Microsoft 365 Identity and Services – Enterprise Administration

~~~~~~

Student Name: …………….…………. Term: …………………………...
Student ID: ………………………………...

~~~~~~

Case Project: Implementing and Managing Microsoft 365 Environment for a Mid-Sized Organization

Objective: To provide hands-on experience in implementing, configuring, and managing a Microsoft 365 environment for a fictional mid-sized organization named "TechSolutions Inc."

Scenario: TechSolutions Inc. is a mid-sized IT services company with 300 employees. The company is transitioning to Microsoft 365 to improve collaboration, security, and productivity. As part of the IT team, you are responsible for setting up and managing the Microsoft 365 environment. This case project will cover various aspects of Microsoft 365, including user and group management, security and compliance, and service configuration.

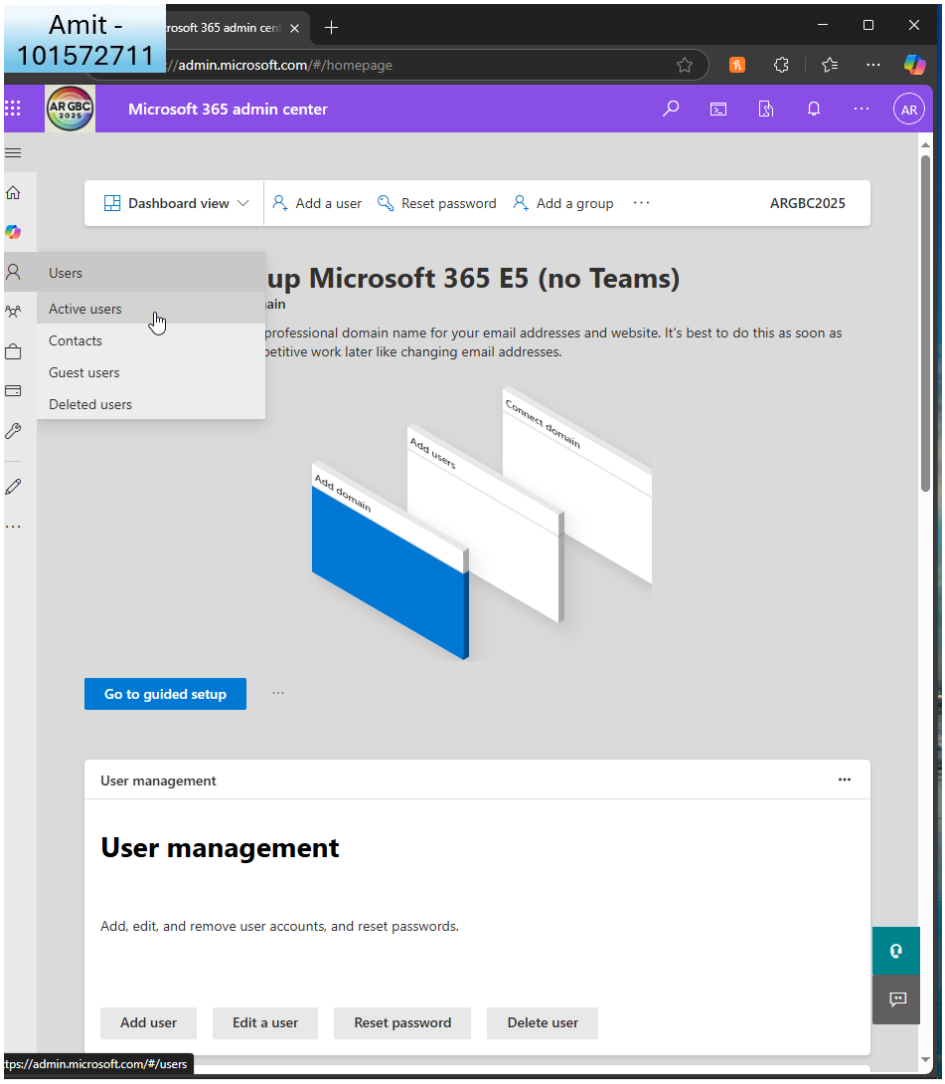
Tasks:

Task 1: Setting Up and Configuring User Accounts

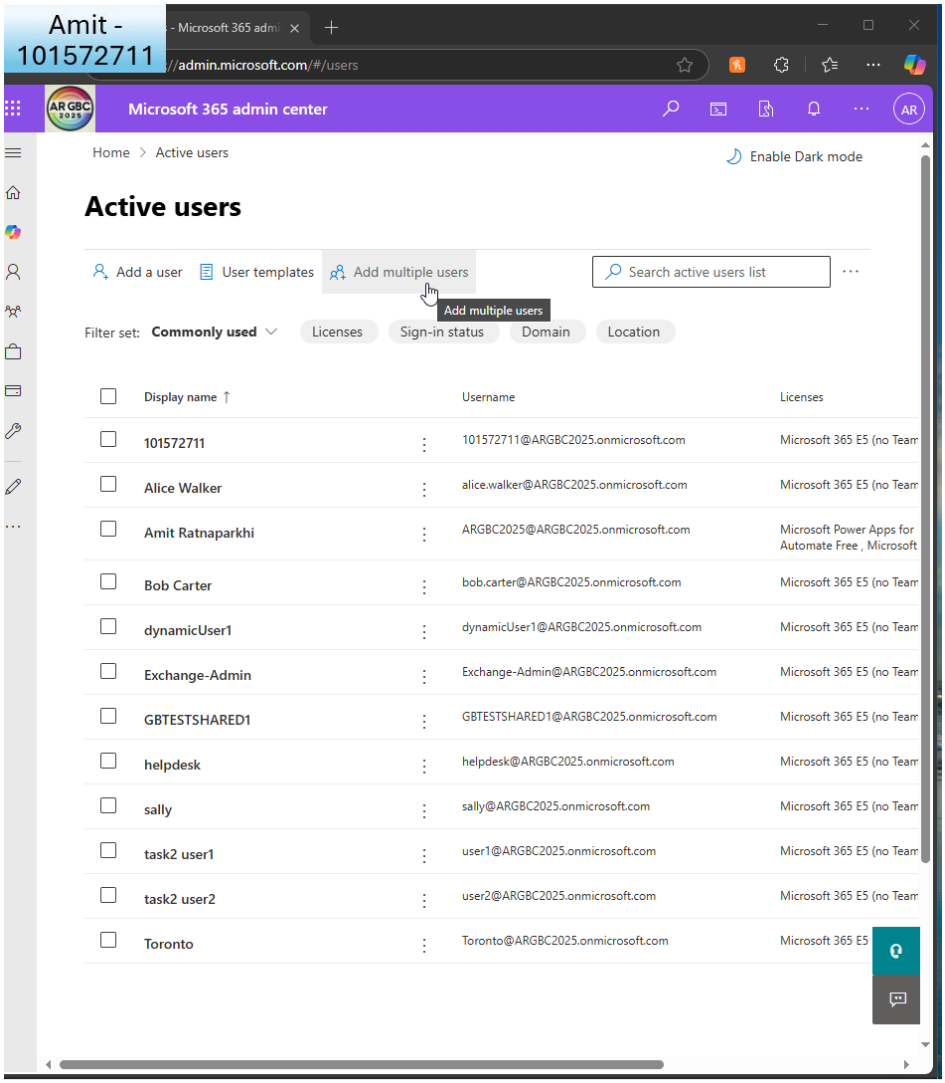
Part A:

1. **Bulk Import Users**:
    - Use the Microsoft 365 admin center to bulk import 10 users from a CSV file.

Student Name: ……. Term: ……..
Student ID: ……..

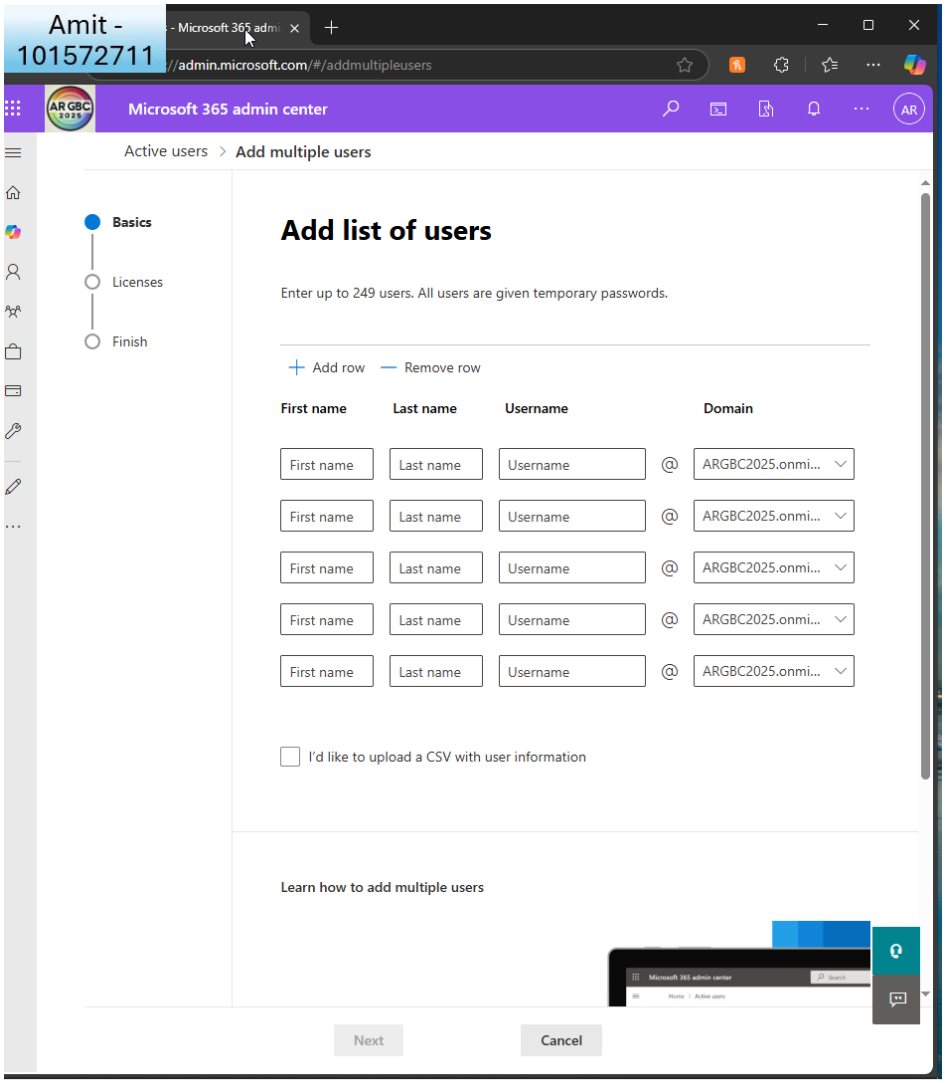


Student Name: ……. Term: ……..
Student ID: ……..



