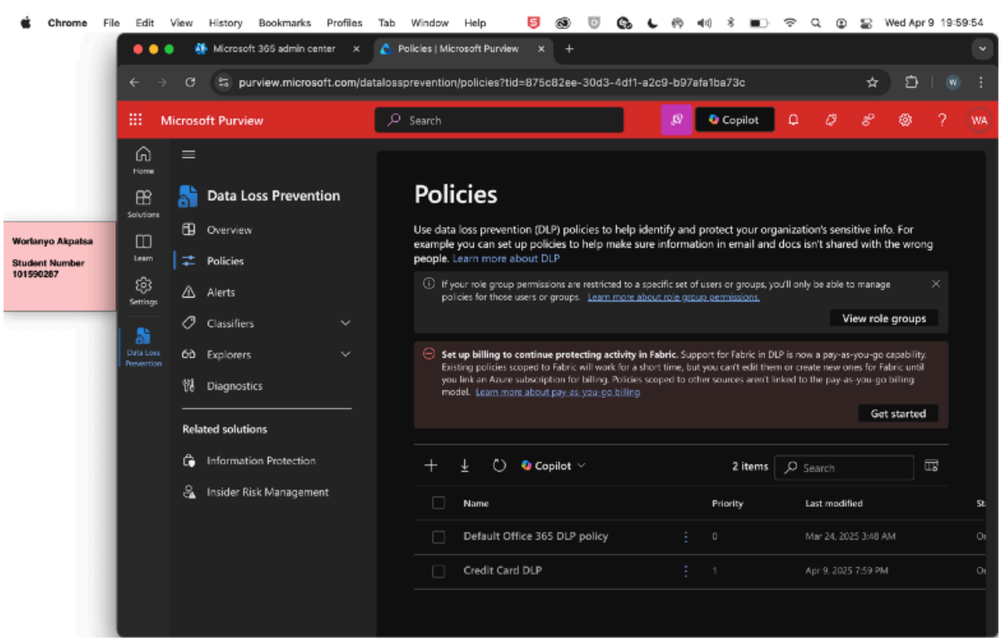


I: Review and finish



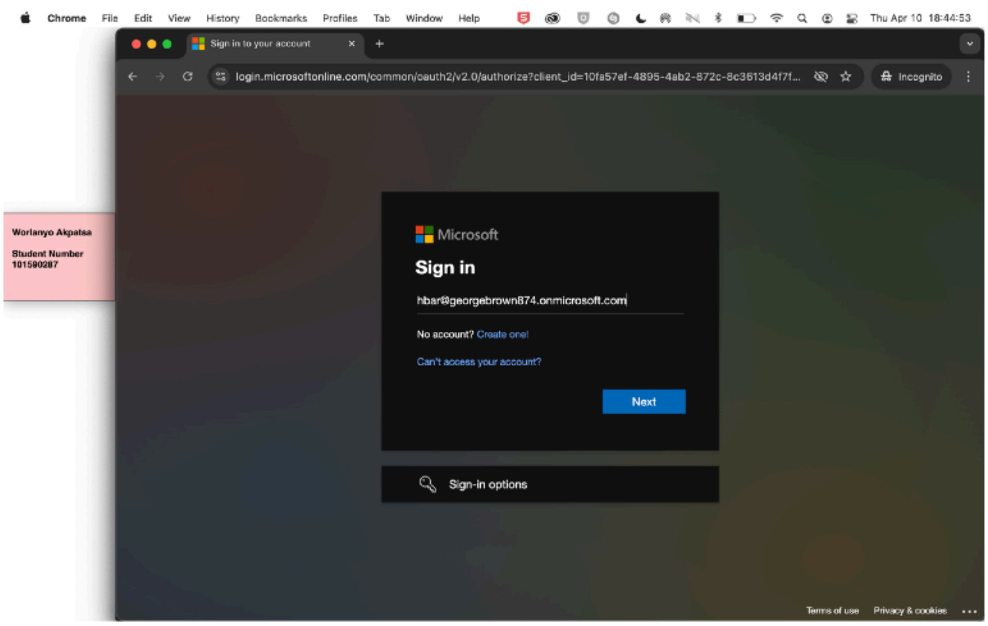
J: Policy created





1.4: Test the policy by attempting to send an email containing sensitive information

A: Signing in to 365 Outlook using a user in the company's credentials

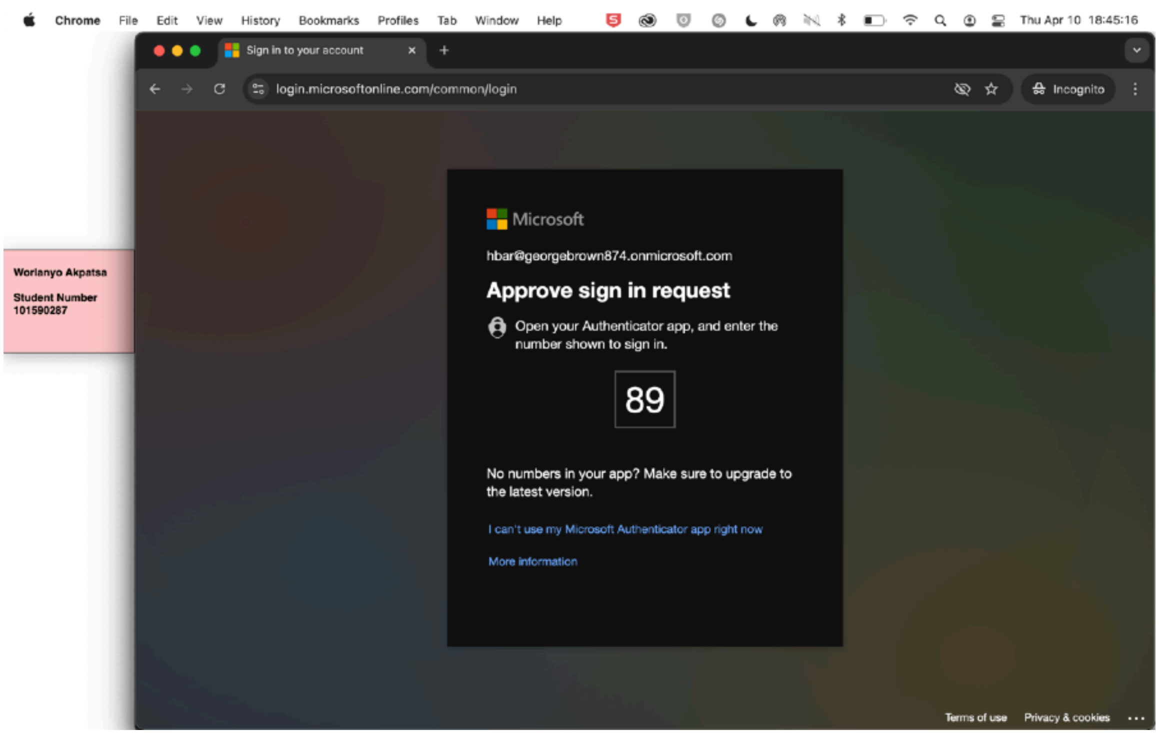


~~~~~~

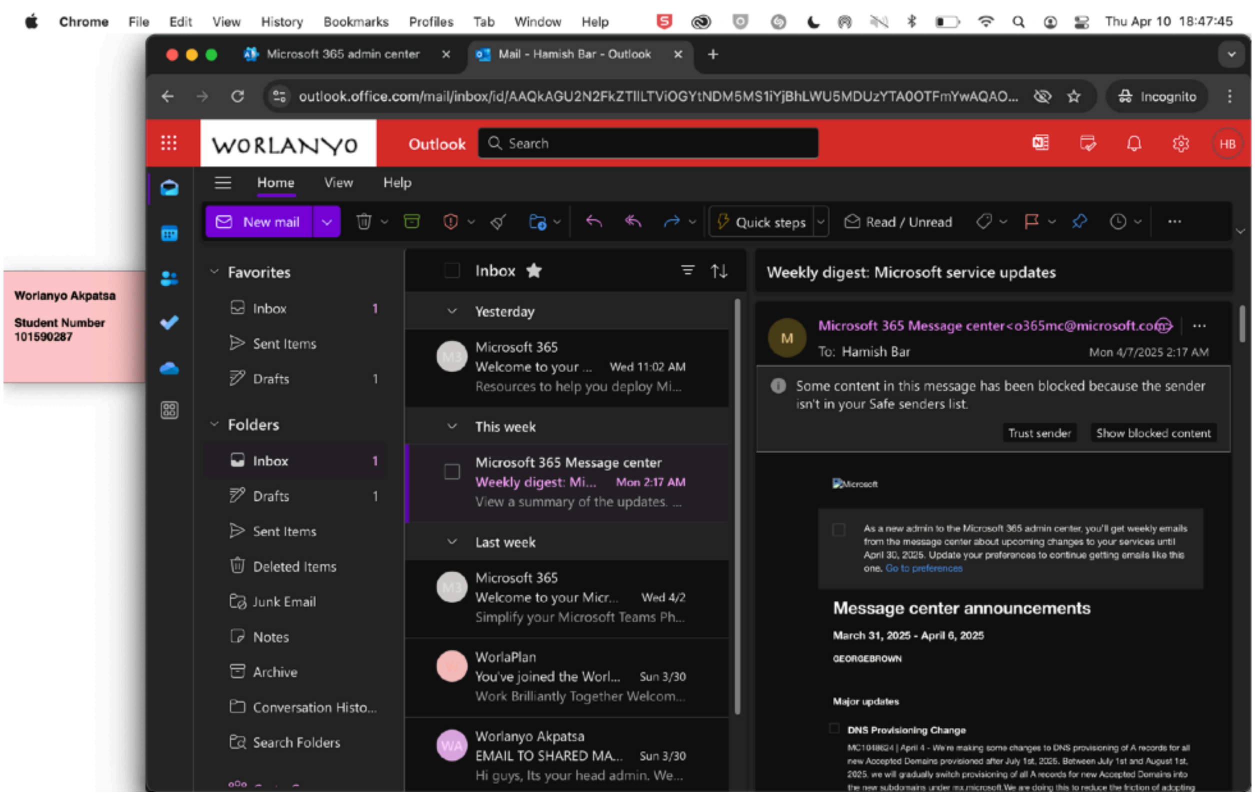
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

B: MultiFactor Authentication



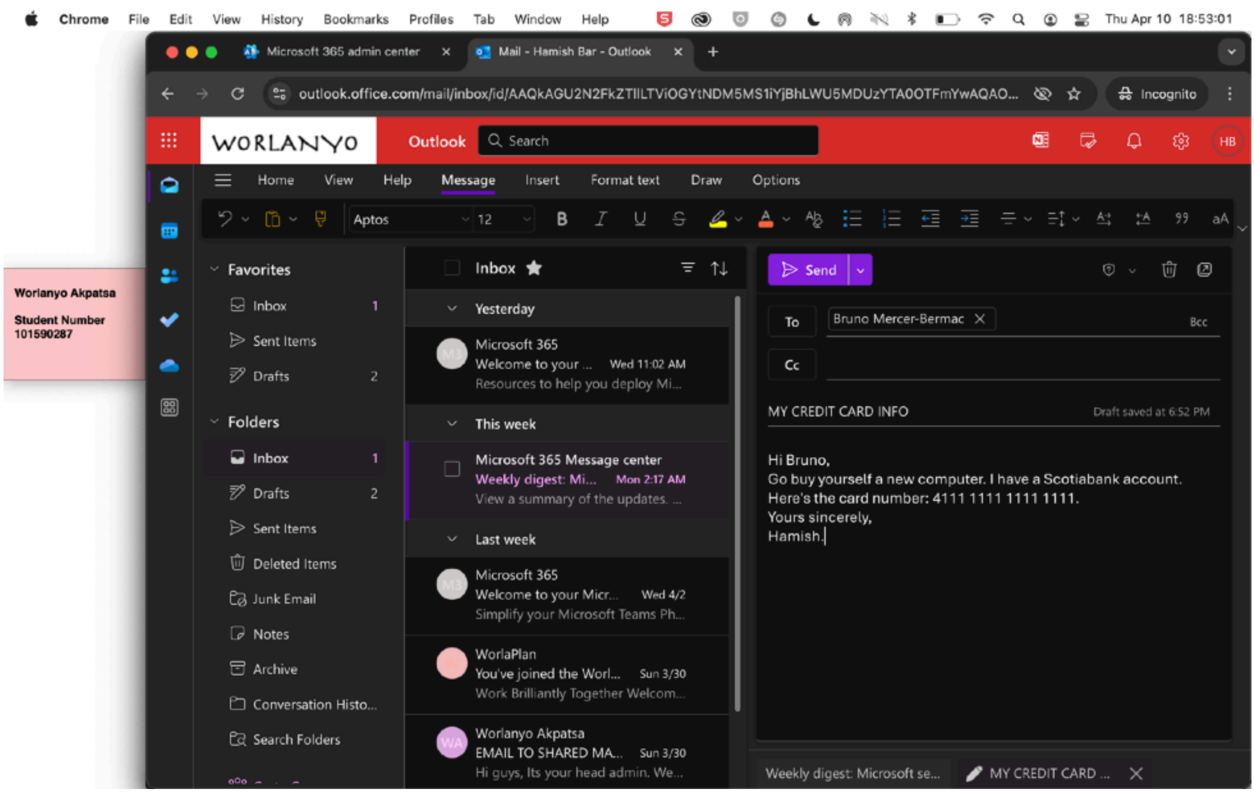
C: User's Outlook homepage



Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

D: Sending email with sensitive info

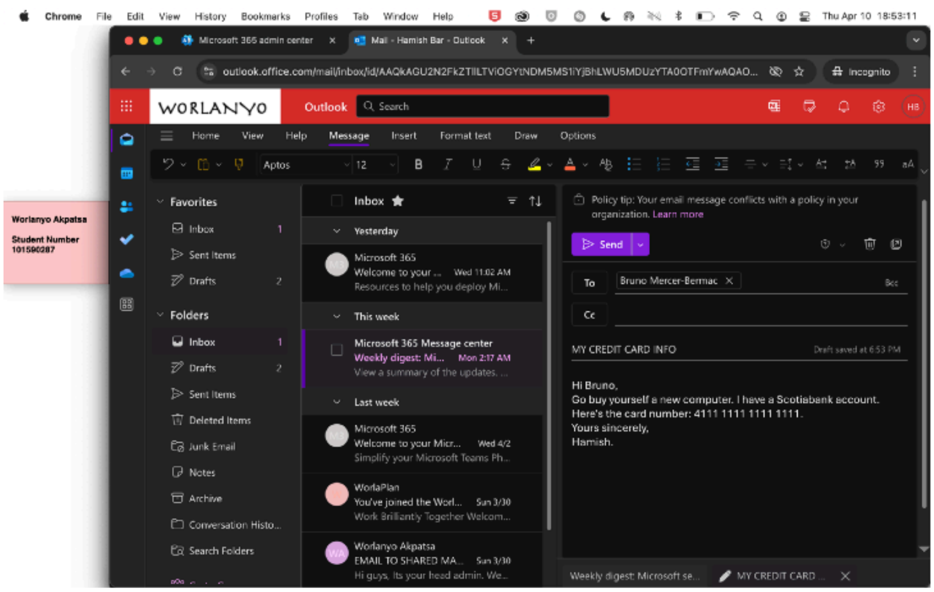


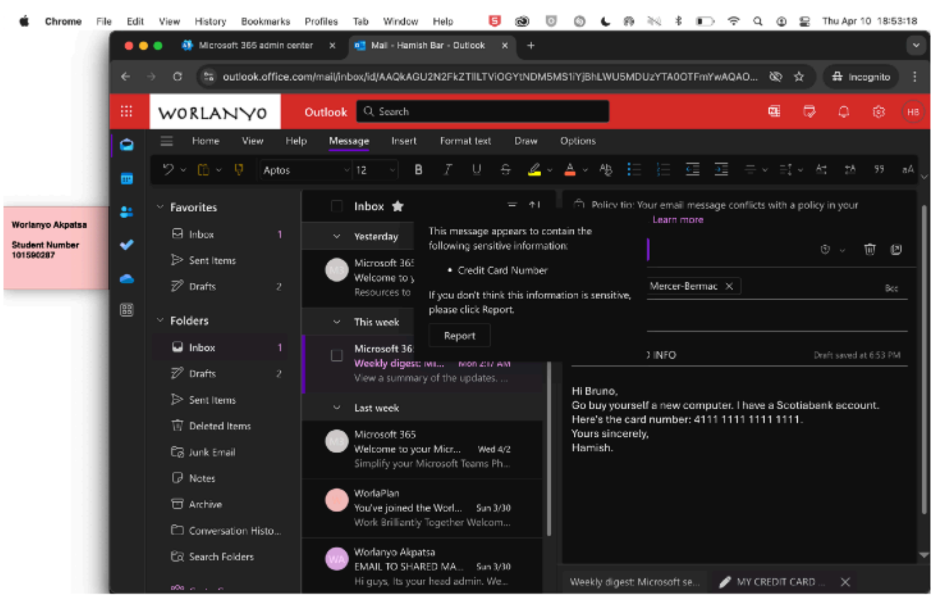
~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

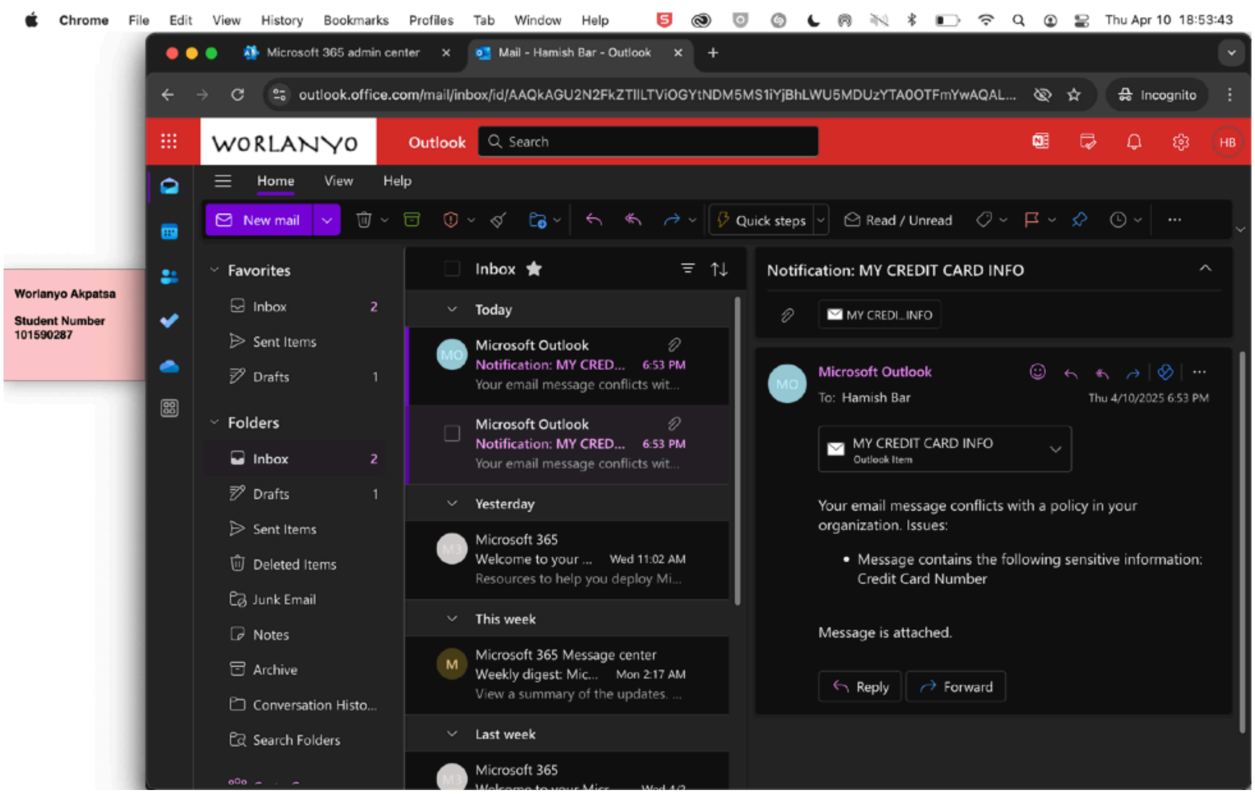
~~~~~~