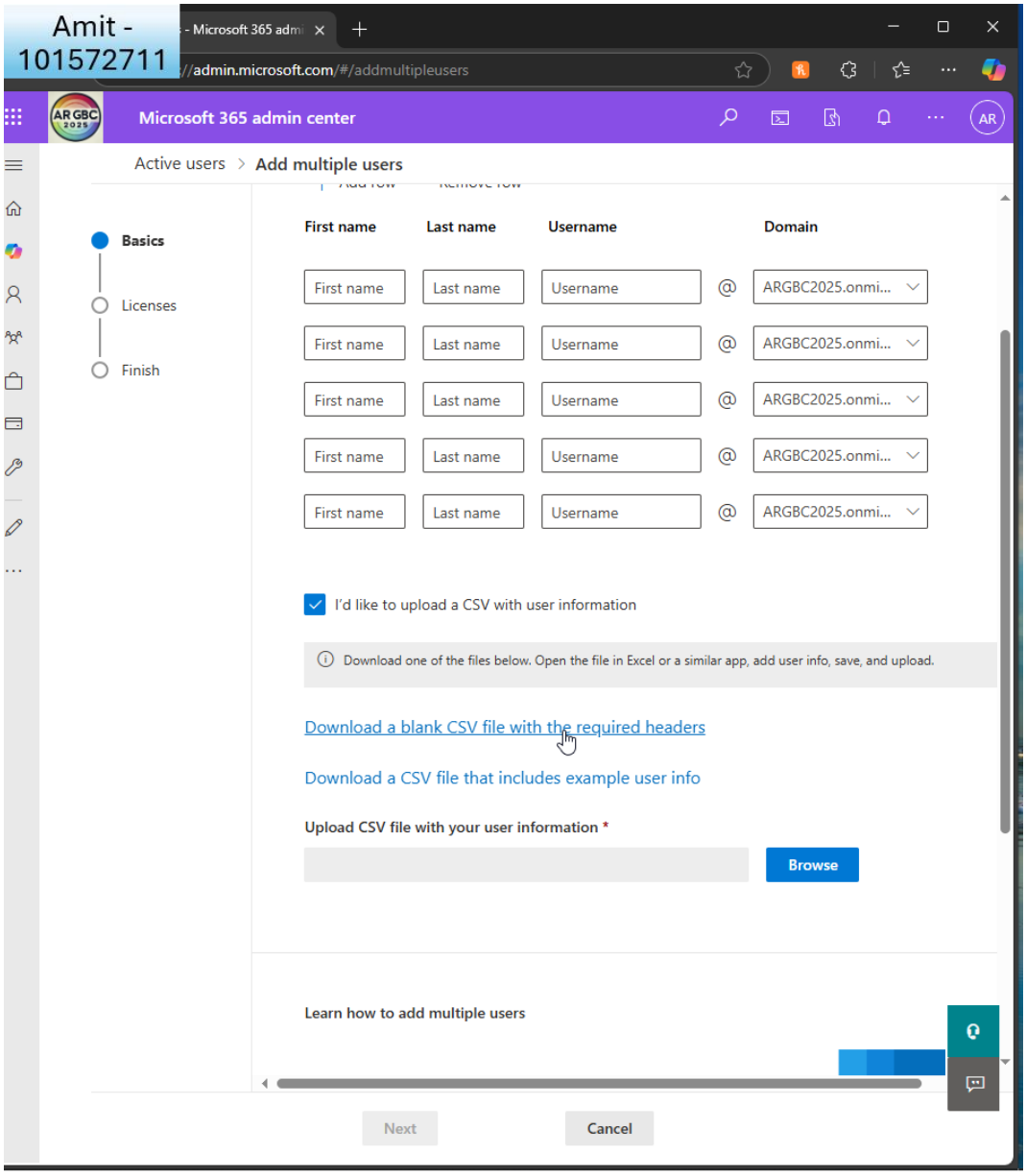
I then add multiple users

Student Name: ……. Term: ……..
Student ID: ……..



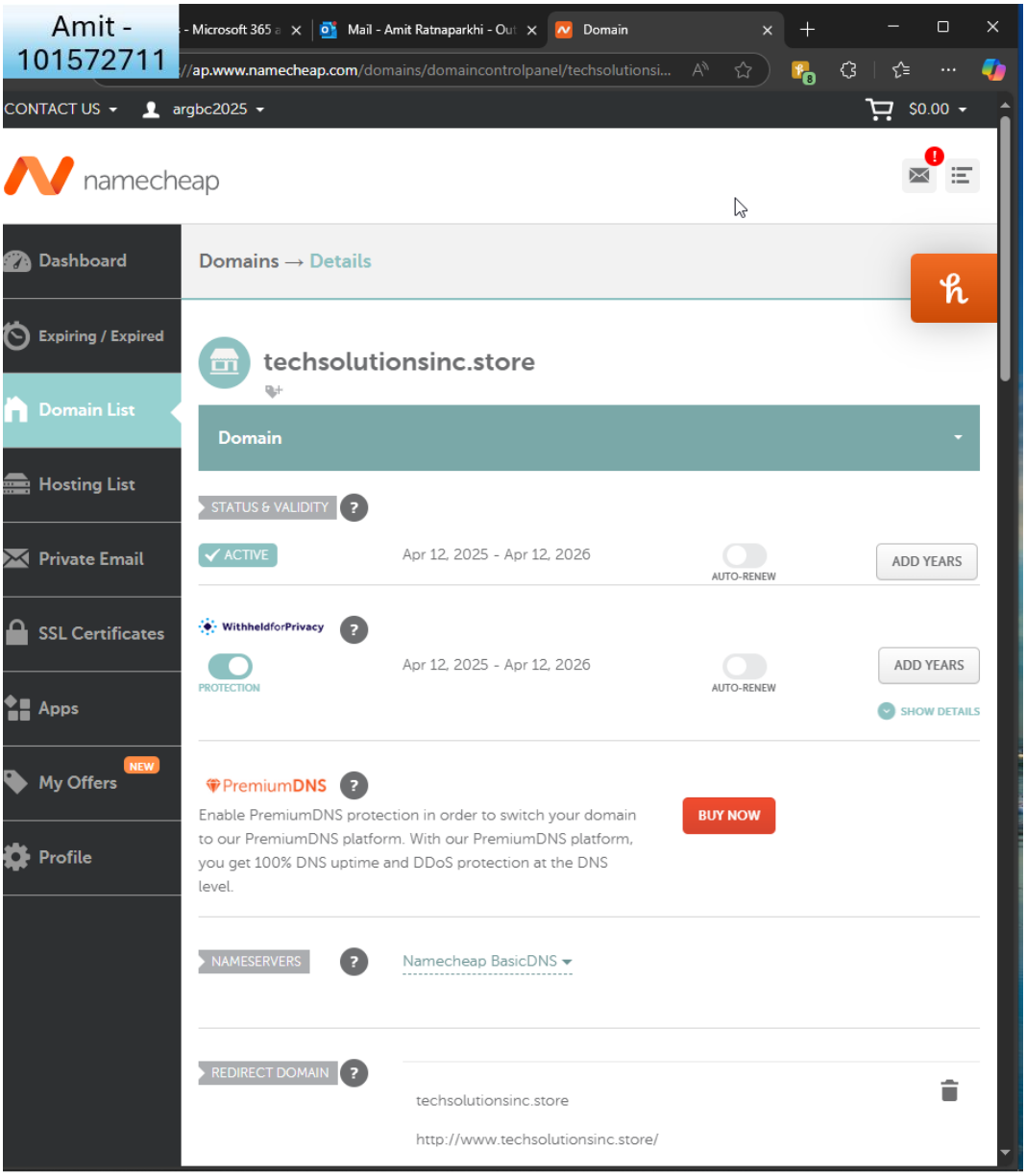
I choose to upload a CSV

Student Name: ……. Term: ……..
Student ID: ……..



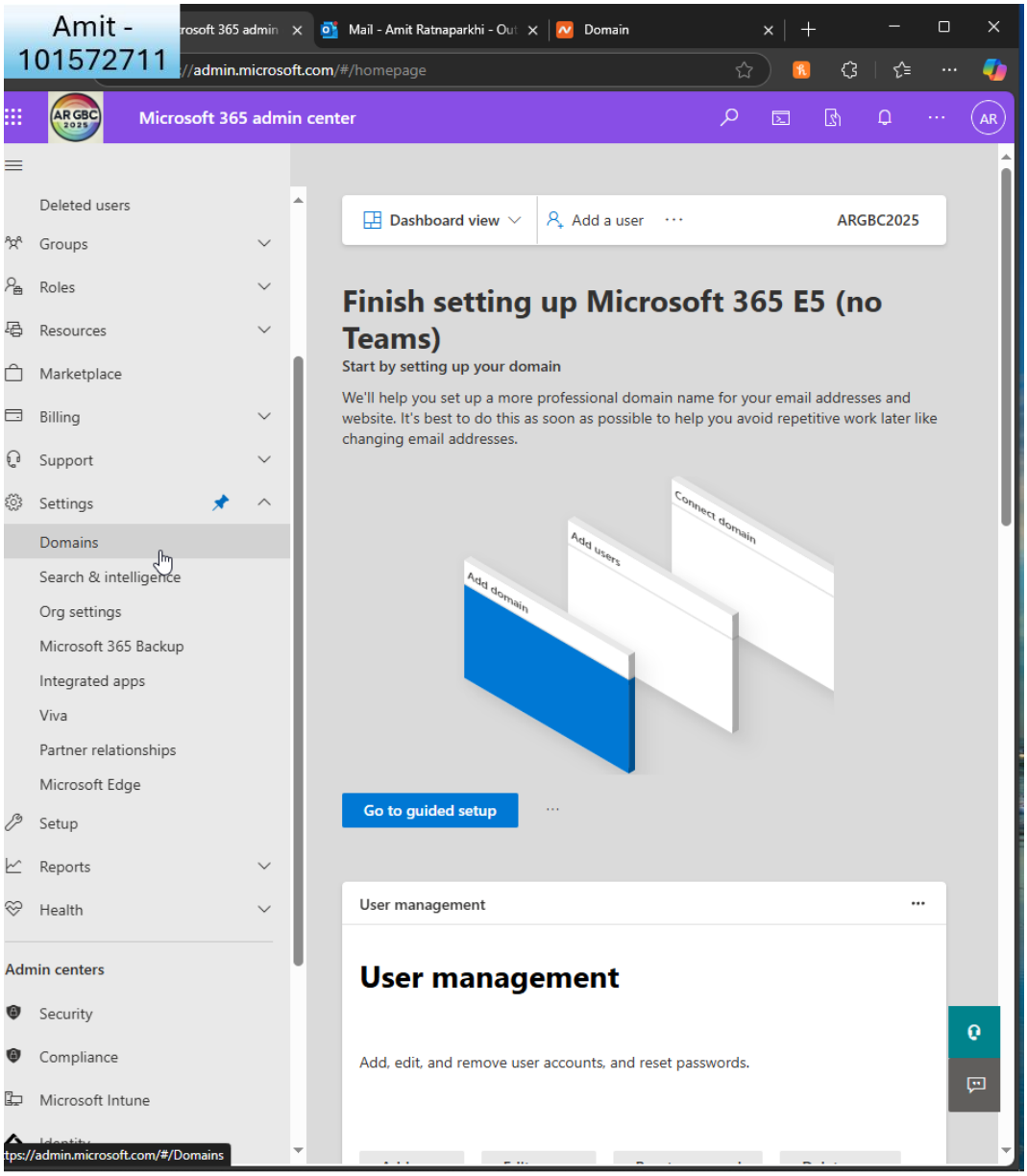
I download a blank CSV template

Student Name: ……. Term: ……..
Student ID: ……..



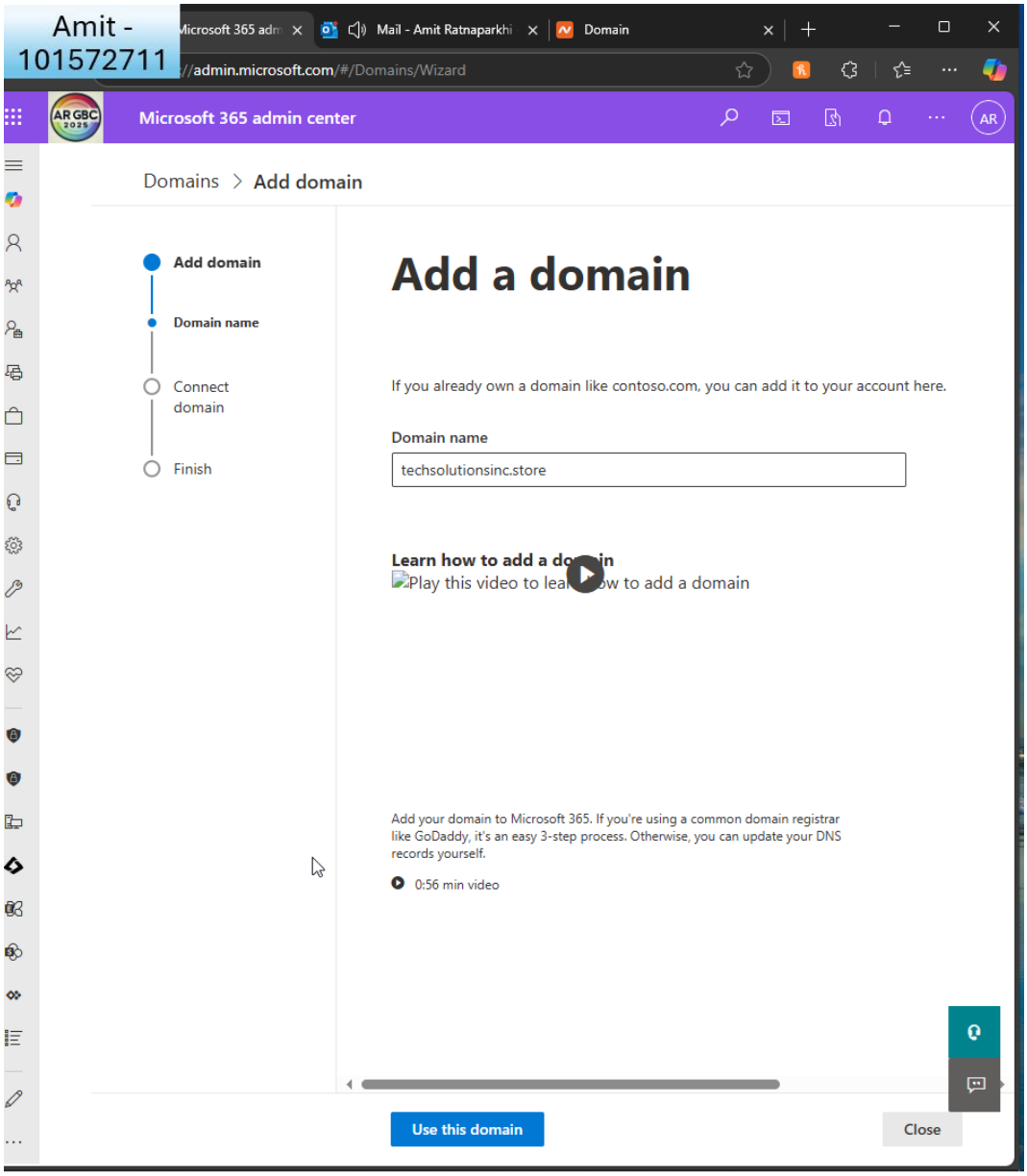
I wanted to reflect Techsolutions as a name, so I bought a domain called techsolutions.store from namecheap

Student Name: ……. Term: ……..
Student ID: ……..



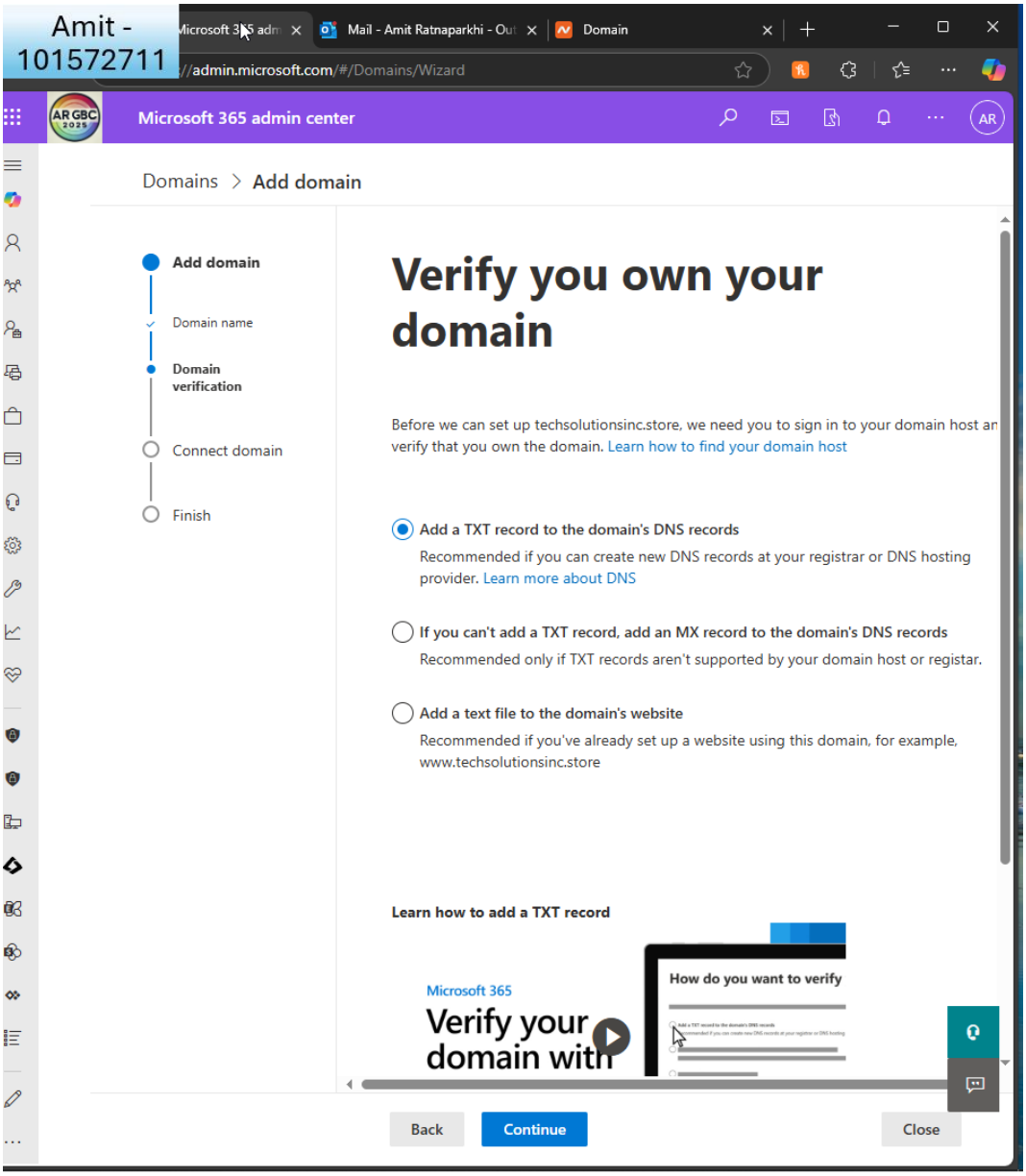
I connect the domain to MS365

Student Name: ……. Term: ……..
Student ID: ……..