E: Evidence that policy is functional (before sending email)





F: Evidence that policy is functional (After sending email)



Task 1 Summary

This whole activity introduced me to a new side of Microsoft 365 Admin Center which I never knew about; the compliance center.

The first task for this activity was to set up Data Loss Prevention (DLP) policies which I had limited knowledge about so I was glad to give it a try and end up knowing exactly what it entails.

To begin, I had to access the 365 compliance center. One thing I have learnt over the course of all the lectures is that most things can be accessed from the 365 Admin Center so I first navigated there. On the left pane in the Admin Center, i scrolled down to the Header that reads "Admin Centers" and selected Compliance. This takes you to the Microsoft Purview Compliance portal welcome page and homepage.

The next steps in this first task was to create a new DLP policy to protect sensitive information and then test that this policy works. I couldn't wait to do this because there is nothing more gratifying than seeing that your work successfully works.

To start creating my DLP policy, I clicked on solutions in the left pane and then under that, clicked Data Loss Prevention. While in the DLP page, I clicked on the Policies subheader and then in that page, I clicked the "+" to create new policy.

Once again, I give high praise to the UX/UI design Microsoft has done. It is really easy to navigate.

Now for policy creation, the first step was selecting policy templates or creating a custom policy. I chose the Financial template for Canada Financial Data which helps detect credit card numbers and other financial information. I chose to do this because to prove that my policy is working, I wanted to send an email with credit card info.

Next step for policy creation is choosing the name and describing what your policy is for. I chose the name "Credit Card DLP".

After this, I had to choose the location where the policy applied to. Luckily for me, everything was already checked (exchange email, sharepoint sites, etc) so I just moved on to the next.

The next step was to create/customize advanced DLP rules. I decided to create a new rule which I found completely fascinating. Just like creating the policy, the first step in creating the DLP rules was to name and describe it. I named it "Block Credit Card Info in email".

While creating a DLP rule, you can add conditions that the policy will apply to. Here, I was allowed to choose credit card number as a sensitive info type which will be detected by the Policy. Next(still in custom DLP rules creation), I enabled notifications to notify users that their sensitive info is being shared. After this, I created my custom DLP rules.

After the rule is created, you are taken back to your policy creation setup. All that is left to be done is turn on the policy immediately and then review and finish.

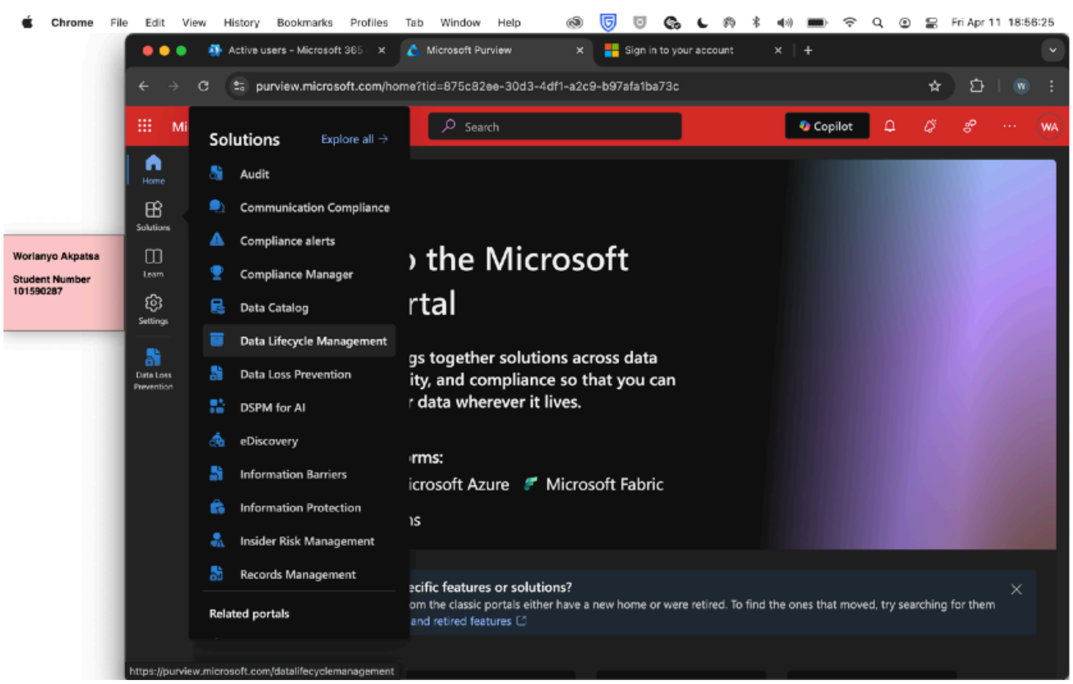
Now it is time to test if my policy works. I logged in to outlook as another user in my company and tried sending an email containing credit card information. Immediately, I got several warnings while still typing the email. After sending email too, I got an email which informed me that the email contains sensitive information.

I am glad that my process of creating a DLP policy works successfully.

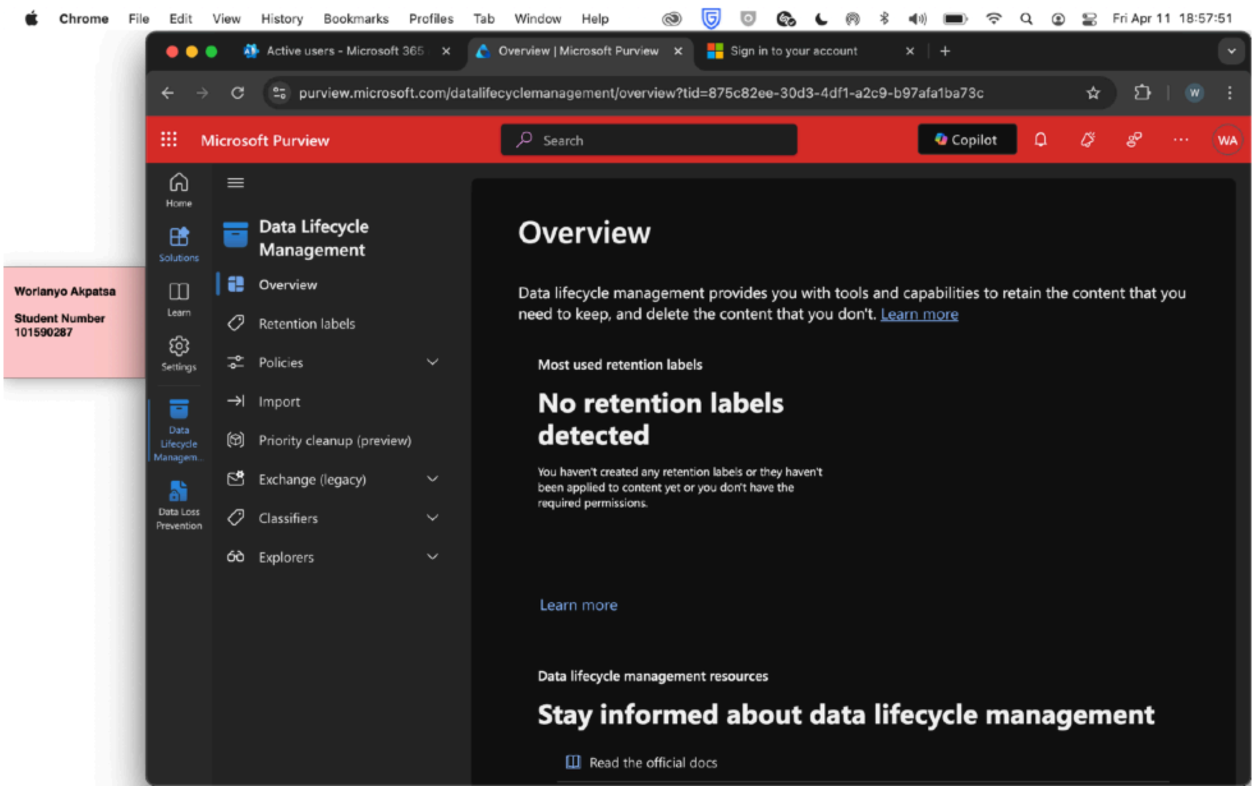
TASK 2: IMPLEMENT RETENTION POLICIES

2.1: Navigate to the Data Lifecycle Management section in the compliance center

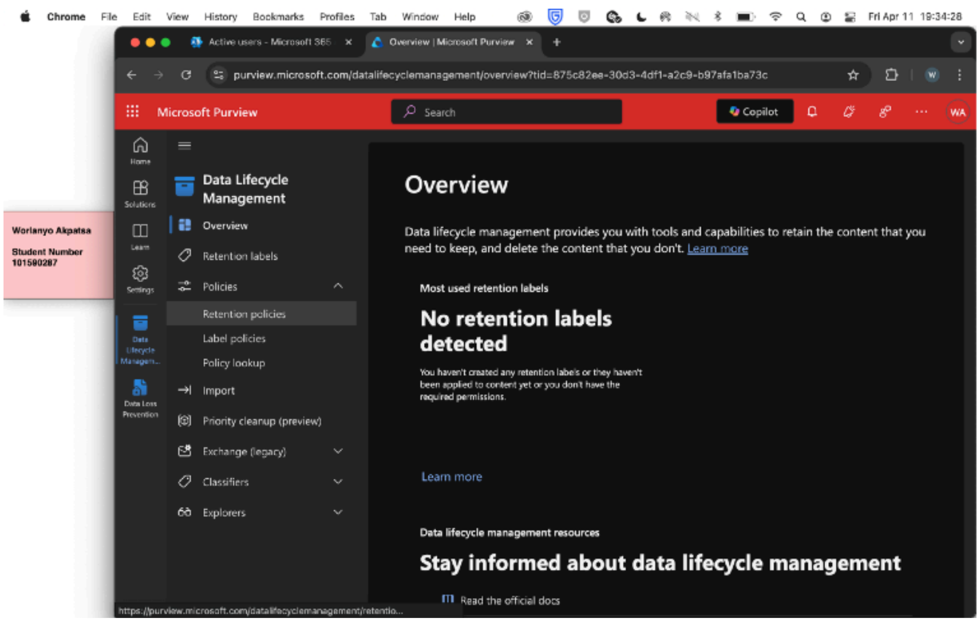
A: Navigate to solutions on the left pane and click Data Lifecycle Management

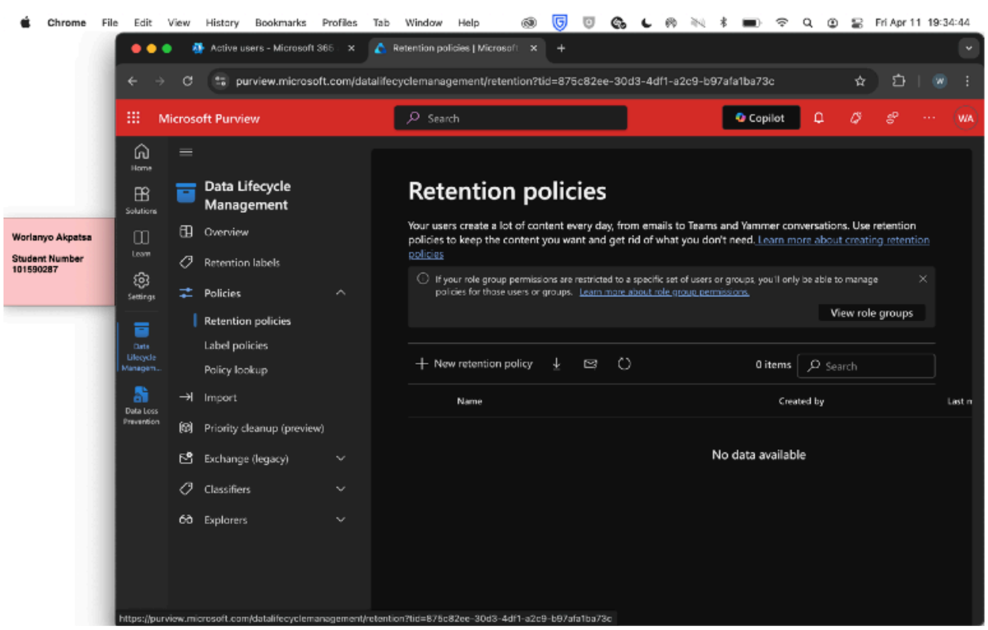


B: Data Lifecycle Management Overview Page



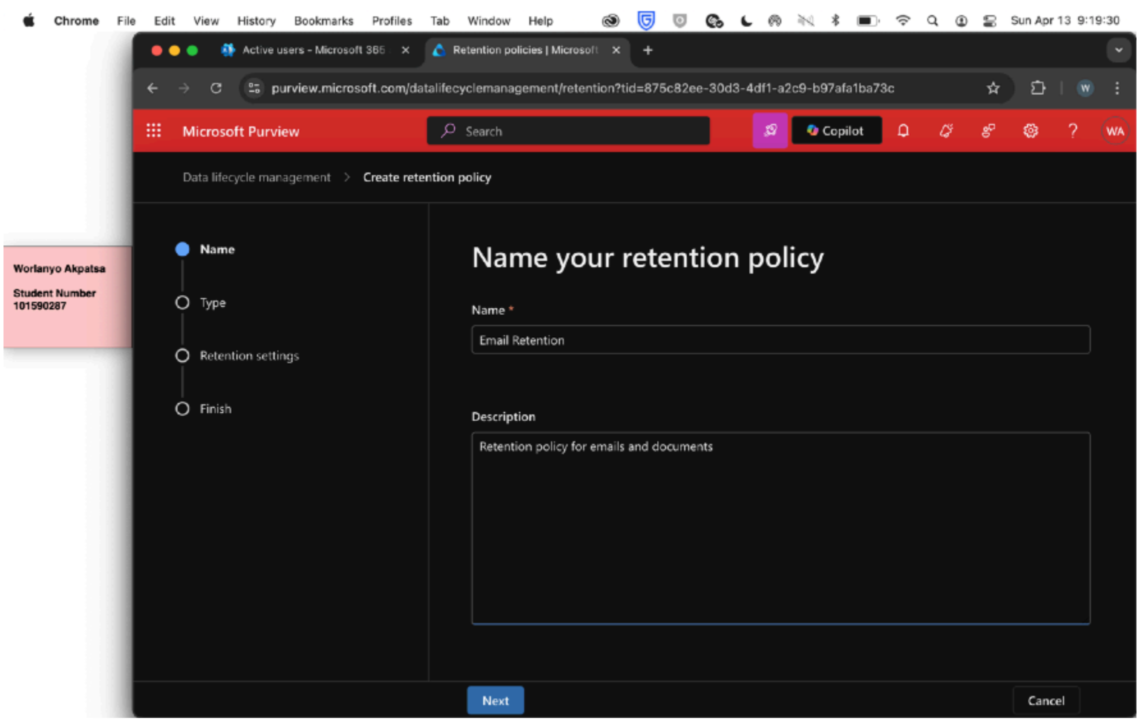
C: Click the policies subheader and select Retention Policies



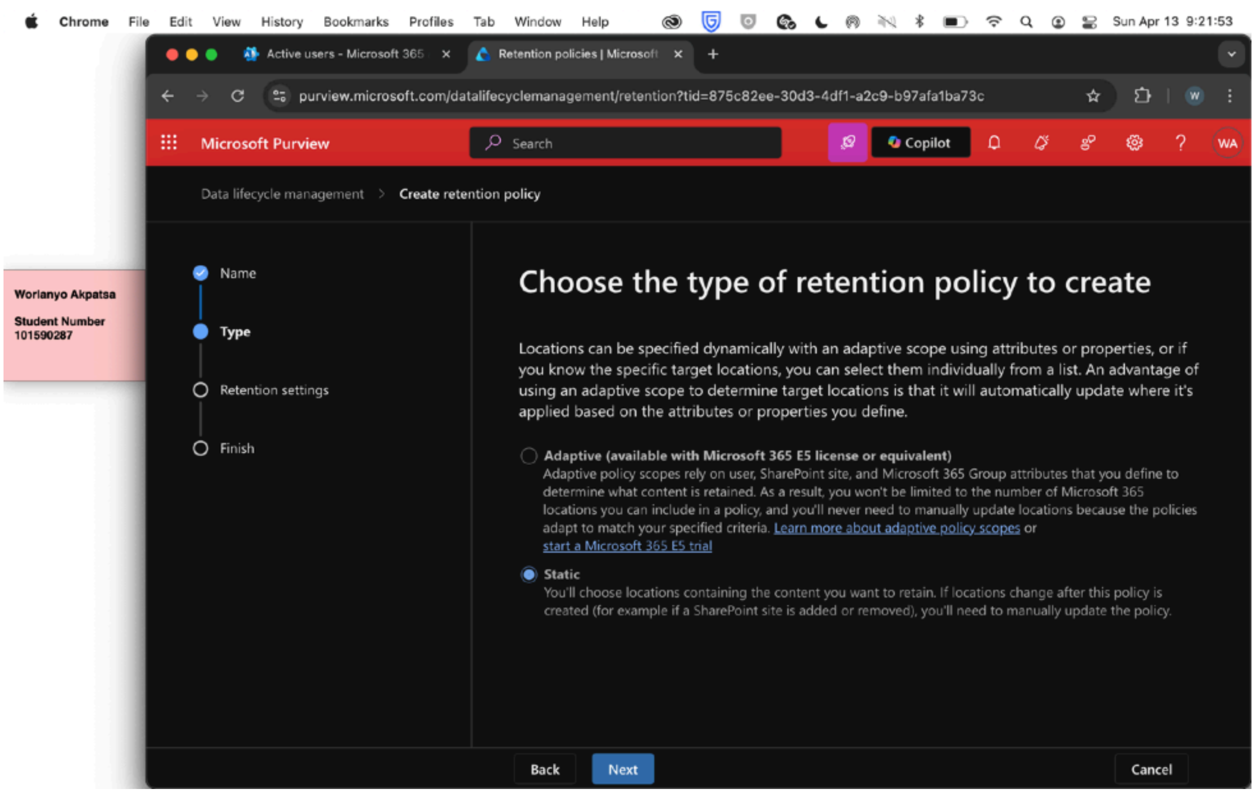


2.2: Create a new retention policy for emails and documents

A: Click on "+ new retention policy" to begin process for creating a policy and then name and describe it.



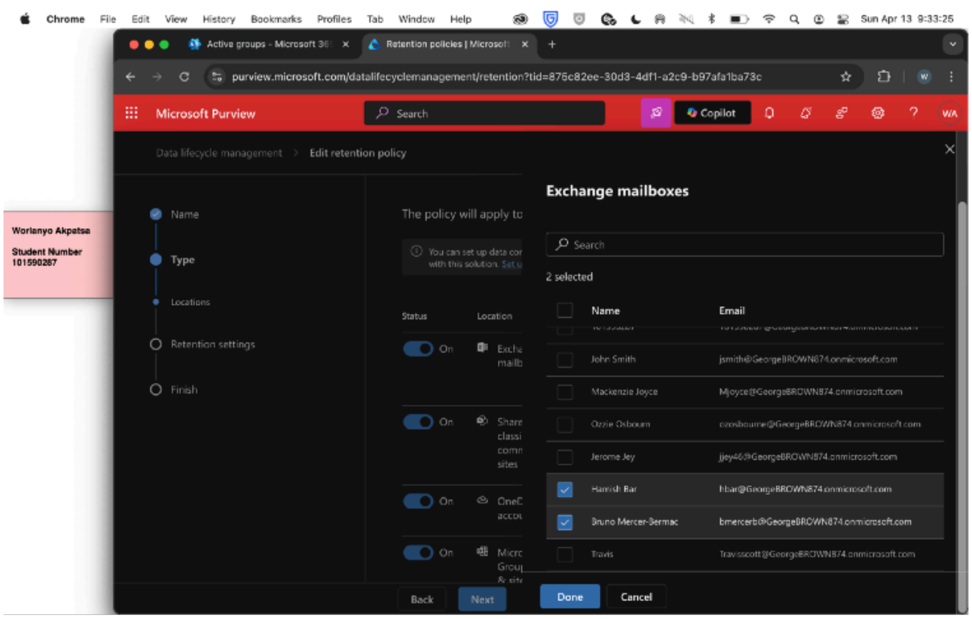
B: Choosing type of retention policy (static)

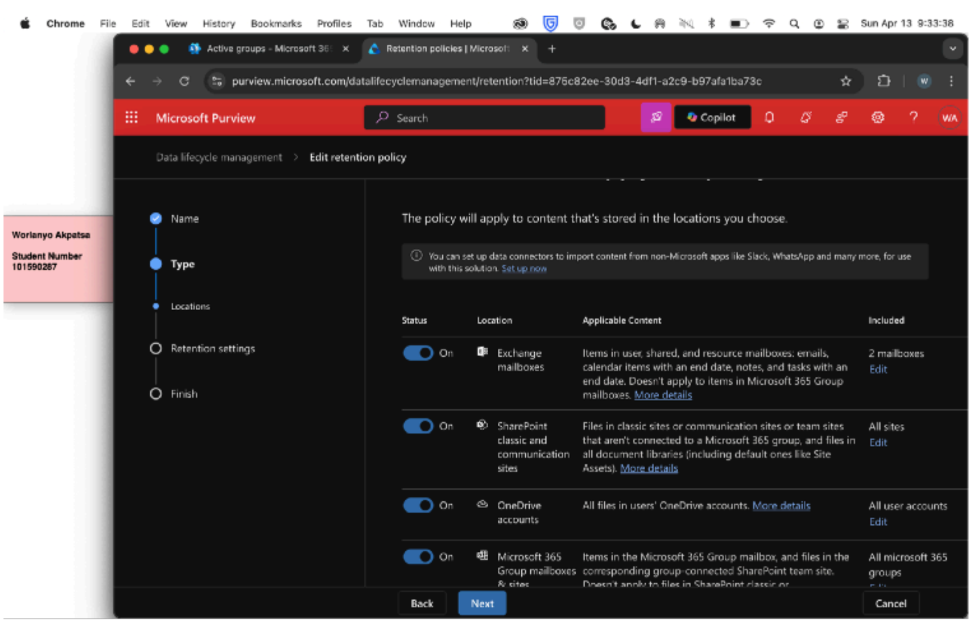


Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

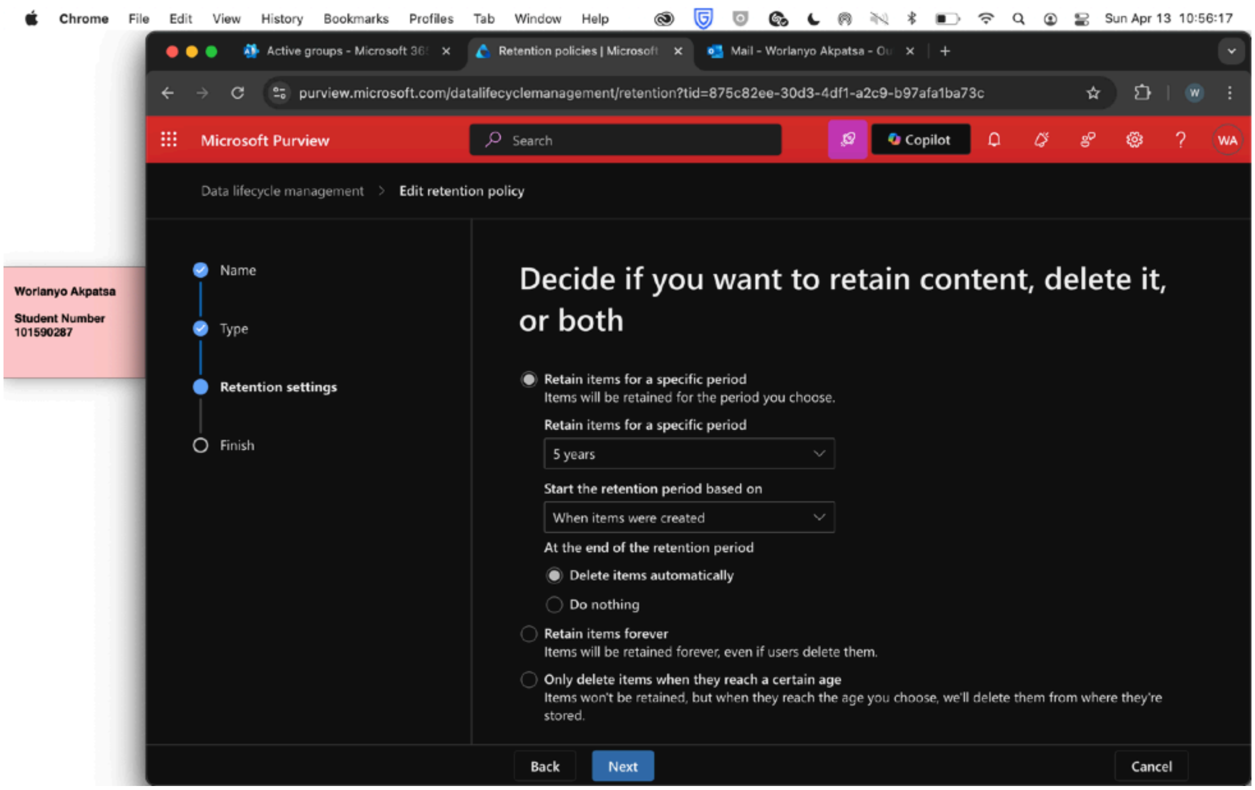
2.3: Apply the policy to a specific group of users

C: Choosing locations for where retention policy would apply





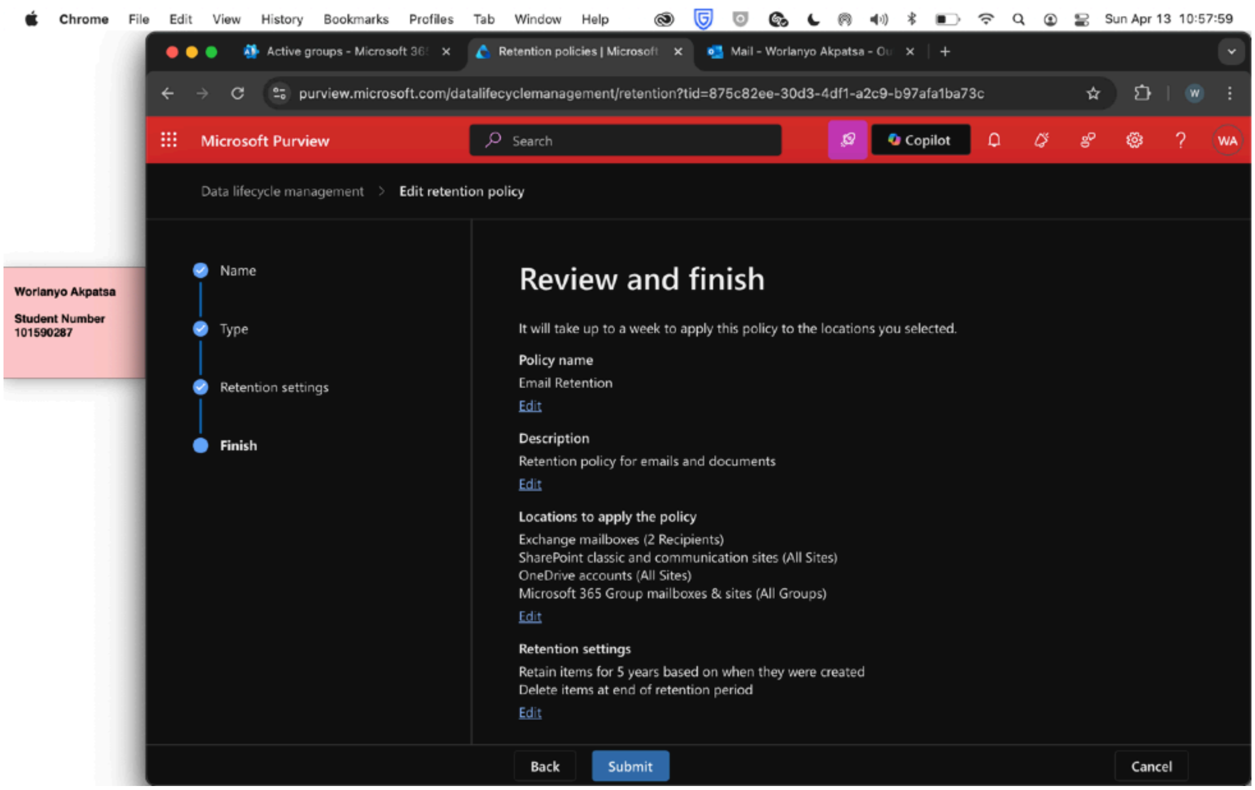
D: Selecting retention settings (i chose to retain for 5 years then delete after)



Student Name: Worlanyo Akpatsa
Student ID: 101590287
Term: Winter 2025

~ ~

E: Review and finish



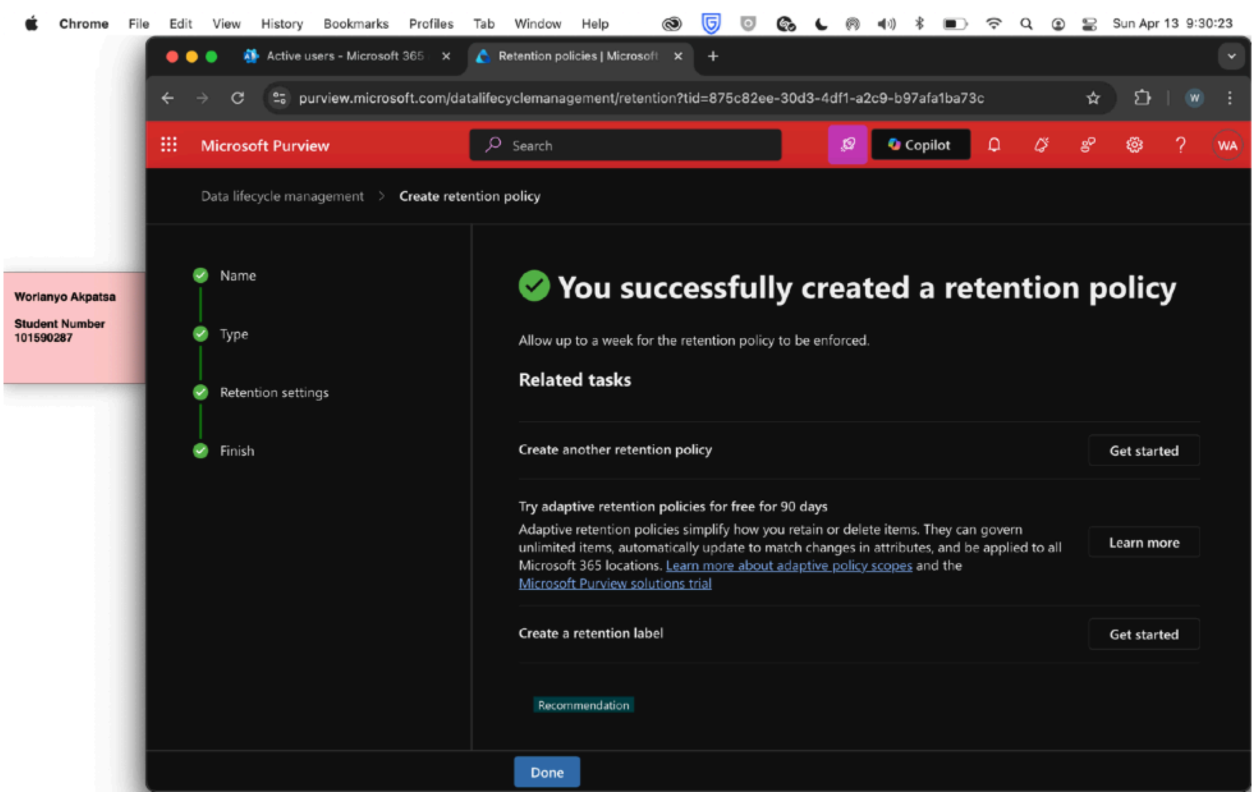
~~~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

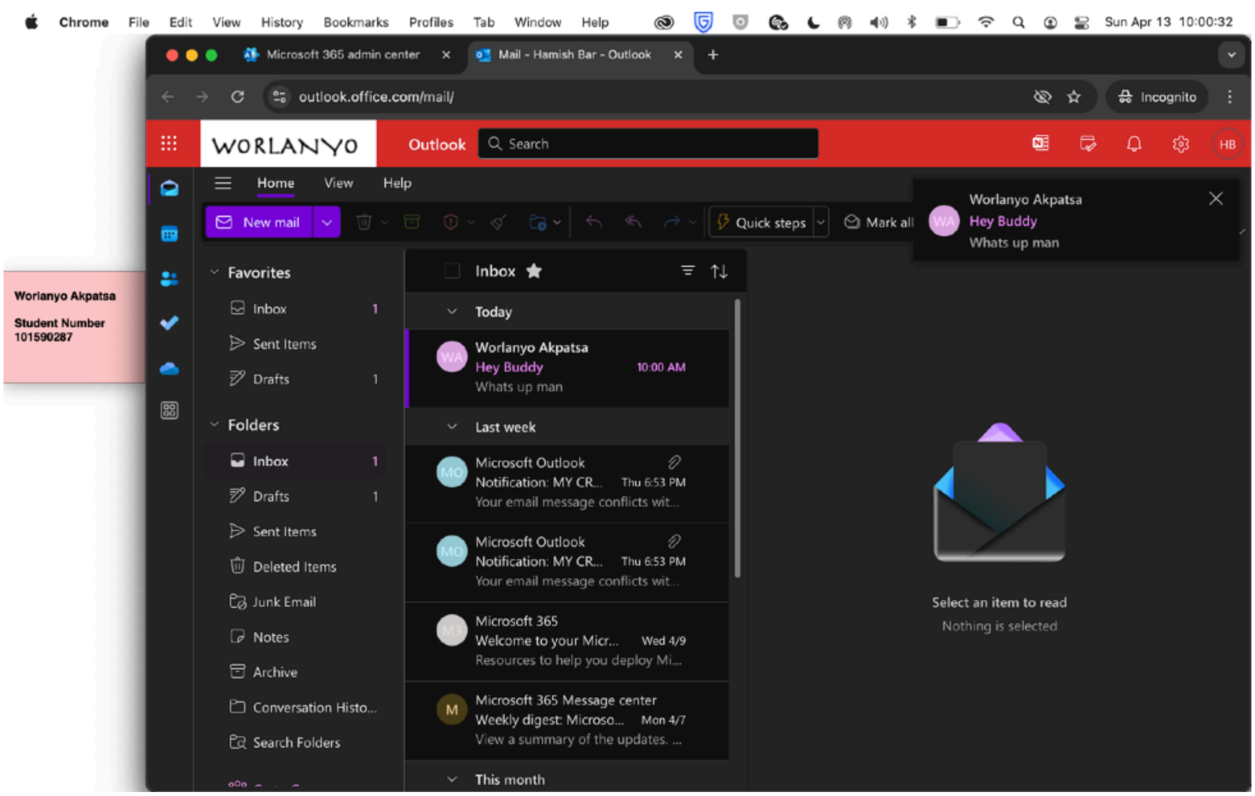
~~~~~~