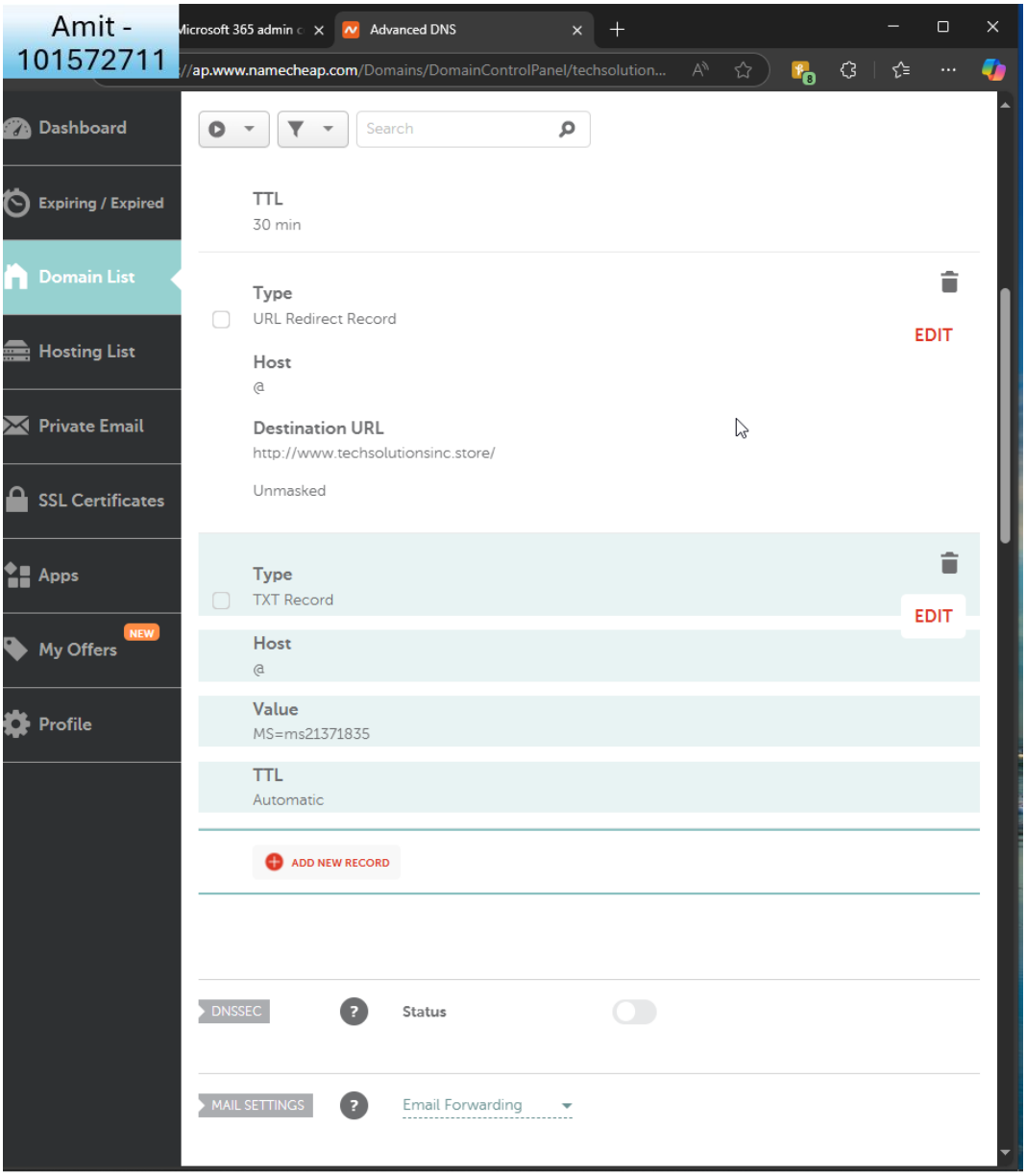
I add the domain

Student Name: ……. Term: ……..
Student ID: ……..

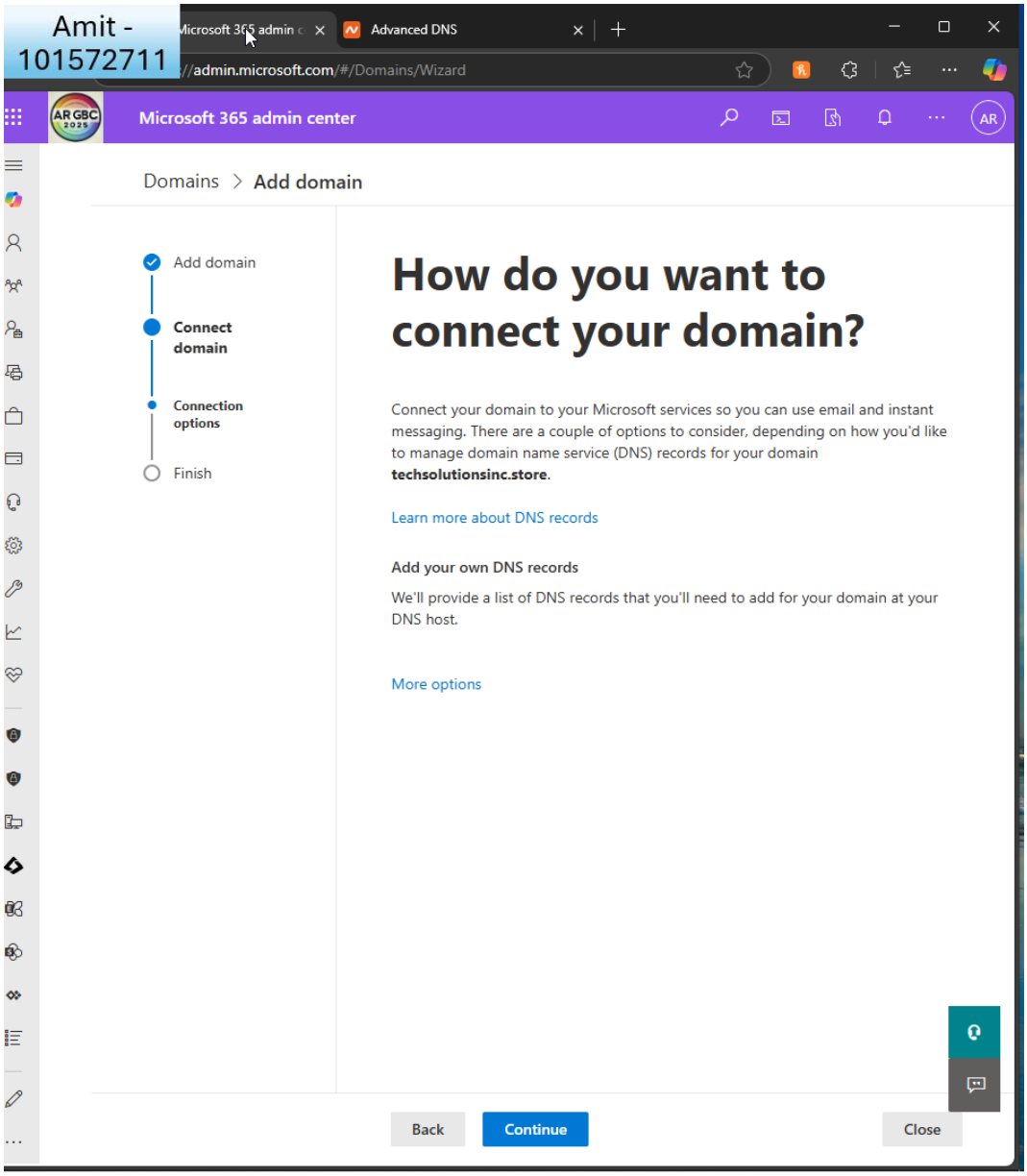


I add the TXT

Student Name: ……. Term: ……..
Student ID: ……..

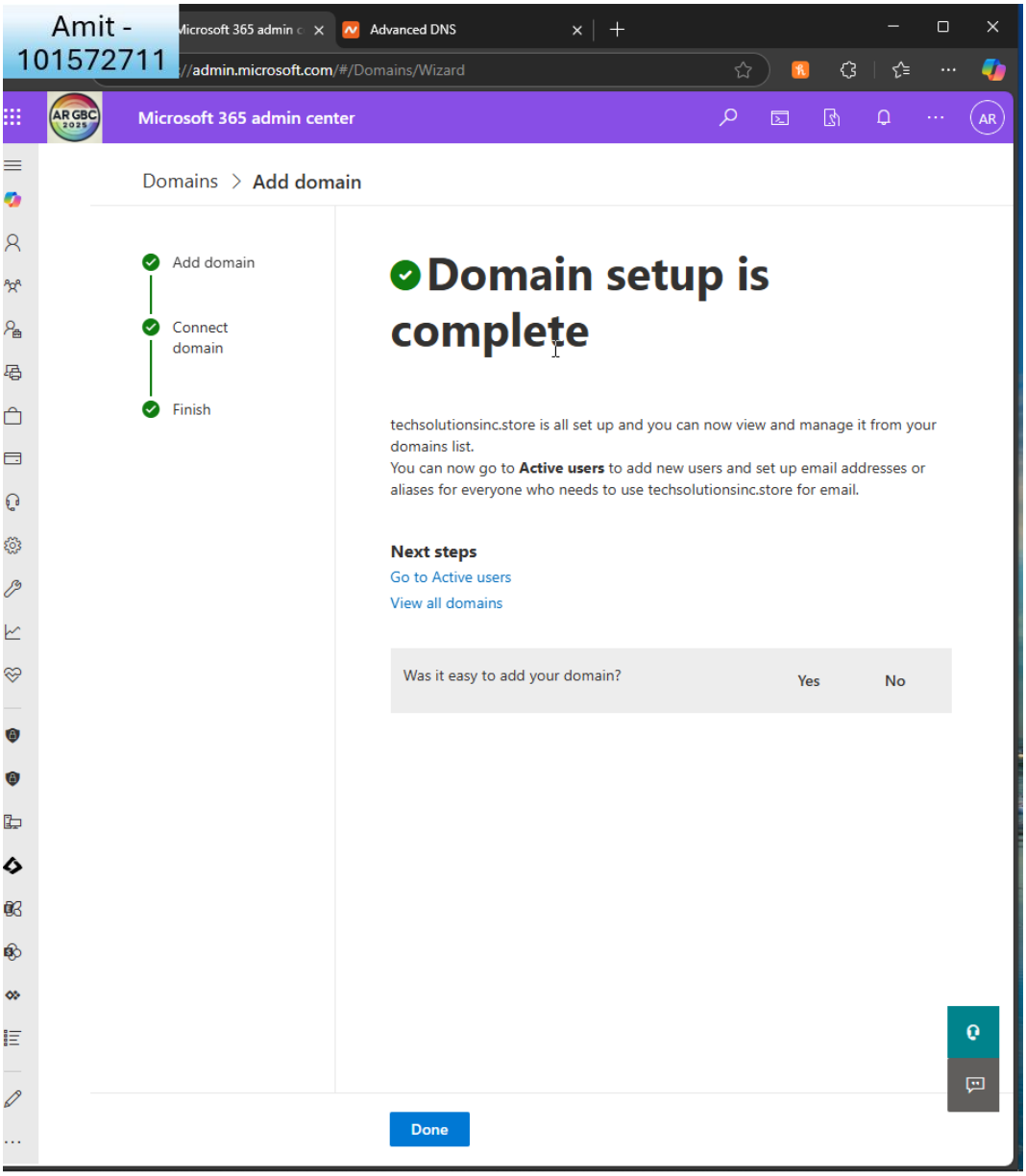


Student Name: ……. Term: ……..
Student ID: ……..