F: Retention Policy created

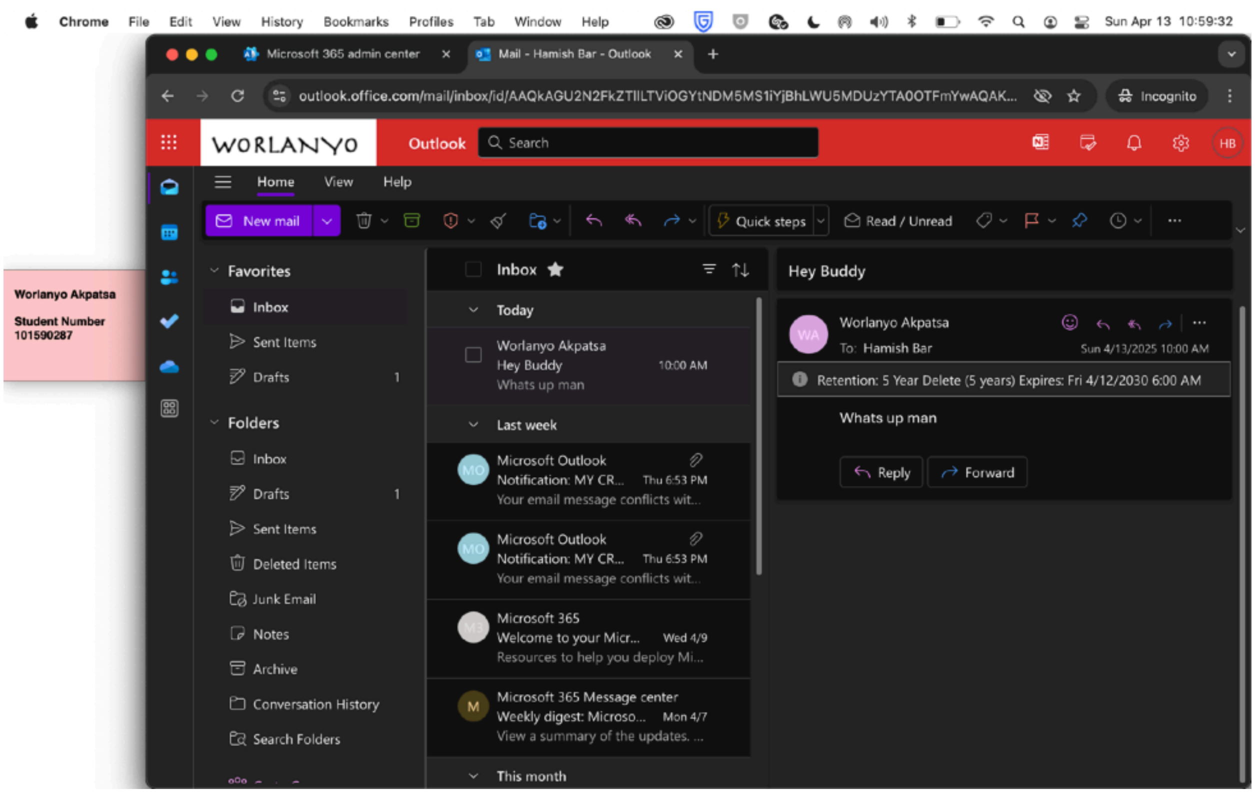


2.4: Verify the policy is working by checking the retention status of emails and documents

A: Sign in to Outlook of one of the users selection for the policy



B: Open a new email from the inbox (retention label at the top of the message)



Task 2 Summary

Task 2 was very similar to task 1 in the sense that I had to create a policy in the compliance center and test that it was working. Because I was so familiar with the process from task 1, doing this task was pretty easy.

To begin I had to navigate to the left pane and select solutions and then under solutions, chose Data Lifecycle Management. When this page opens, I navigate to the subheader “policies” and under that, selected retention policies.

Next, it is time for me to create my policy. I chose “+ Create New Policy” and entered the create policy page.

I entered my policy name, which was email retention. After this, I chose my retention type which was static. I learnt that the other type, which was adaptive is best for big businesses while the static one could be used for labs like this one.

After this, I chose the locations for the policy to be applied. Just like for DLP, they were already selected so I just chose 2 users for exchange and clicked next.

Next step was to decide if I want to retain content, delete it or both. I ended up choosing to retain the content for 5 years and automatically delete it after. After this I just reviewed my policy settings and finished. My retention policy was created.

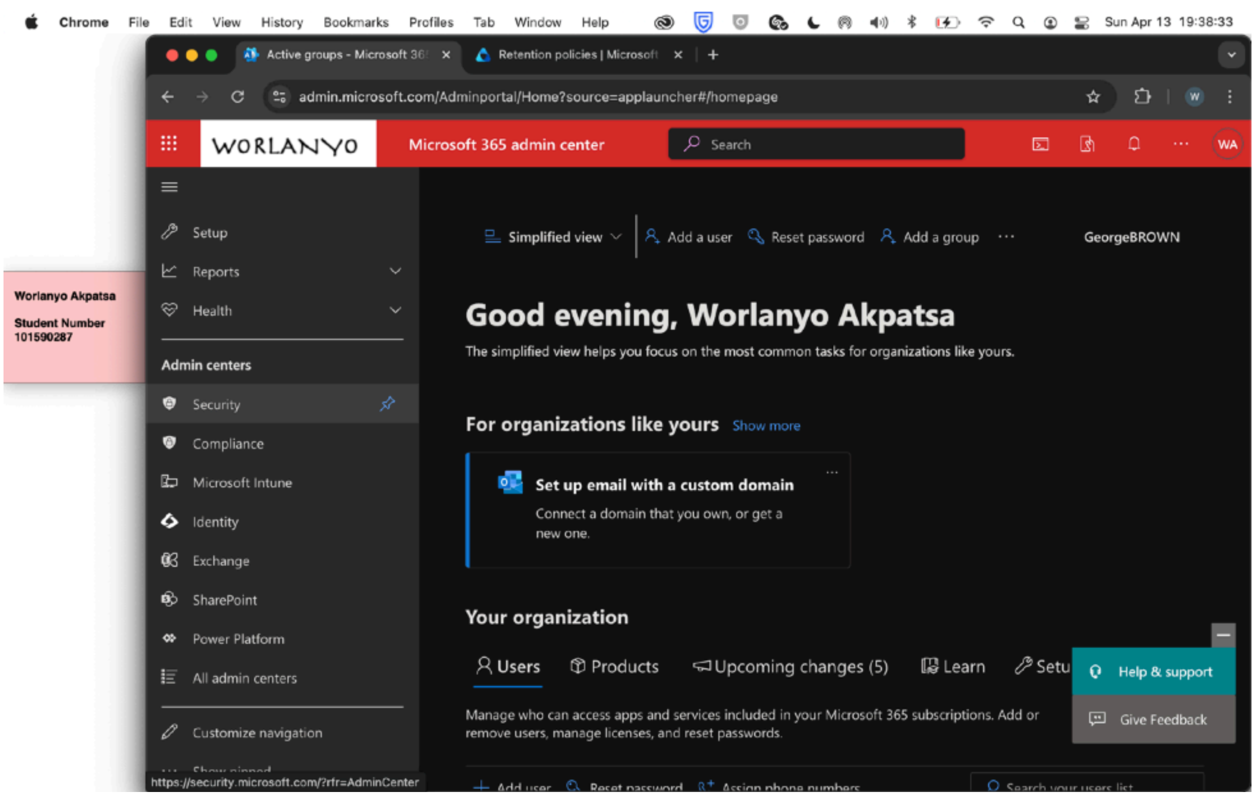
Now it was time to test it. I logged into Outlook with one of the selected users credentials and viewed a recently sent email in the inbox. At the top, there was a label at the top which displayed my retention policy. With this, I knew my policy creation was successful.

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

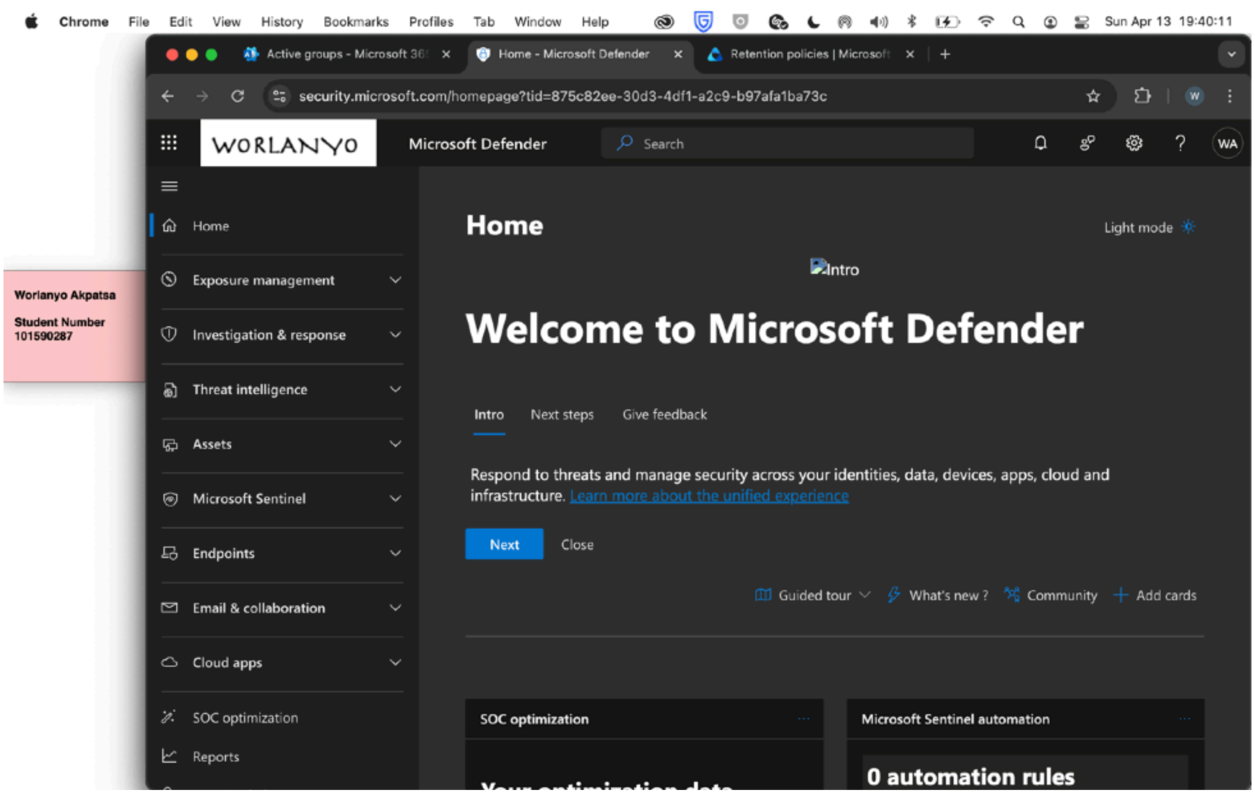
TASK 3: CONFIGURE AND MONITOR SECURITY ALERTS

3.1: Access the security center (MS Defender)

A: Navigate to Admin Center Homepage and select security on the left pane



B: Defender Homepage



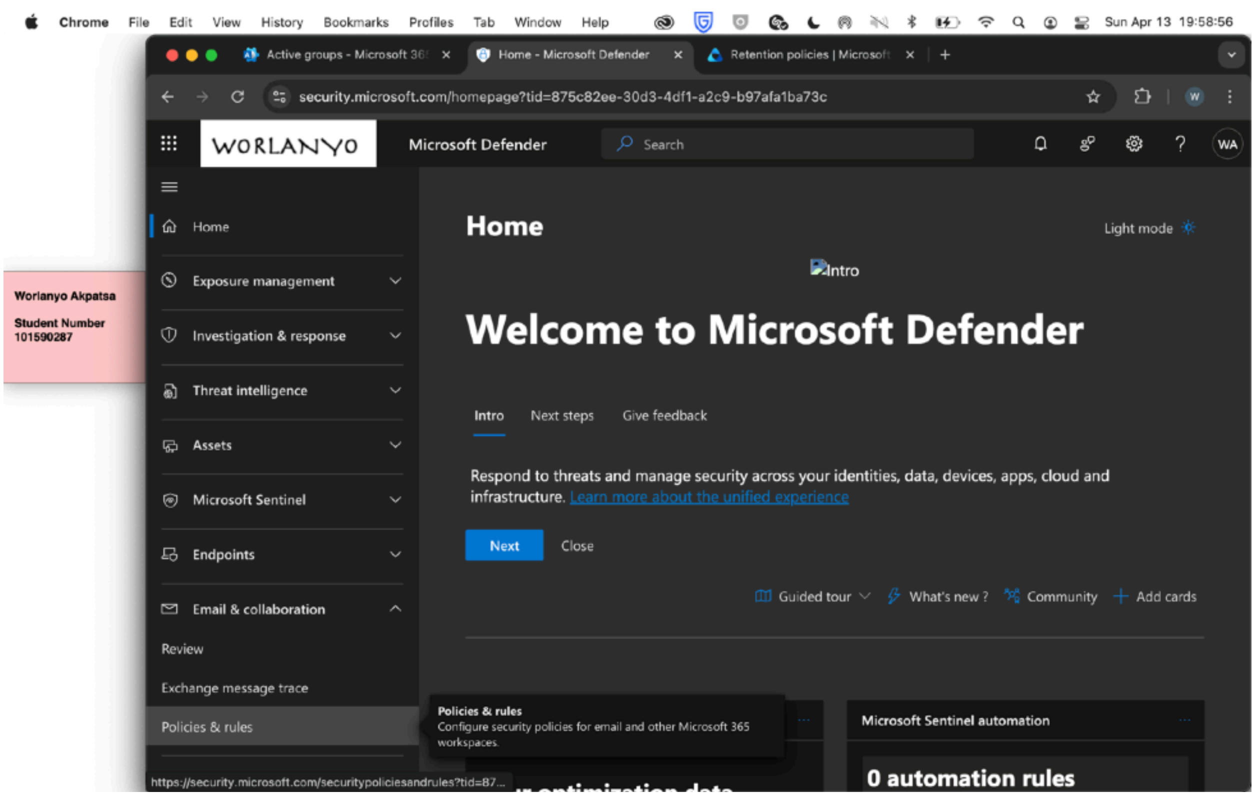
~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

3.2: Set up security alerts (Medium severity) if the users created a mail forward/redirect rule.