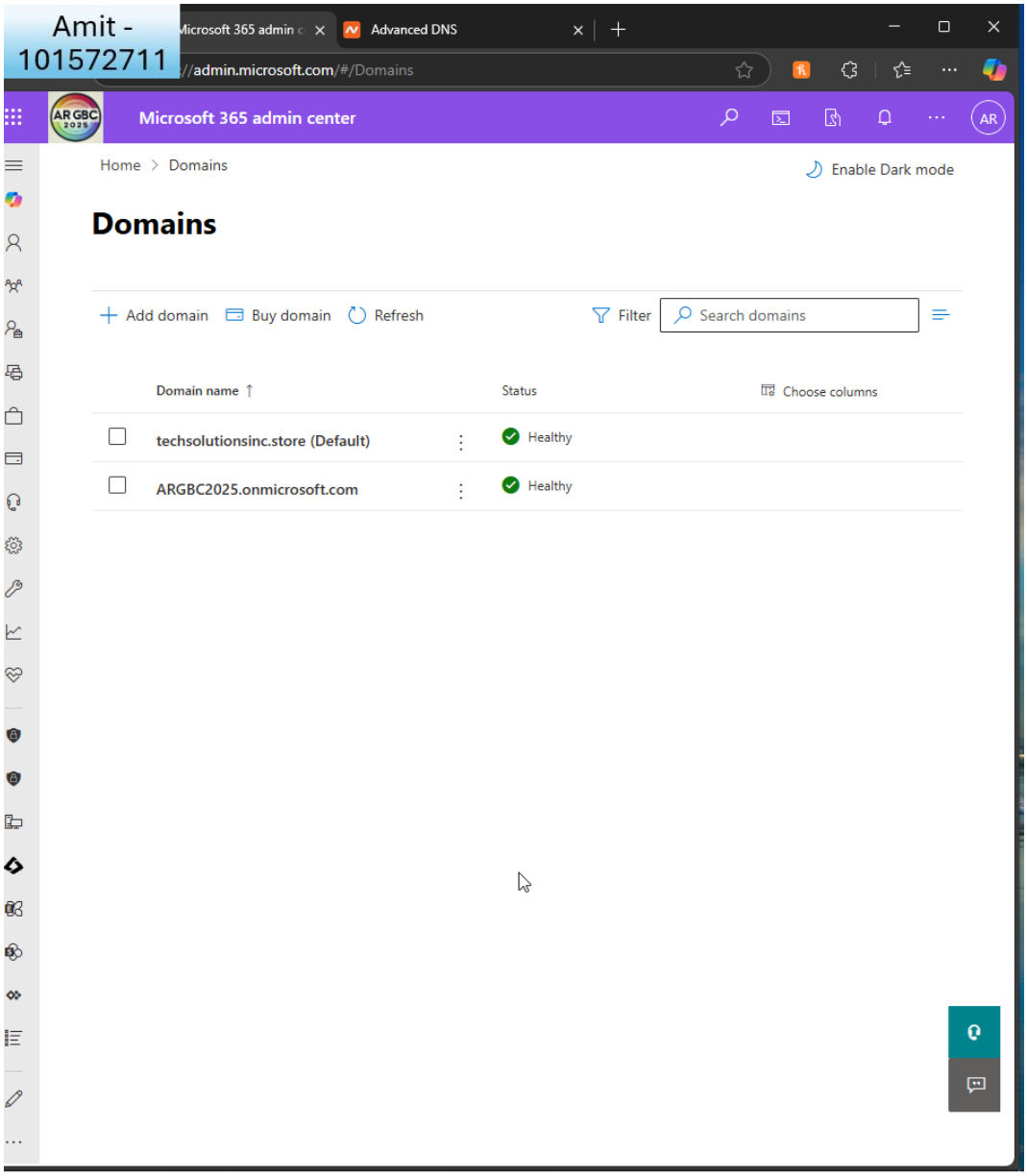
I go back to admin centre to connect the domain

Student Name: ……. Term: ……..
Student ID: ……..



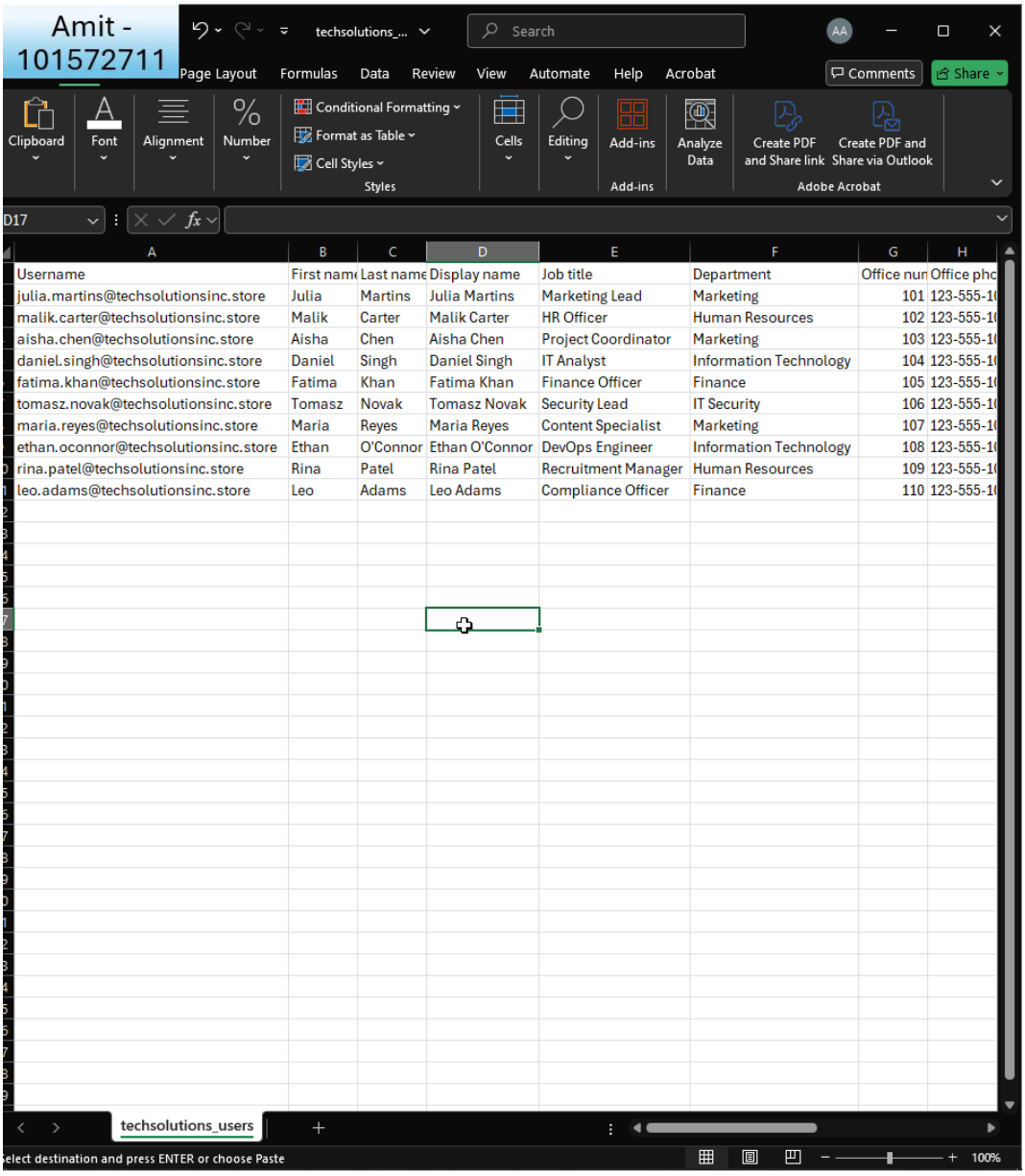
I also made sure the MX and TXT records are correct

Student Name: ……. Term: ……..
Student ID: ……..



I can see my domain now and it's default

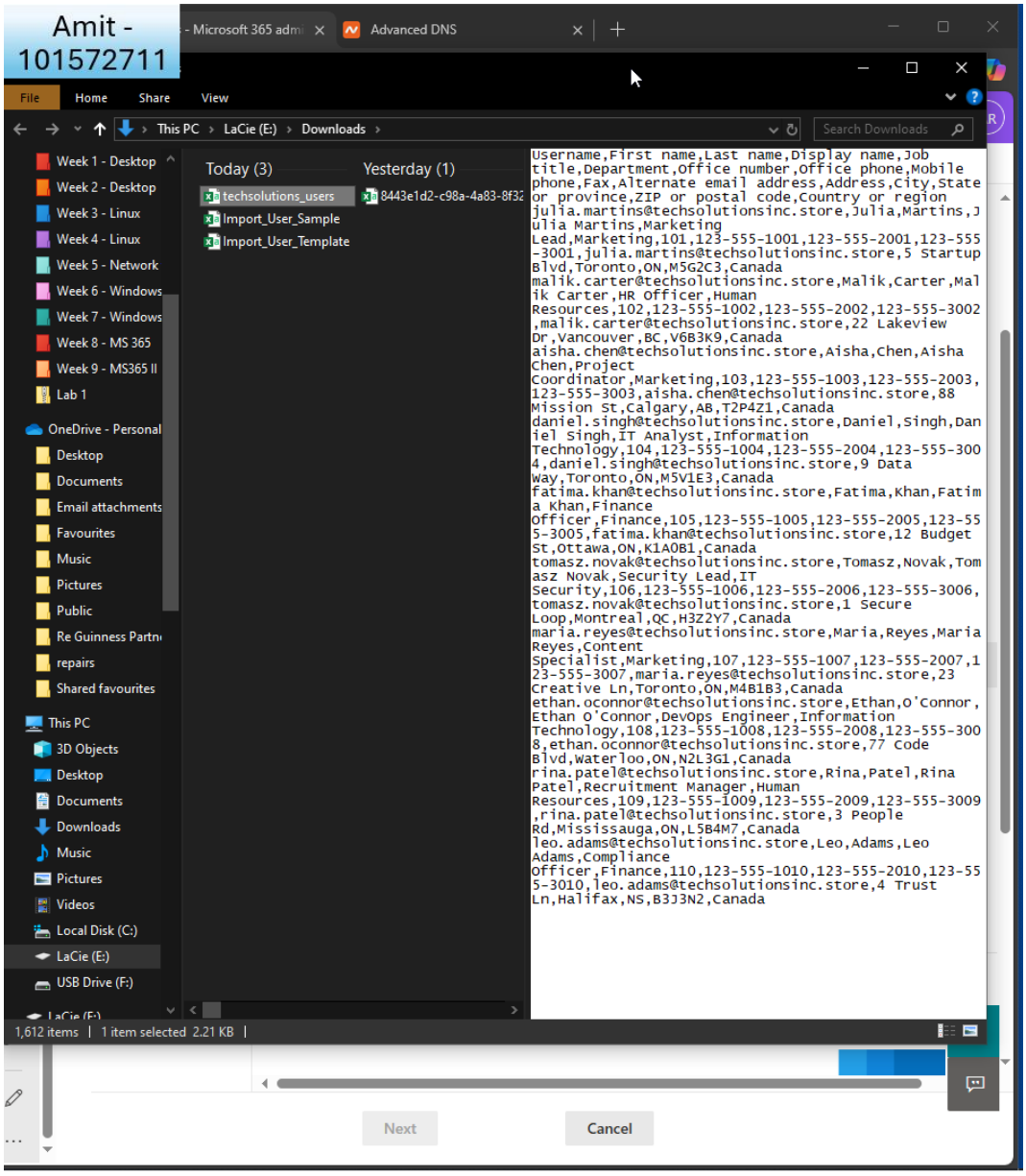
Student Name: ……. Term: ……..
Student ID: ……..