A: Navigate to email & collaboration on the left pane then click policies & rules

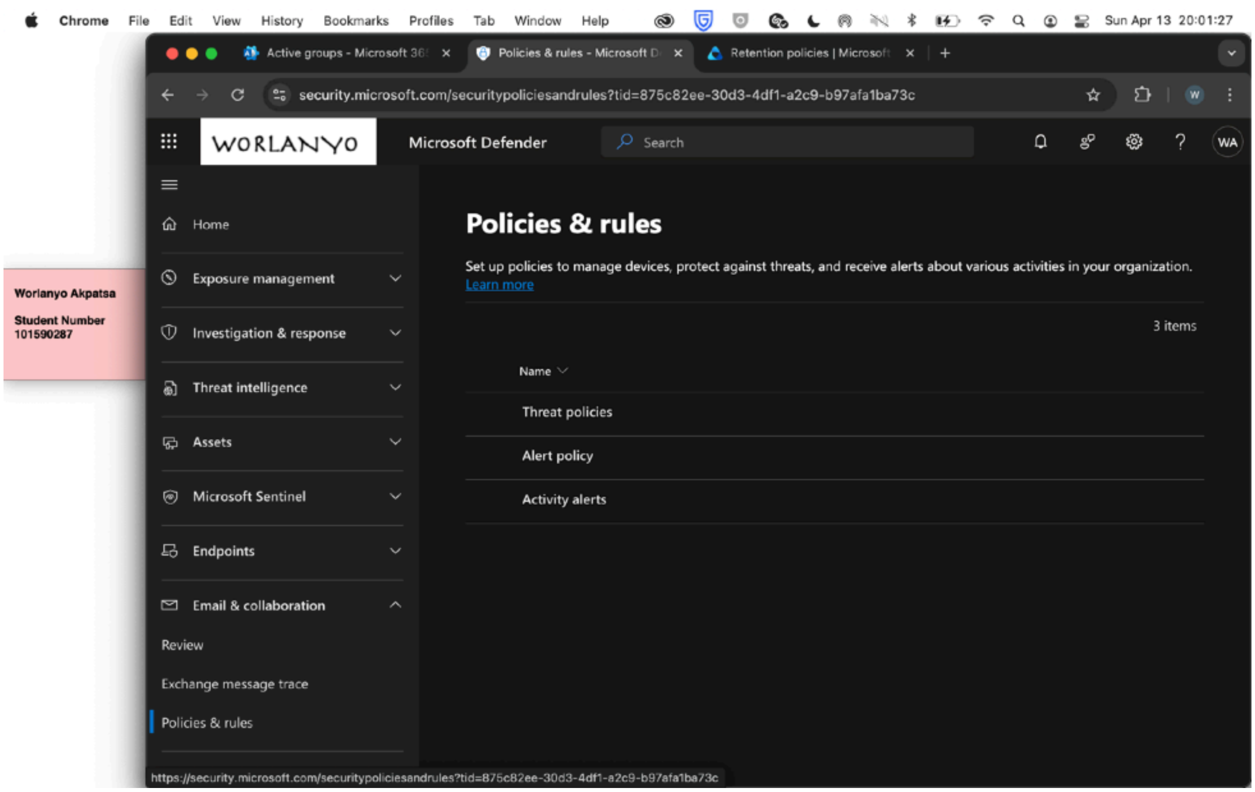


~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

B Select Alert Policy

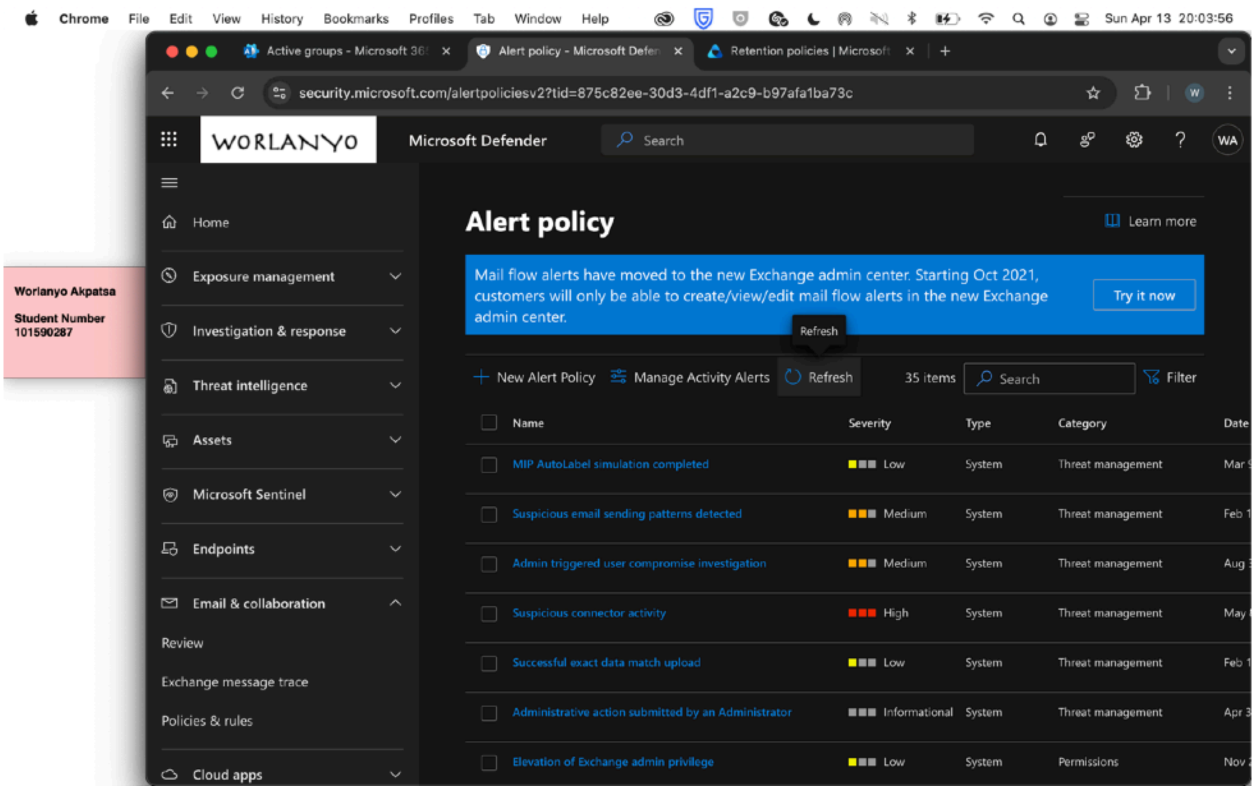


~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

C: Click New Alert Policy



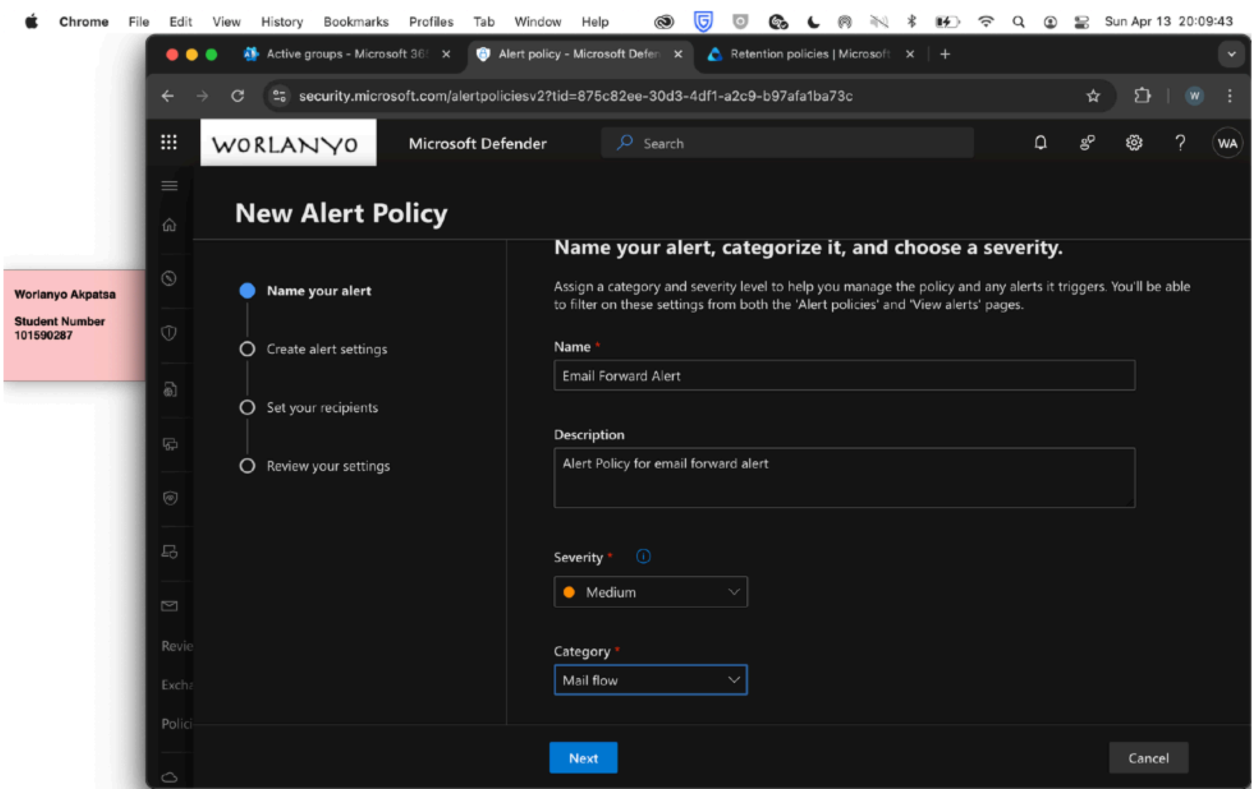
~~~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287

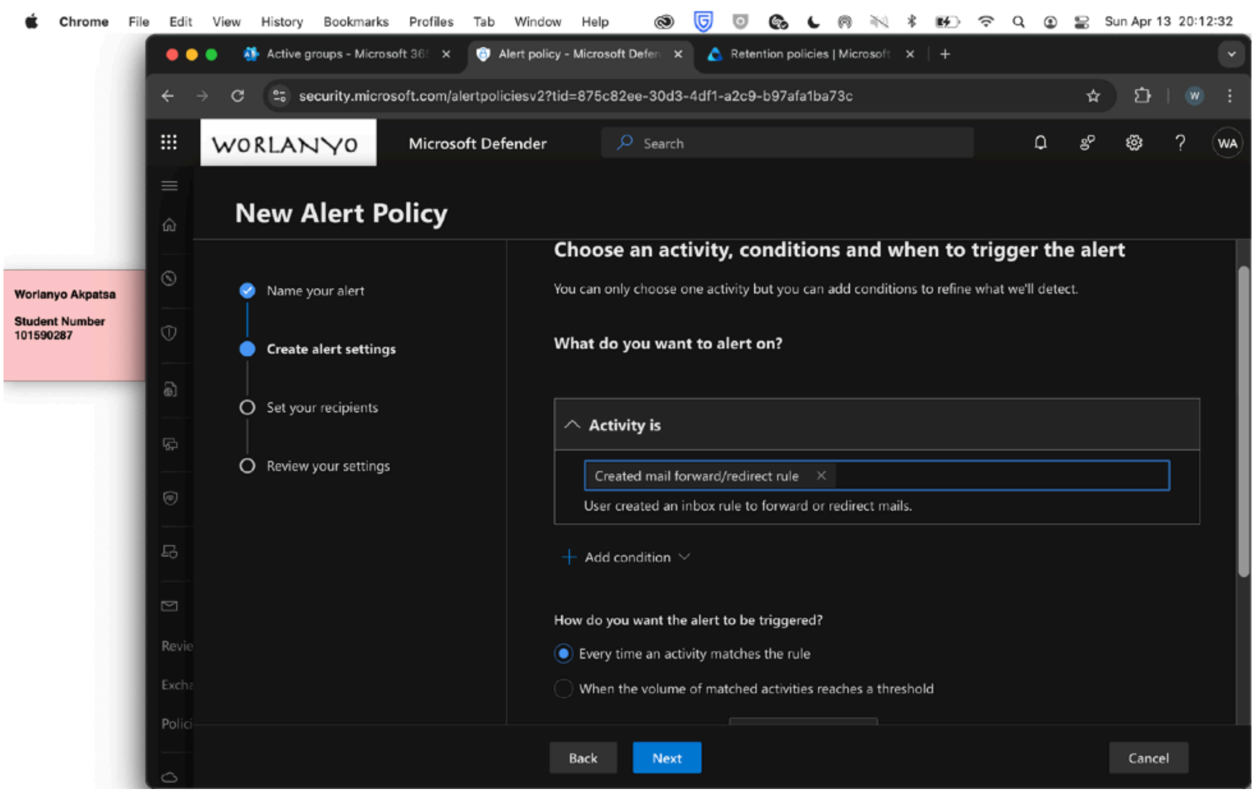
Term: Winter 2025

~~~~~~

D: Setting up name, description and choosing severity as medium

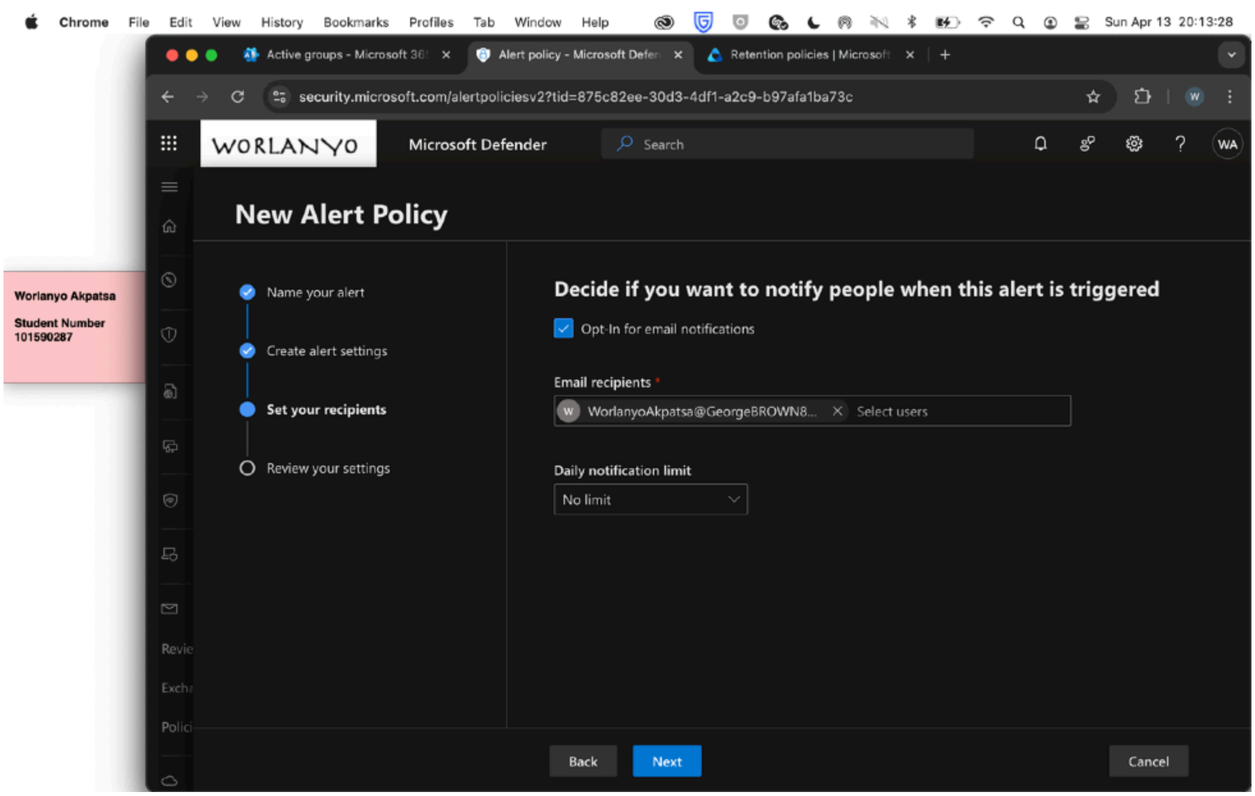


E: Further alert settings (choosing created mail forward/redirect rule)



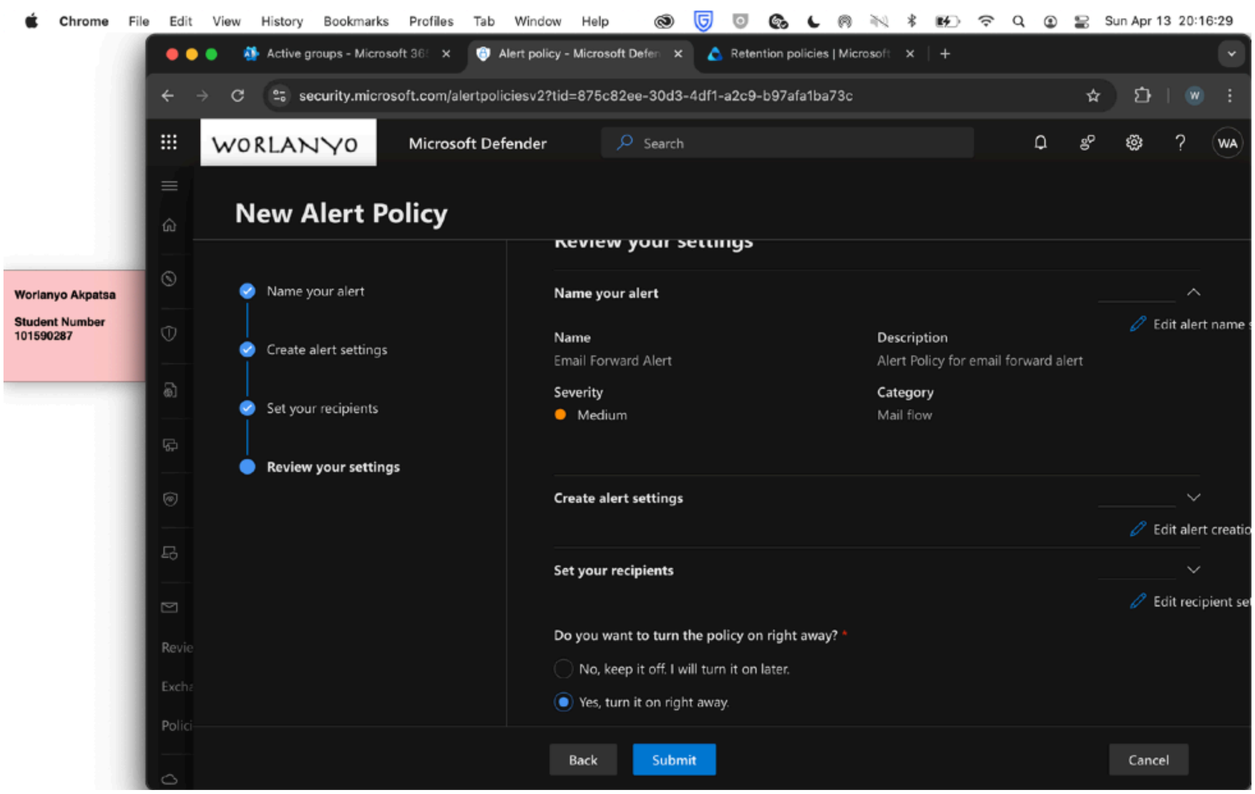
3.3: Configure alert notifications to be sent to an administrator