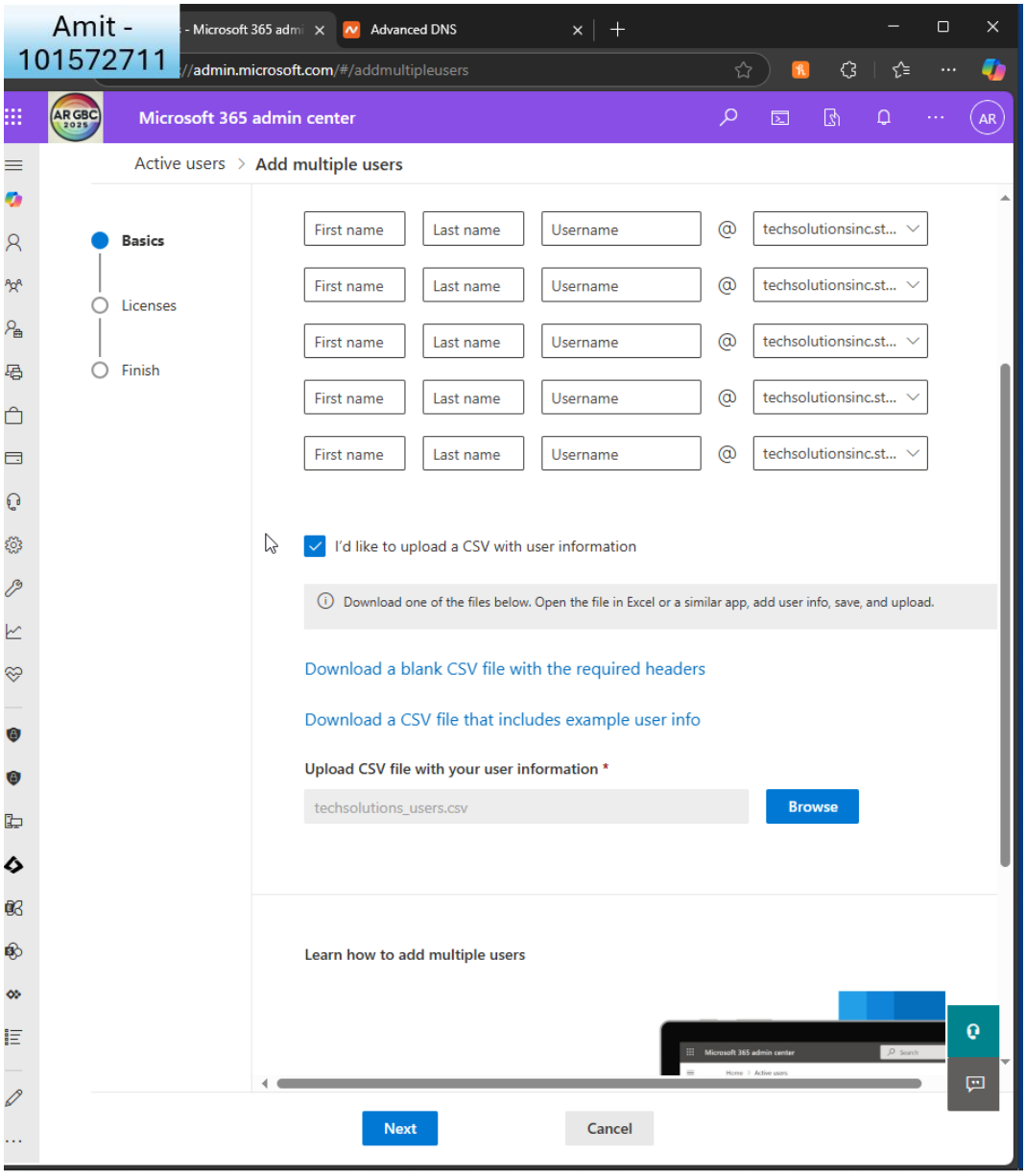
Username	First name	Last name	Display name	Job title	Department	Office nun	Office phc
julia.martins@techsolutionsinc.store	Julia	Martins	Julia Martins	Marketing Lead	Marketing	101	123-555-1(
malik.carter@techsolutionsinc.store	Malik	Carter	Malik Carter	HR Officer	Human Resources	102	123-555-1(
aisha.chen@techsolutionsinc.store	Aisha	Chen	Aisha Chen	Project Coordinator	Marketing	103	123-555-1(
daniel.singh@techsolutionsinc.store	Daniel	Singh	Daniel Singh	IT Analyst	Information Technology	104	123-555-1(
fatima.khan@techsolutionsinc.store	Fatima	Khan	Fatima Khan	Finance Officer	Finance	105	123-555-1(
tomasz.novak@techsolutionsinc.store	Tomasz	Novak	Tomasz Novak	Security Lead	IT Security	106	123-555-1(
maria.reyes@techsolutionsinc.store	Maria	Reyes	Maria Reyes	Content Specialist	Marketing	107	123-555-1(
ethan.oconnor@techsolutionsinc.store	Ethan	O'Connor	Ethan O'Connor	DevOps Engineer	Information Technology	108	123-555-1(
rina.patel@techsolutionsinc.store	Rina	Patel	Rina Patel	Recruitment Manager	Human Resources	109	123-555-1(
leo.adams@techsolutionsinc.store	Leo	Adams	Leo Adams	Compliance Officer	Finance	110	123-555-1(

I used chatGPT to fill the CSV file with information

Student Name: ……. Term: ……..
Student ID: ……..



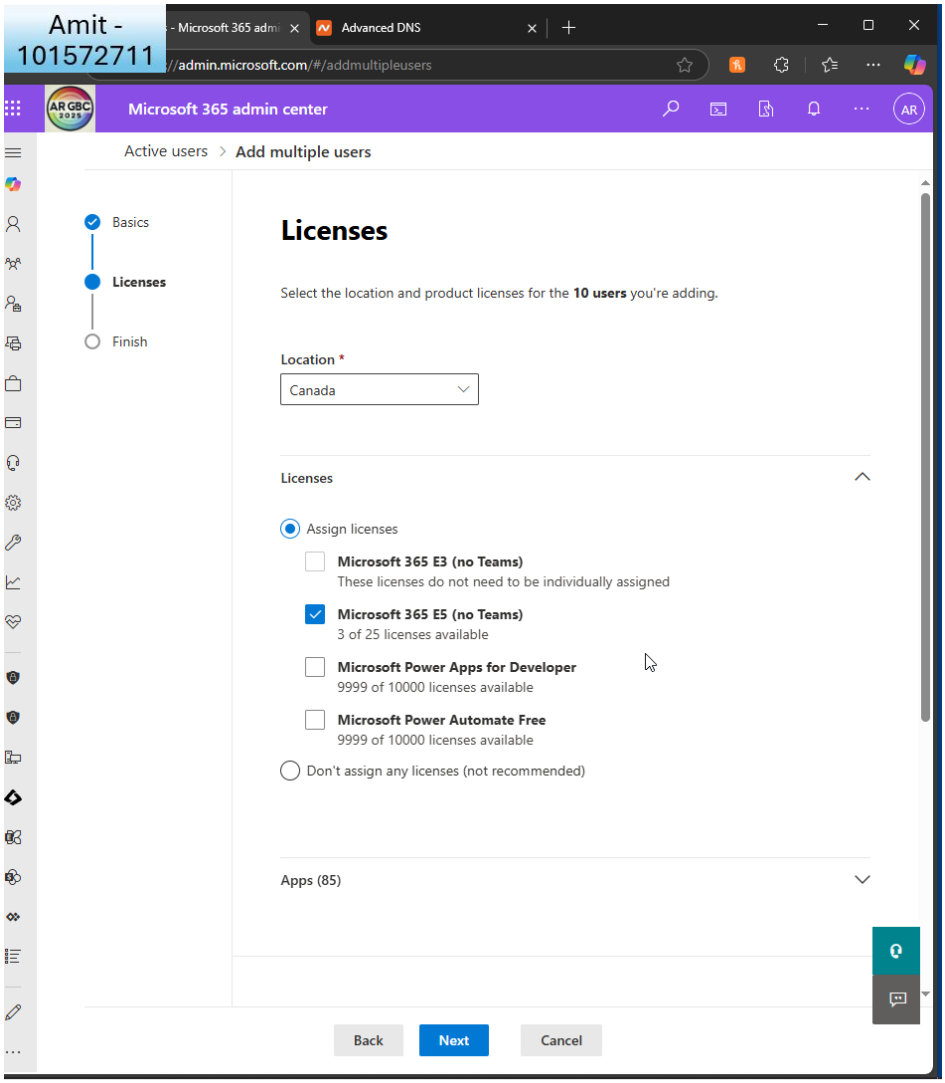
Student Name: ……. Term: ……..
Student ID: ……..