A: Sending alert notifications to admin



Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

B: Reviewing settings and turning policy on immediately



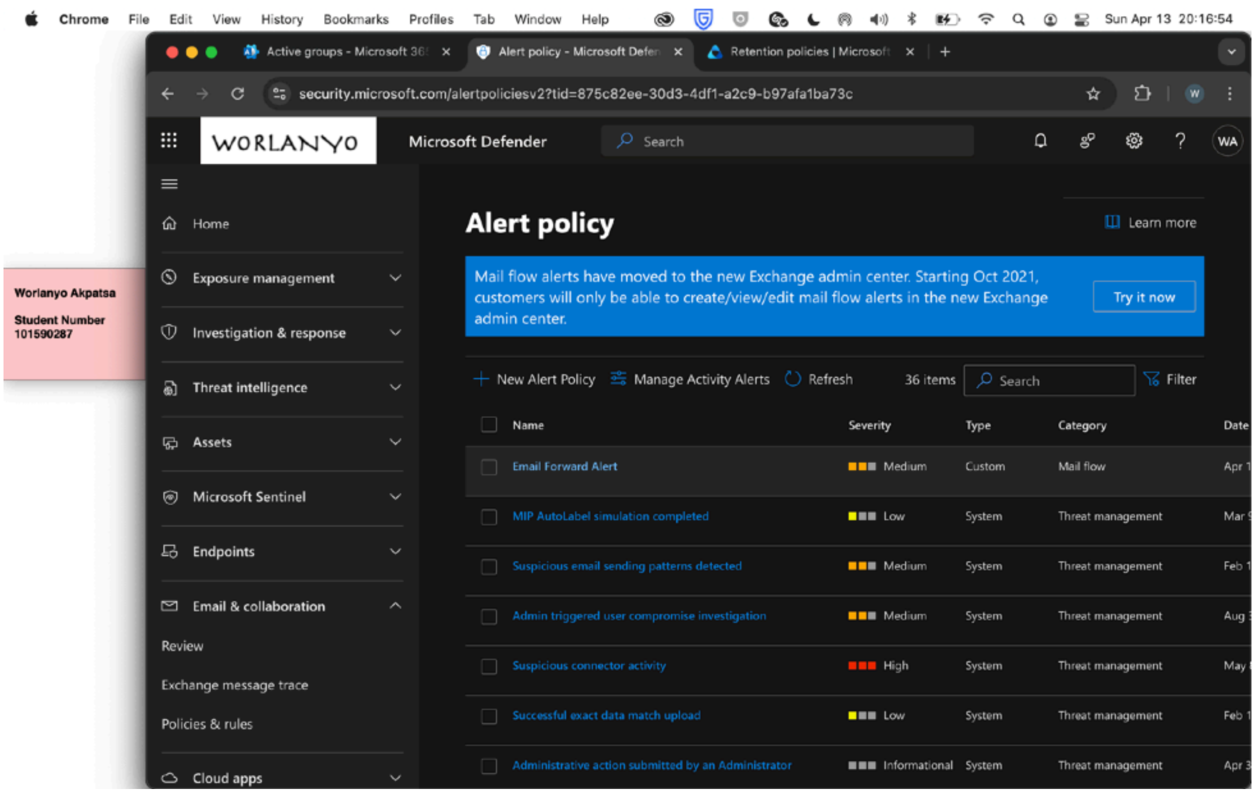
~~~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

~~~~~~

C: Alert policy created

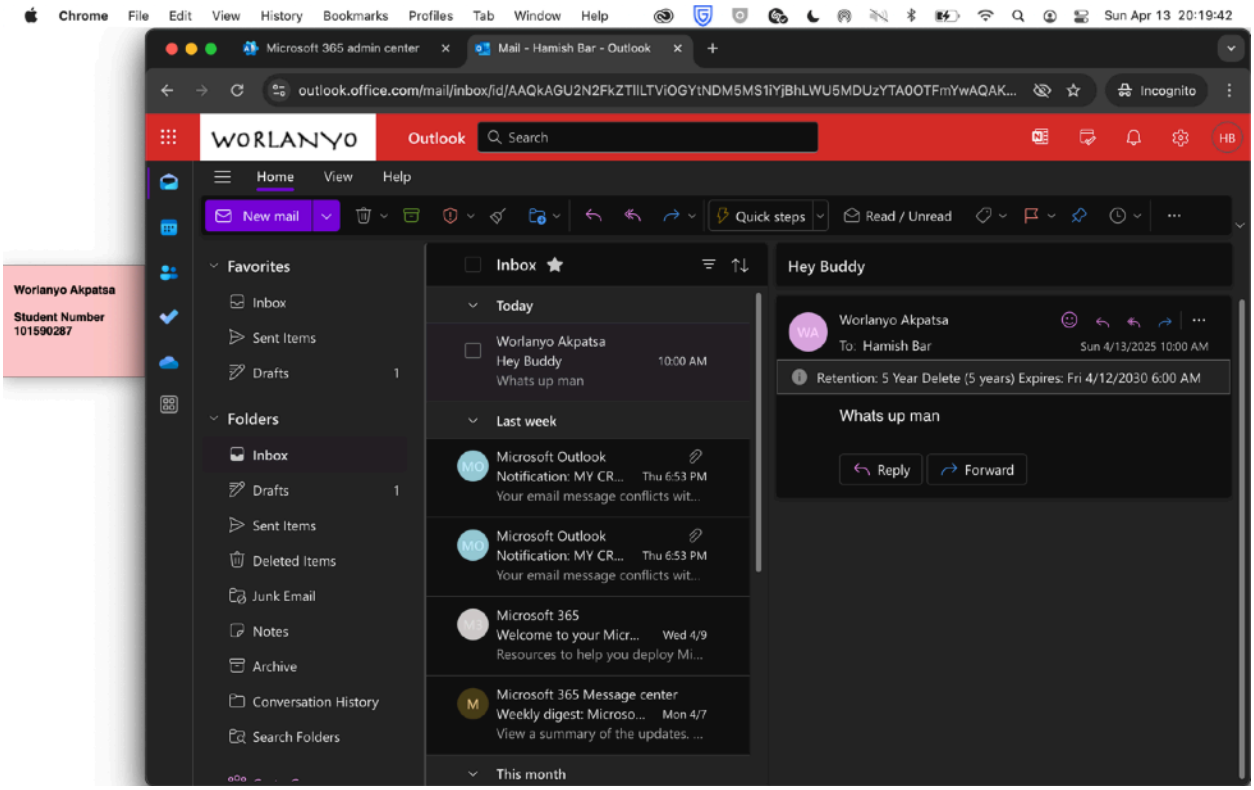


Student Name: Worlanyo Akpatsa
Student ID: 101590287

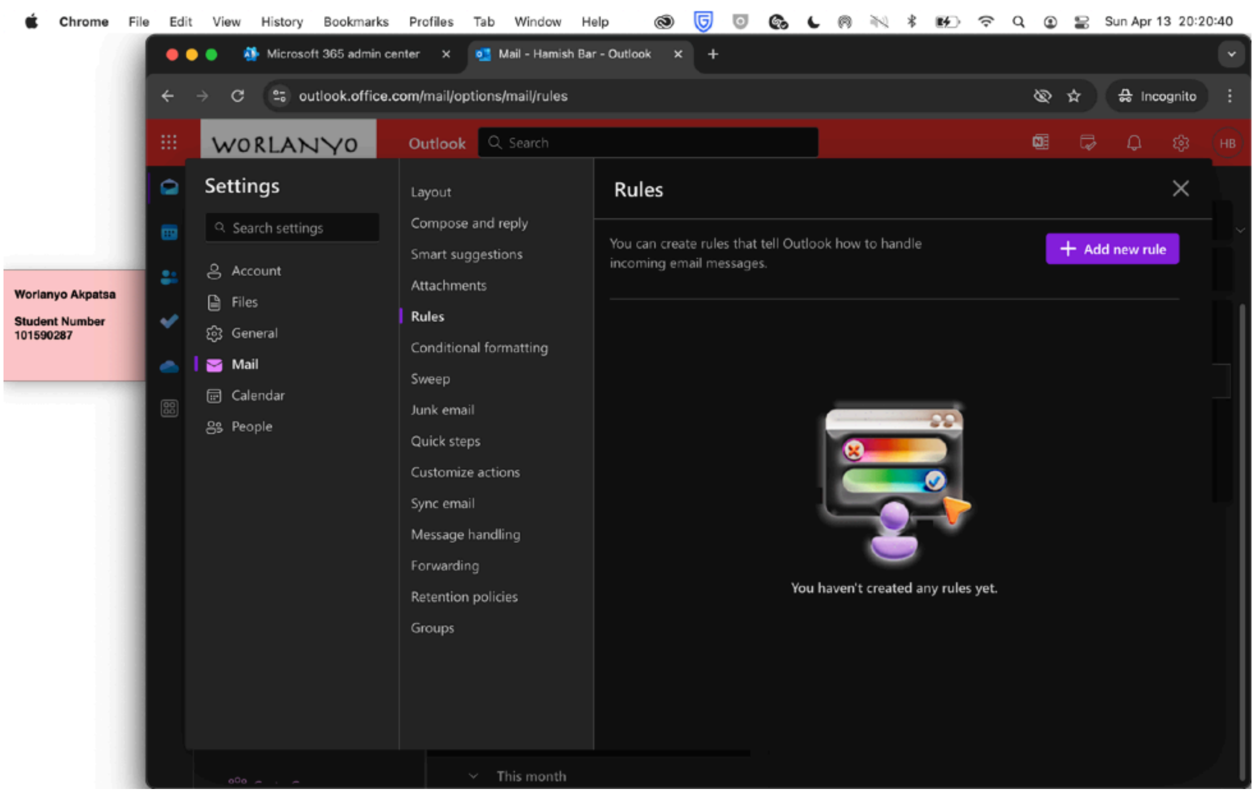
Term: Winter 2025

3.4: Simulate suspicious activity and verify that an alert is triggered

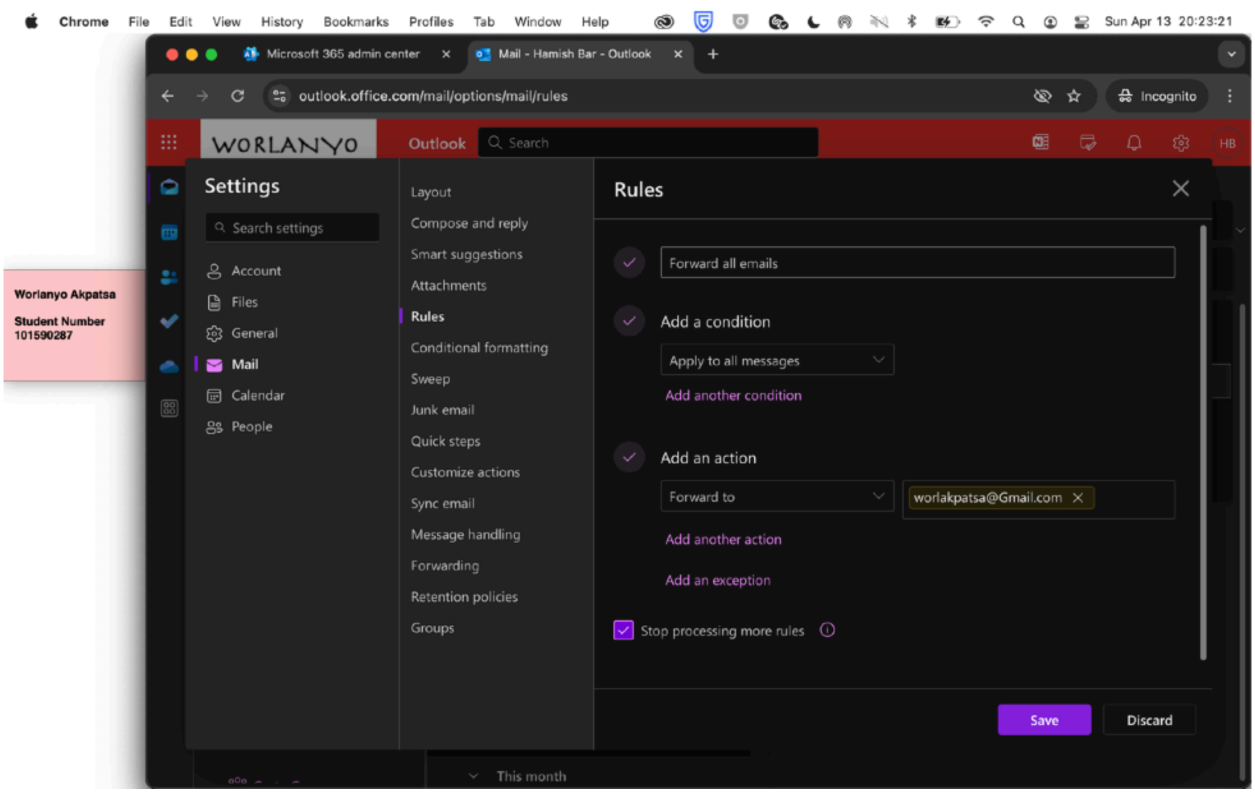
A: Logging into Outlook as another user



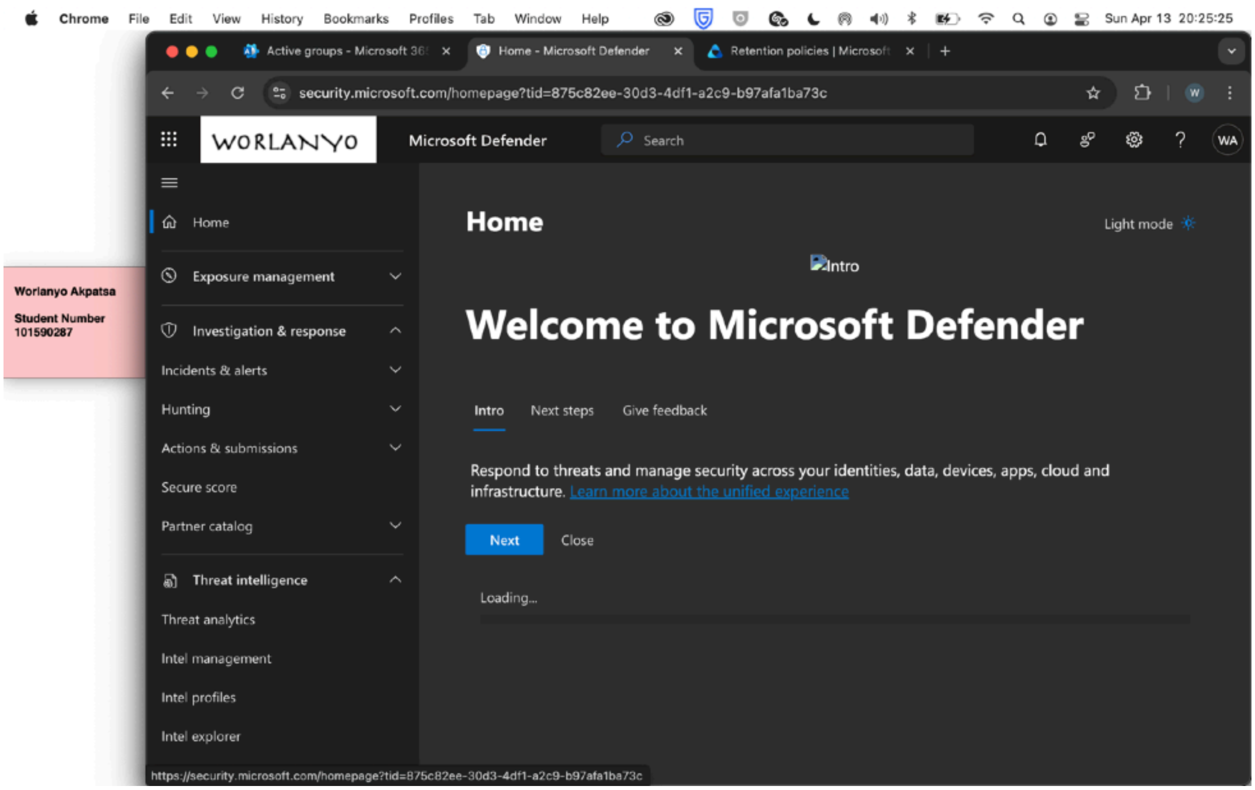
B: Visit Outlook in top right corner and go to Mail->Rules