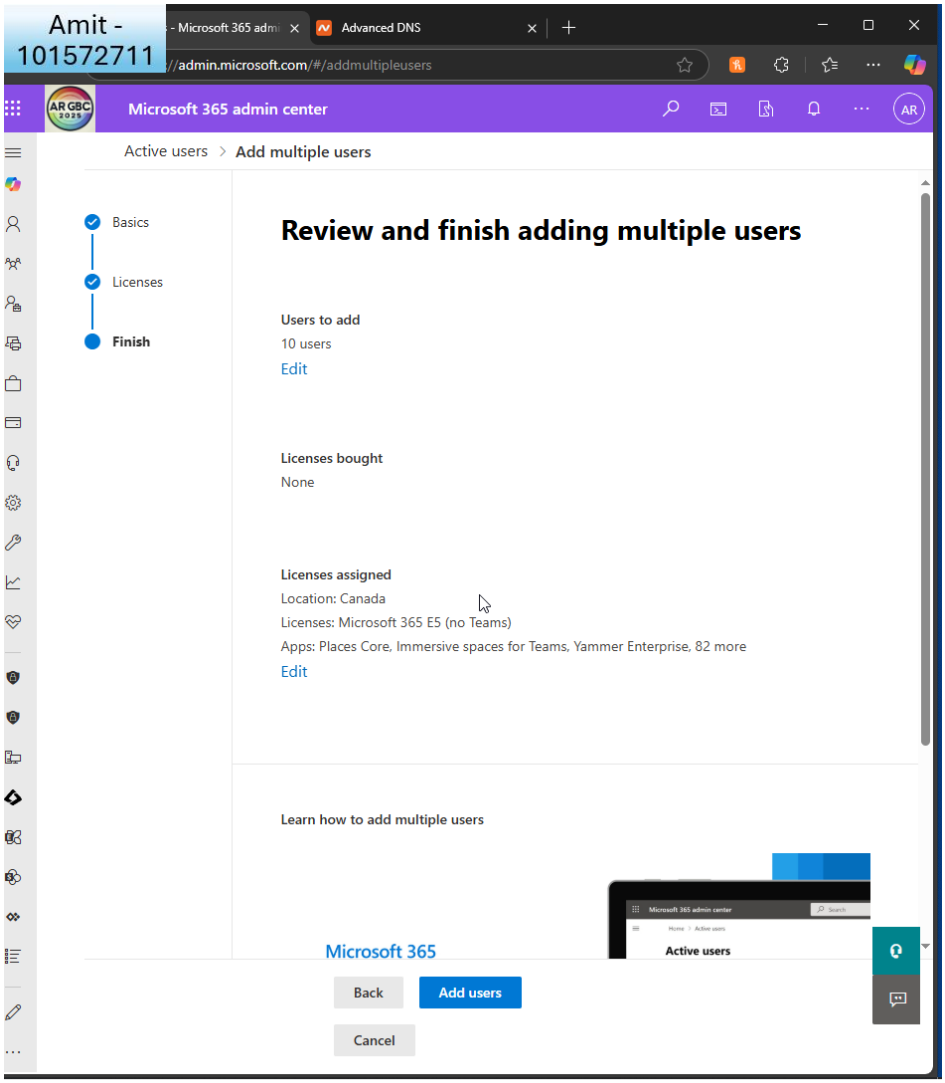
I upload the file

- Assign appropriate licenses (Microsoft 365 E3 or E5) to the imported users.

Student Name: ……. Term: ……..
Student ID: ……..

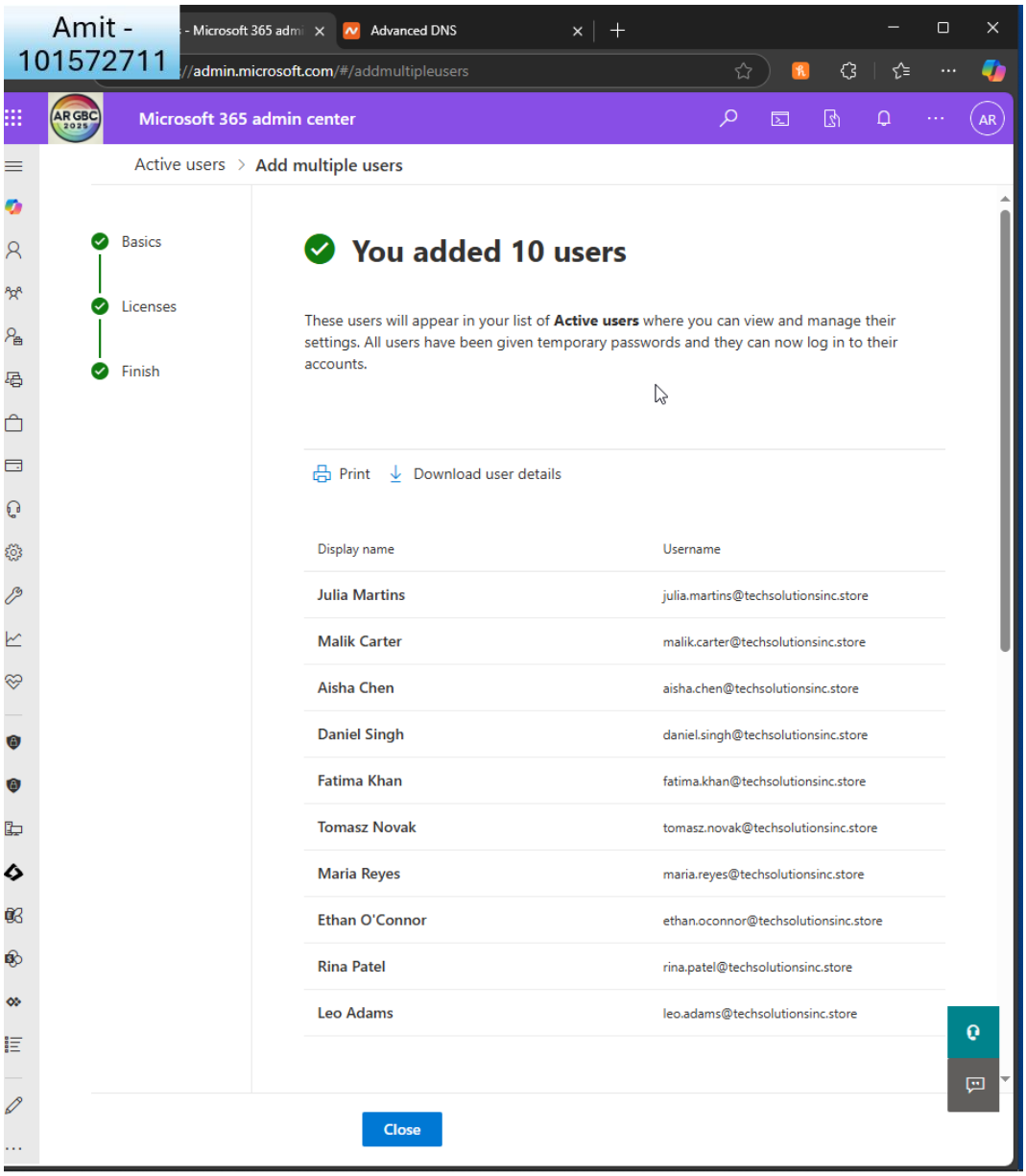


Student Name: ……. Term: ……..
Student ID: ……..



Student Name: ……. Term: ……..
Student ID: ……..

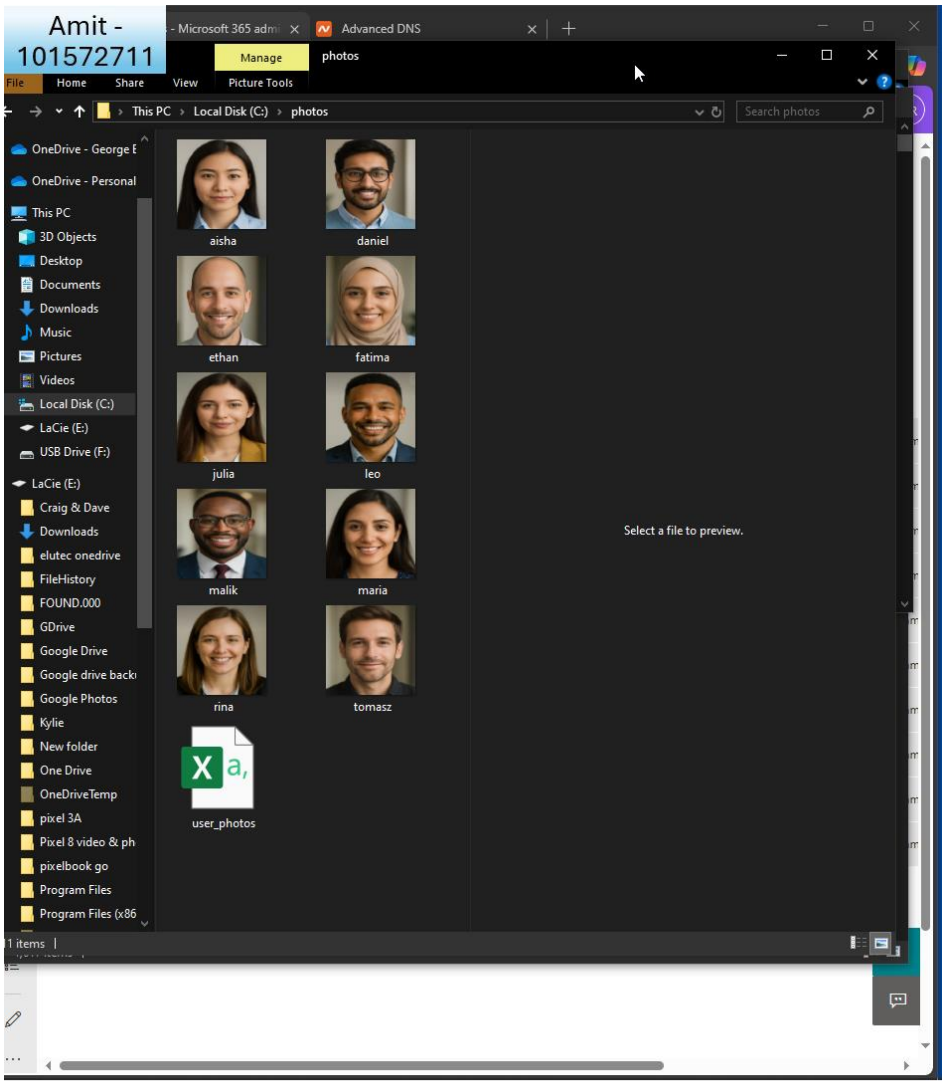
I review and finish adding multiple users