C: Creating rule to forward all emails



D: Go back to Microsoft Defender Portal Homepage for Admin

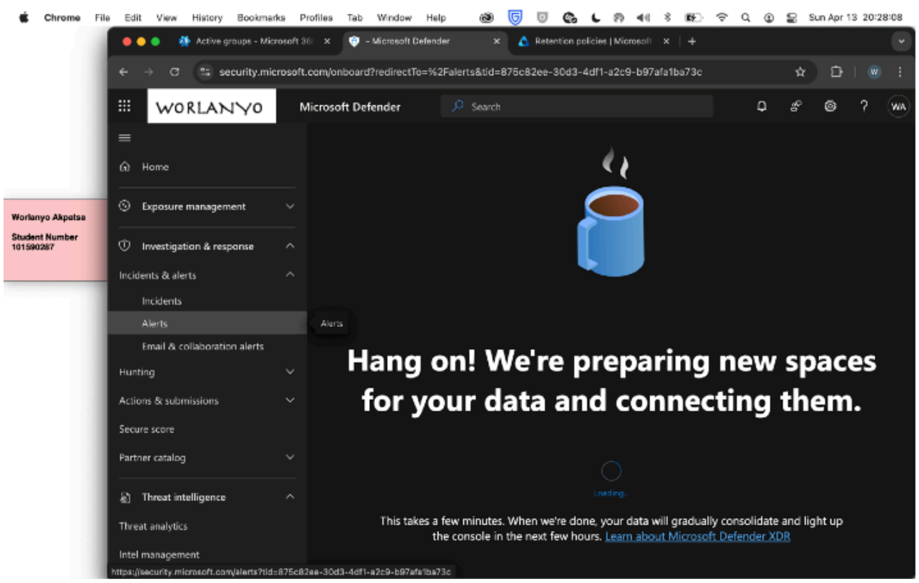


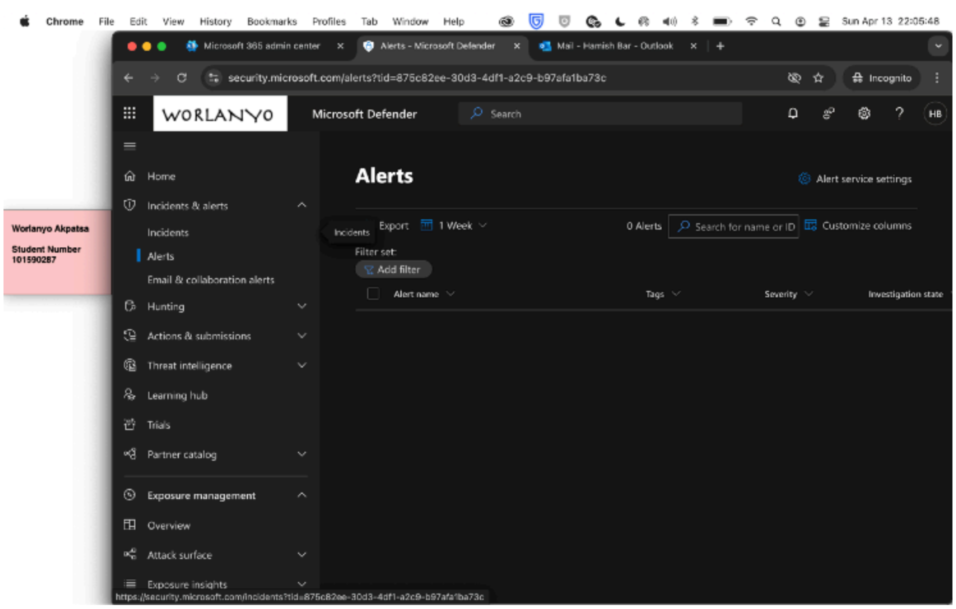
~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

E: On the left pane, under investigation & response, select incidents and alerts, and then alerts





Task 3 Summary

Task 3 followed a similar theme to the past tasks; that is, creating a policy and then testing it. This time, I had to use the 365 Defender portal. To explain, I had to set an alert policy and then simulate something worthy of an alert and view it in the defender portal.

As mentioned earlier, the 365 Admin Center is the one place where you can navigate everywhere so to get to the defender portal, I went to my admin center homepage and on the left pane, I scrolled down and selected security under admin centers. This takes you to the defender portal.

In the defender portal on its left pane, i scrolled to email & collaboration and then selected policies and rules. This opens a page where there are several types of policies. I chose alert policy and chose to create a new policy.

I named my policy email forward alert, described it and set my severity to medium. Next I chose to put an alert on for created mail forward/redirect rule. Then I chose to notify my admin everytime this occurred. After I reviewed and finish my policy creation process.

Next thing was to simulate an alert situation so I signed in to Outlook using another users credentials. Then I went to outlook settings and then mail rules and created a rule to forward all emails to an outside email address.

After this I went back to my defender portal and on the left pane, under incidents and alerts, I clicked on alerts. Unfortunately, I was not able to immediately see the alert to prove that my policy was working; however, I truly understand the process and for that I am grateful for.

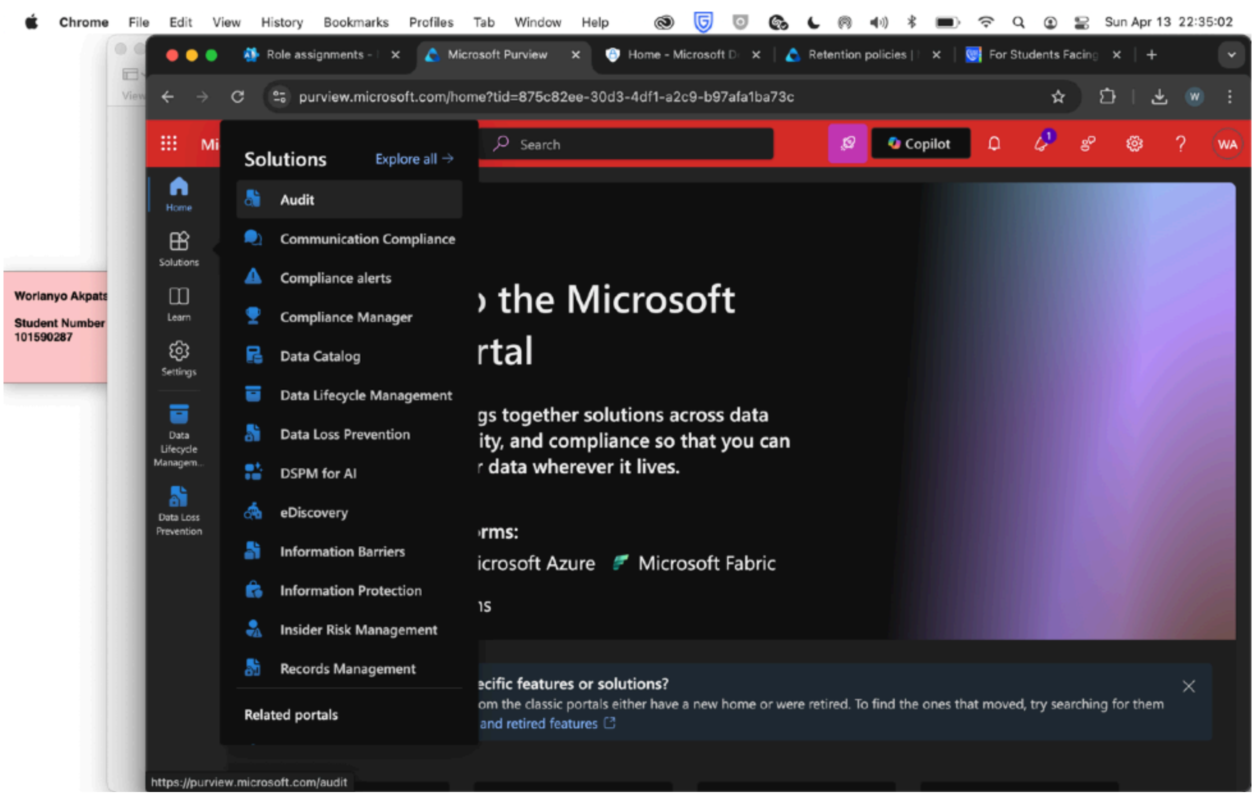
I read that it takes a while for policies to go into effect so maybe that it what was occurring but I will keep checking to make sure it worked and if not, I will contact prof for answers or try to troubleshoot myself.

Something I also learnt is that global admins don't have access to view alerts so I had to assign the role of security admin to the user whose account I was using in the defender portal.

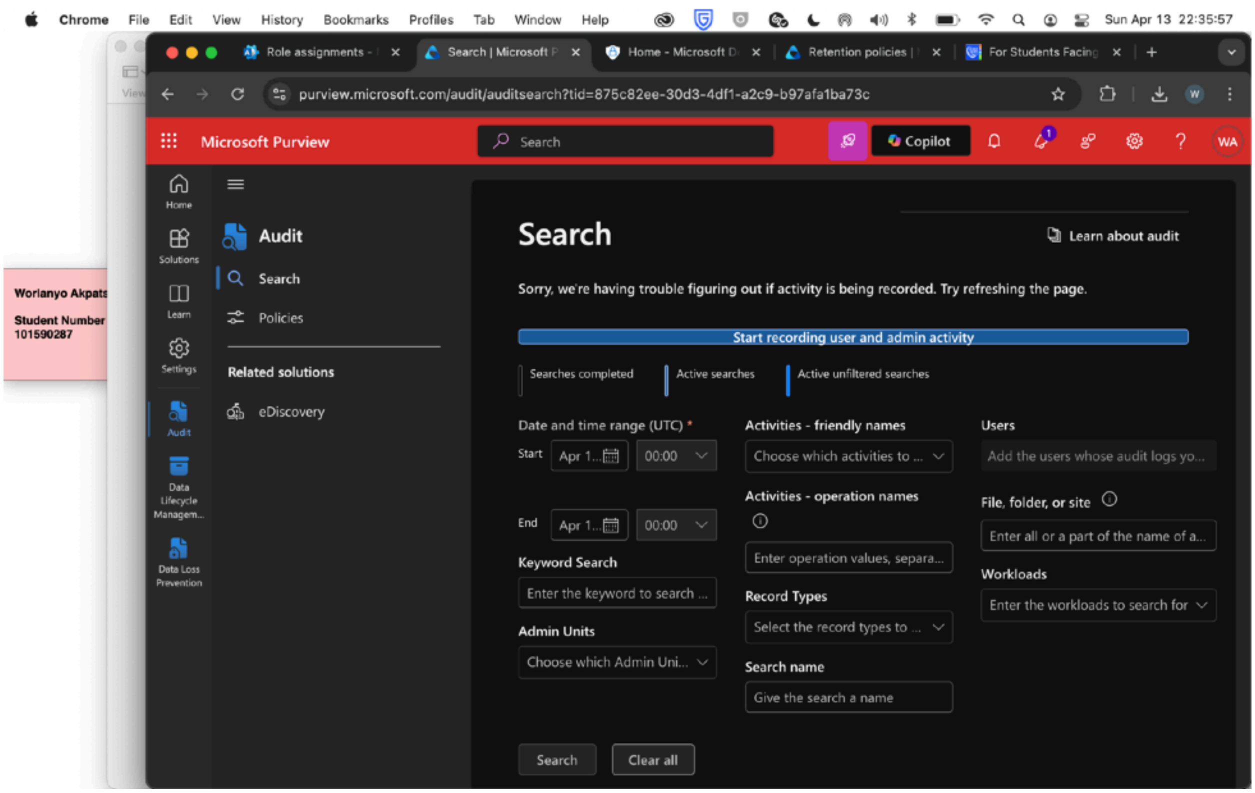
TASK 4: REVIEW AND MANAGE AUDIT LOGS

4.1: Enable auditing in the Microsoft 365 Compliance Center

A: Open Compliance Center Homepage. Under Solutions, click audit



B: Enabling Auditing by clicking 'start recording user and admin activity"



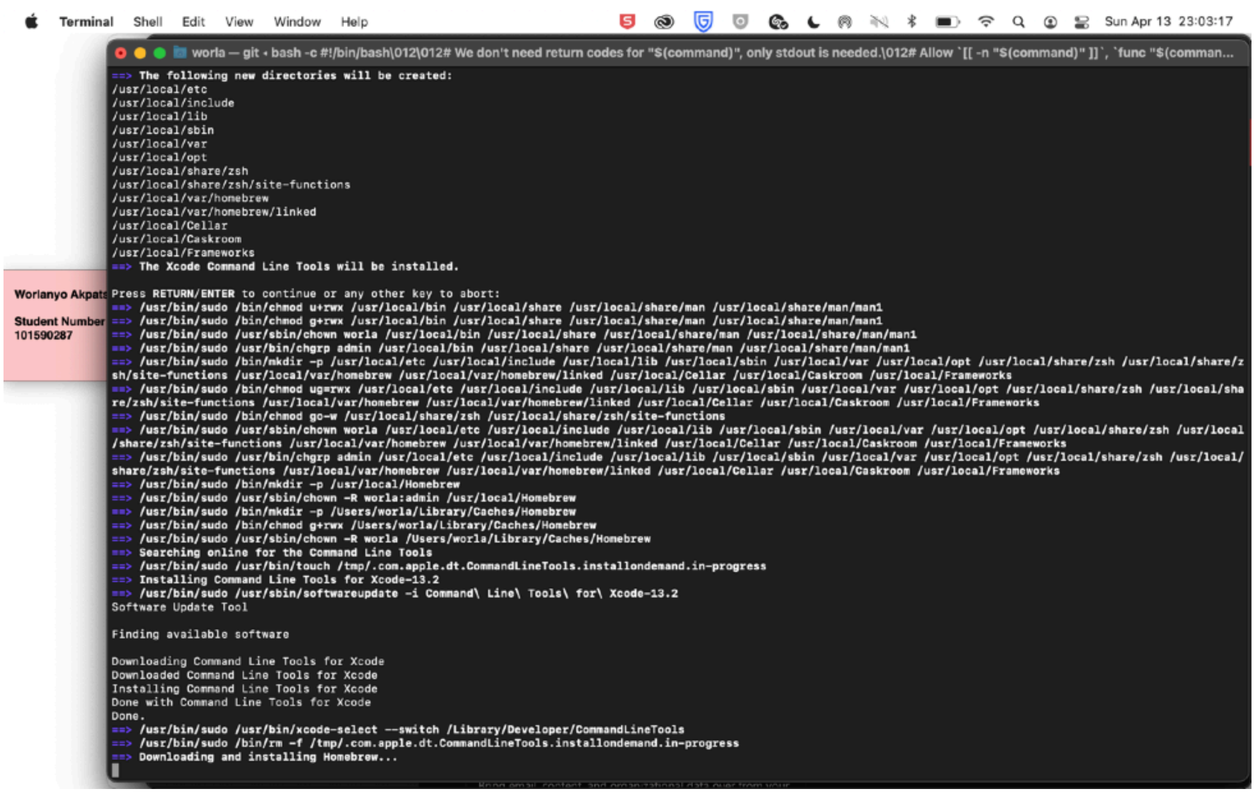
~~~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

~~~~~~

C: Installing powershell on macbook using terminal (first, I had to download and install command line tools for xcode as well as Homebrew)

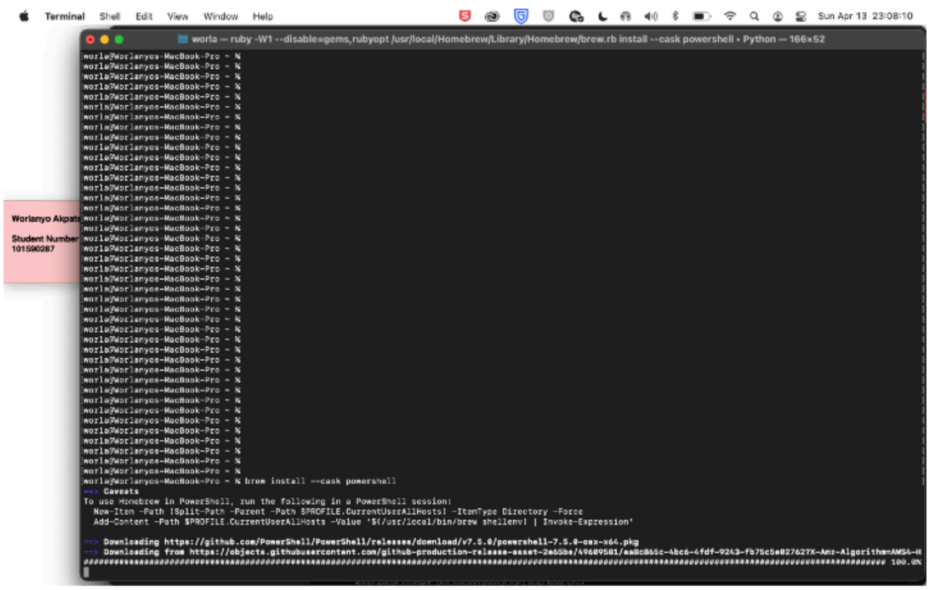


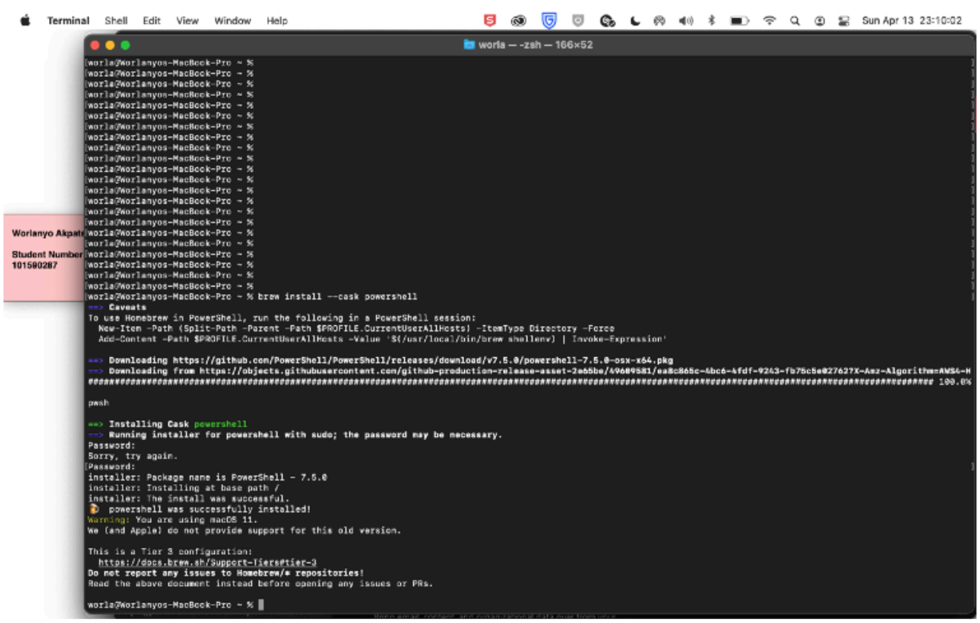
~~~~~~

Student Name: Worlanyo Akpatsa | Term: Winter 2025
Student ID: 101590287

~~~~~~

D: Downloading and Installing powershell on Mac using terminal

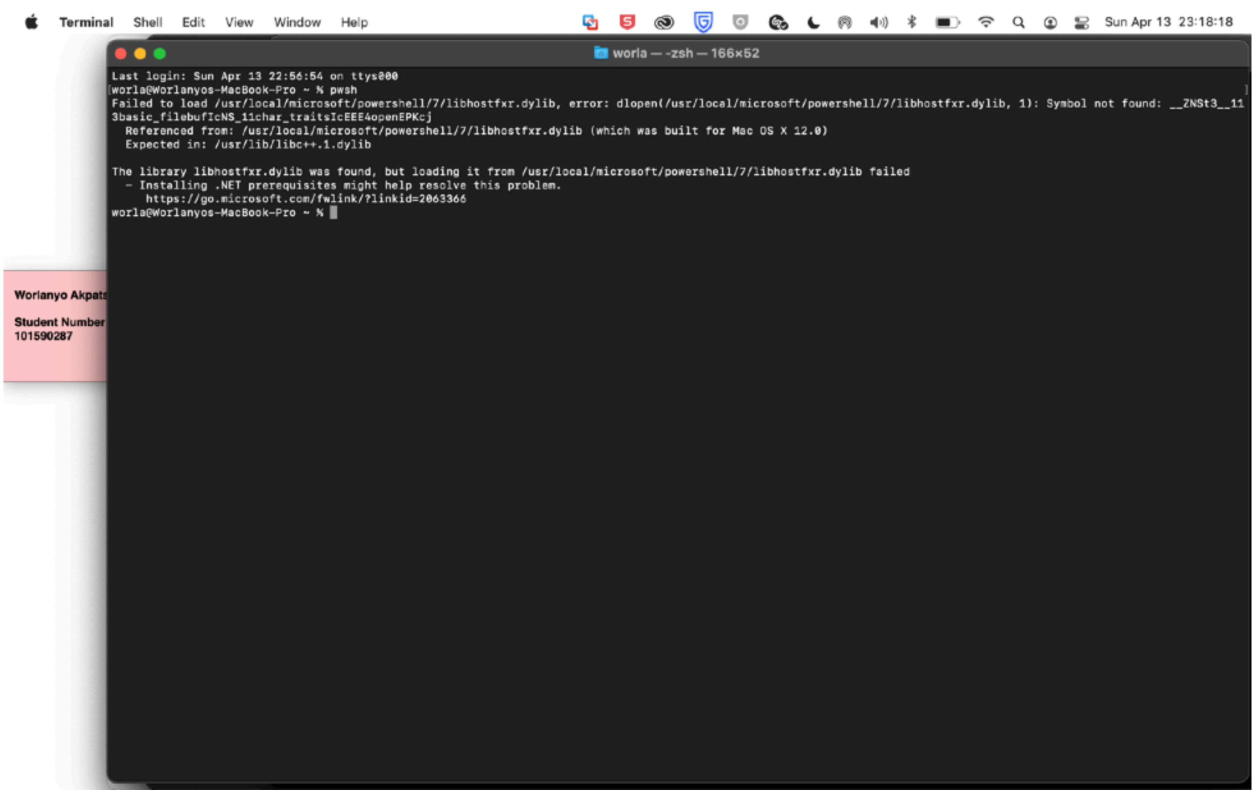




Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

E: Launching Powershell (keep receiving errors which are due to my macs old operating system)



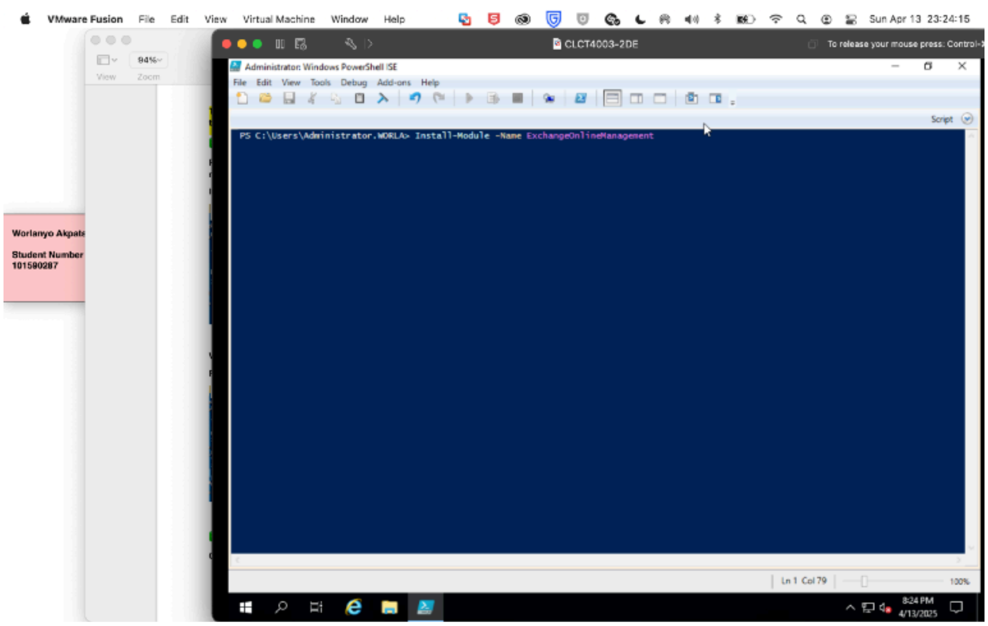
The process of running powershell on my mac was absolutely not working as the hardware is quite old so I decided to continue the steps of Auditing Log reviews on powershell using a VM.

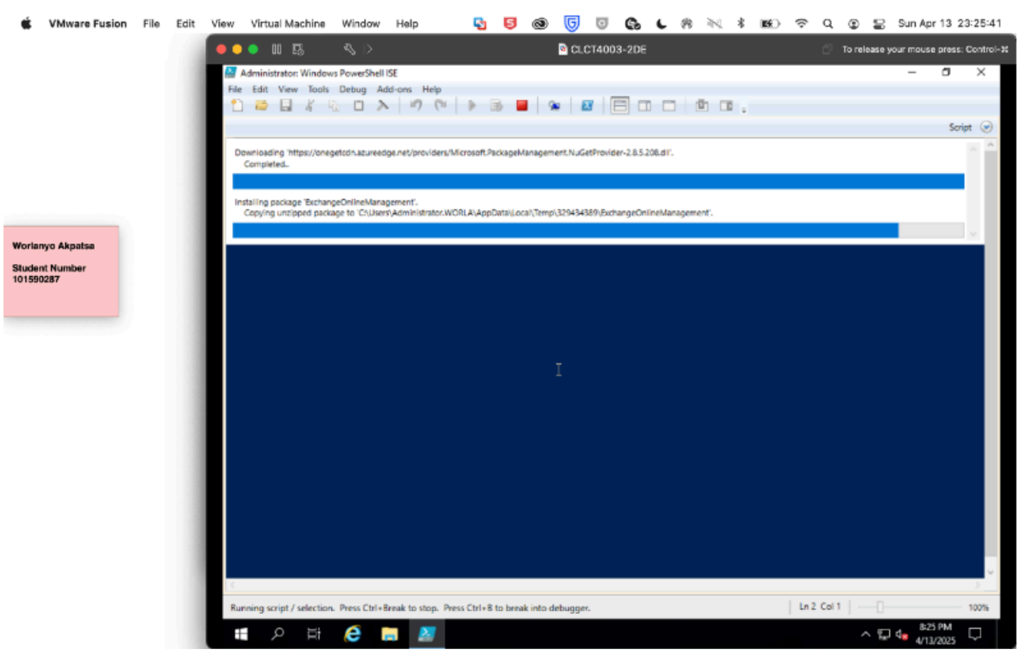
~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

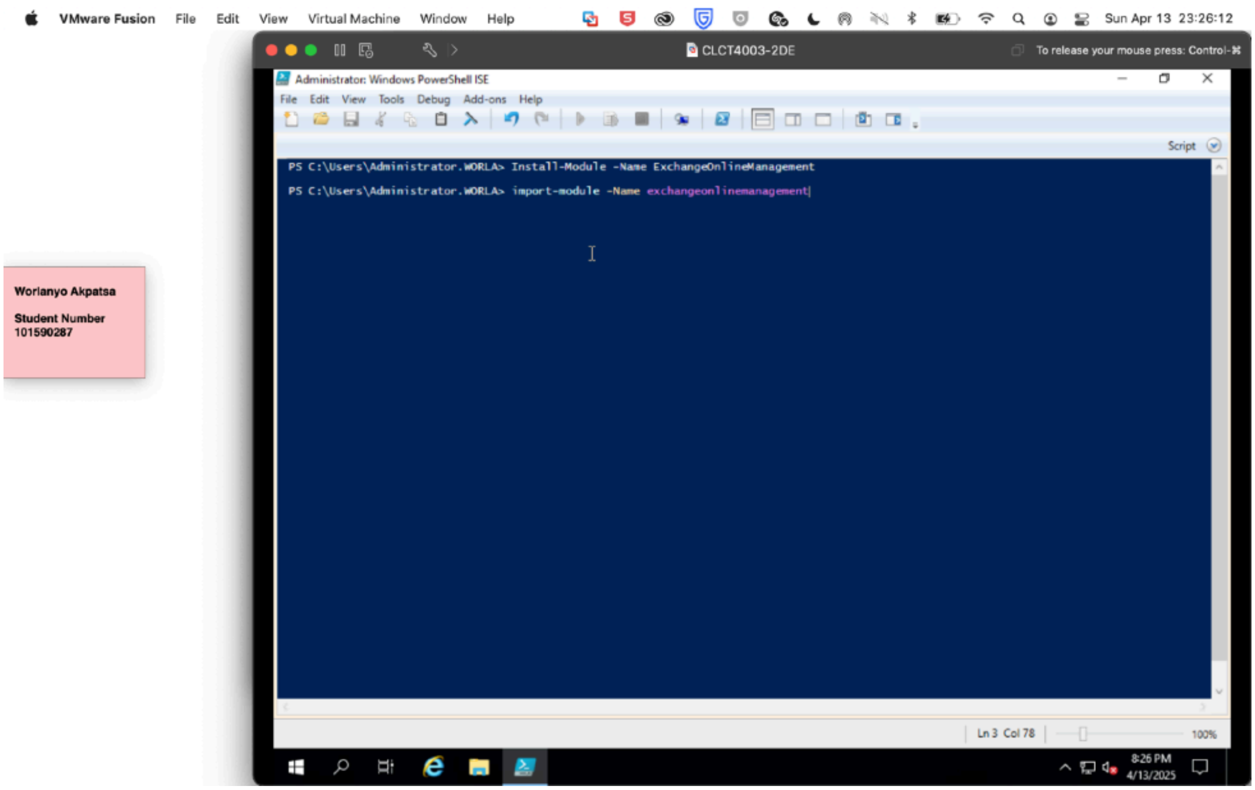
~~~~~~

A: Installing Exchange Online Module





B: Importing Module

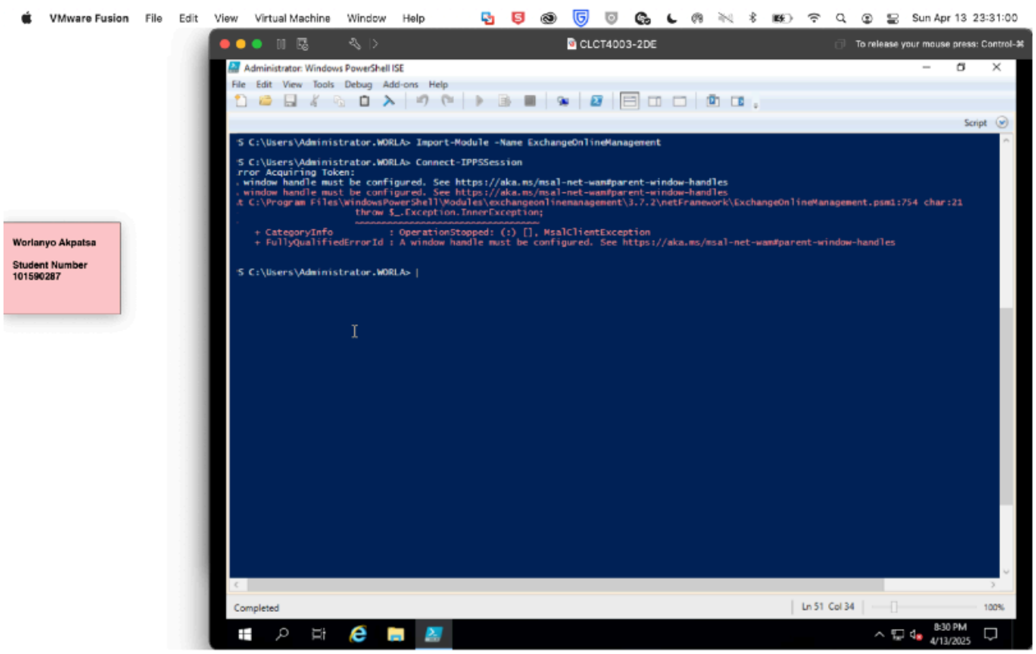


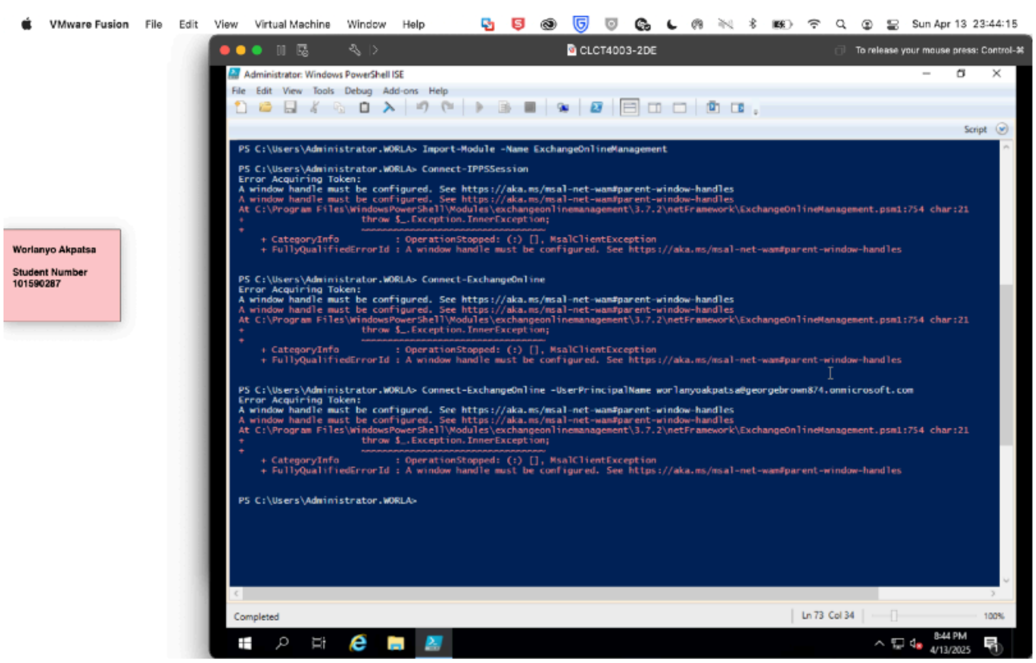
~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

C: Connecting to 365 Compliance Center





I am having so much trouble with this task I must admit and it is not allowing me to move forward and connect to Microsoft using powershell. I want to prove that i know the steps to be taken.

After you import the module, you have to connect to 365 Compliance Powershell using Connect-IPPSSession. Then log in using your 365 admin credentials.

After you can search the Audit Logs. I planned to search user sign-in activities, email sends and user searches using the following:

Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-2) -EndDate (Get-Date) -Operations "UserLoggedIn" -ResultSize 100

Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-2) -EndDate (Get-Date) -Operations "Send", "SendAs" -ResultSize 100

Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-2) -EndDate (Get-Date) -UserIds "testuser@yourdomain.com" -ResultSize 100

Then I would save this audit log to csv using this code on powershell:

Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-2) -EndDate (Get-Date) -UserIds "testuser@yourdomain.com" -ResultSize 100 | Export-Csv -Path ~/Desktop/AuditLog.csv -NoTypeInformation

And after this, I can visit the compliance center and click audits. Then manually search for whatever I want.

I vow to master this specific task because in the whole Microsoft 365, this is the first task to give me a challenge.

Task 4 was something new altogether as we had to incorporate the use of powershell to audit logs.

To begin, I had to go to the compliance center and on the left pane, under solutions I selected audit and clicked on start recording user and admin activity.

Next thing I had to do was download powershell on my laptop using Terminal as I use a Mac. To do this, I had to install command line tools for xcode as well as install Homebrew.

Next, I used terminal to download and install powershell. Due to my mac's hardware issues because it is old, powershell was not running thus I attempted to continue the process on a vm. I managed to install the exchange online module and import it but after this, i just kept getting met with errors as powershell would not allow me to connect to Microsoft.

Nonetheless, I made sure to learn more about auditing logs in this task and I guarantee I will master it in no time.

All in all, I enjoyed activity 2. It showed me parts of Microsoft 365 I never knew and I will make sure to keep practicing to master it.