2. **Configure User Profiles**:

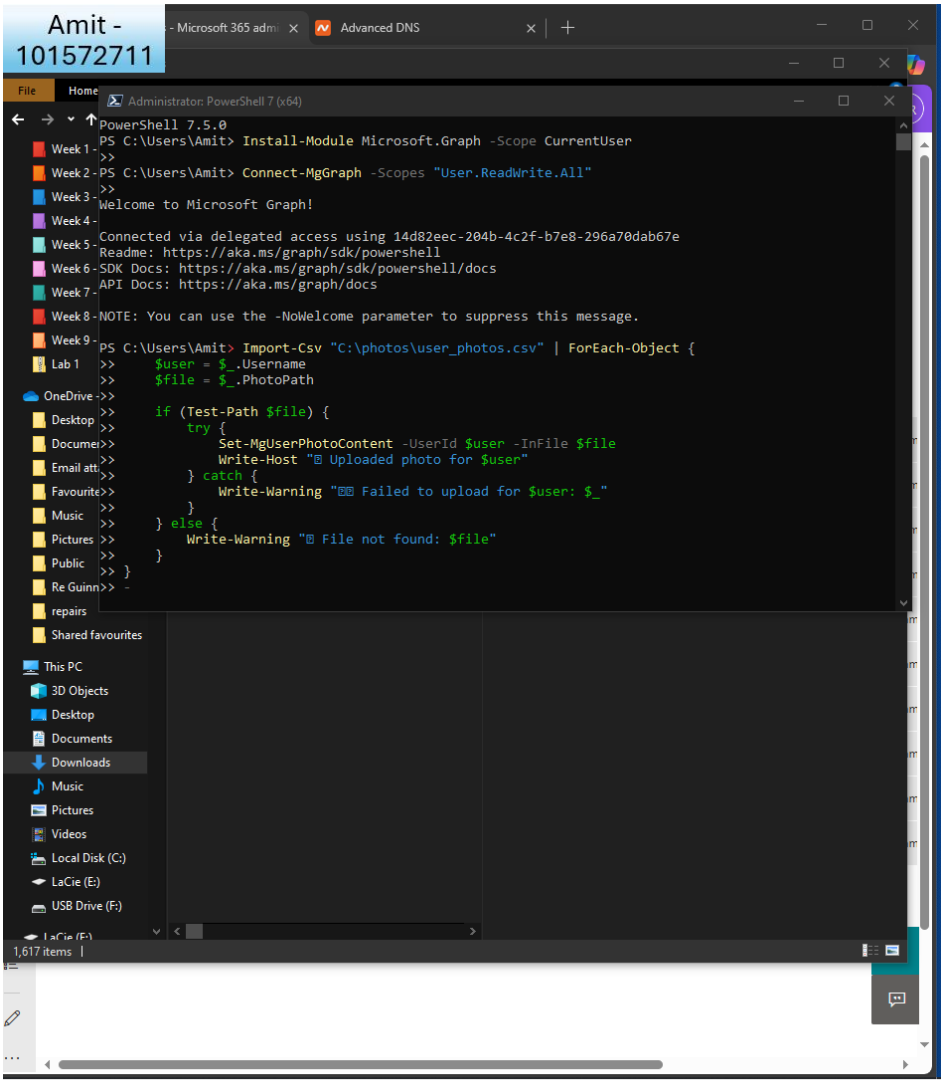
Student Name: ……. Term: ……..
Student ID: ……..

- Ensure each user has a profile picture, contact information, and job title set.



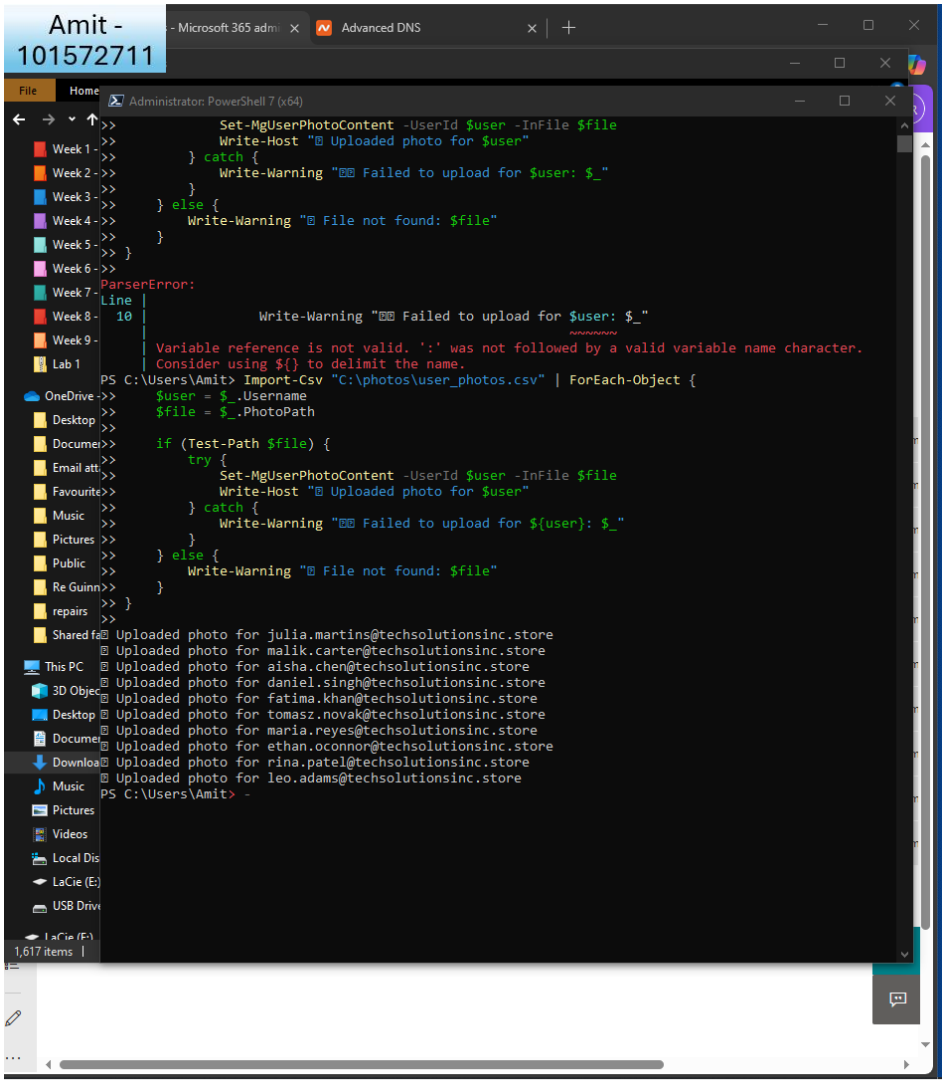
I used chatgpt to create 10 photos and ensure they are all square, all PNG and all same pixels so MS365 can import them via powershell

Student Name: ……. Term: ……..
Student ID: ……..

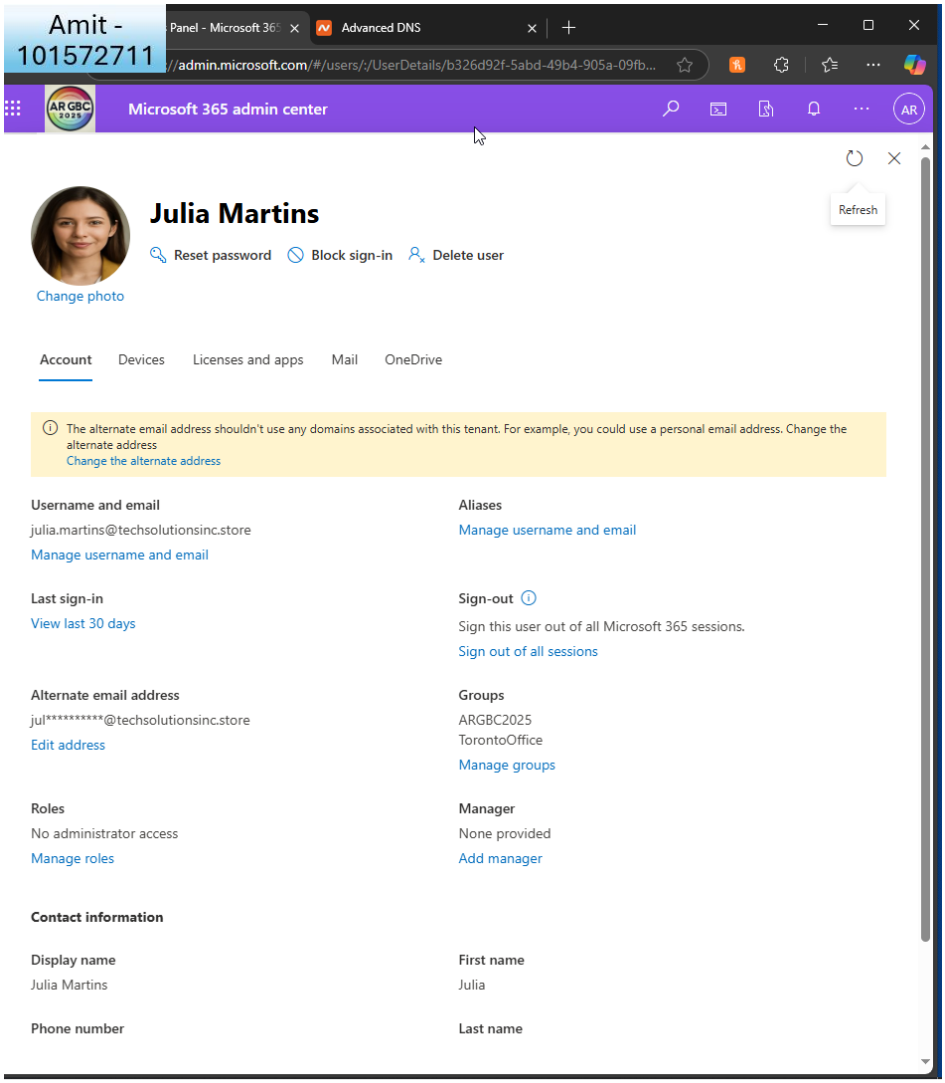


I use this script to set the photo in the profile

Student Name: ……. Term: ……..
Student ID: ……..



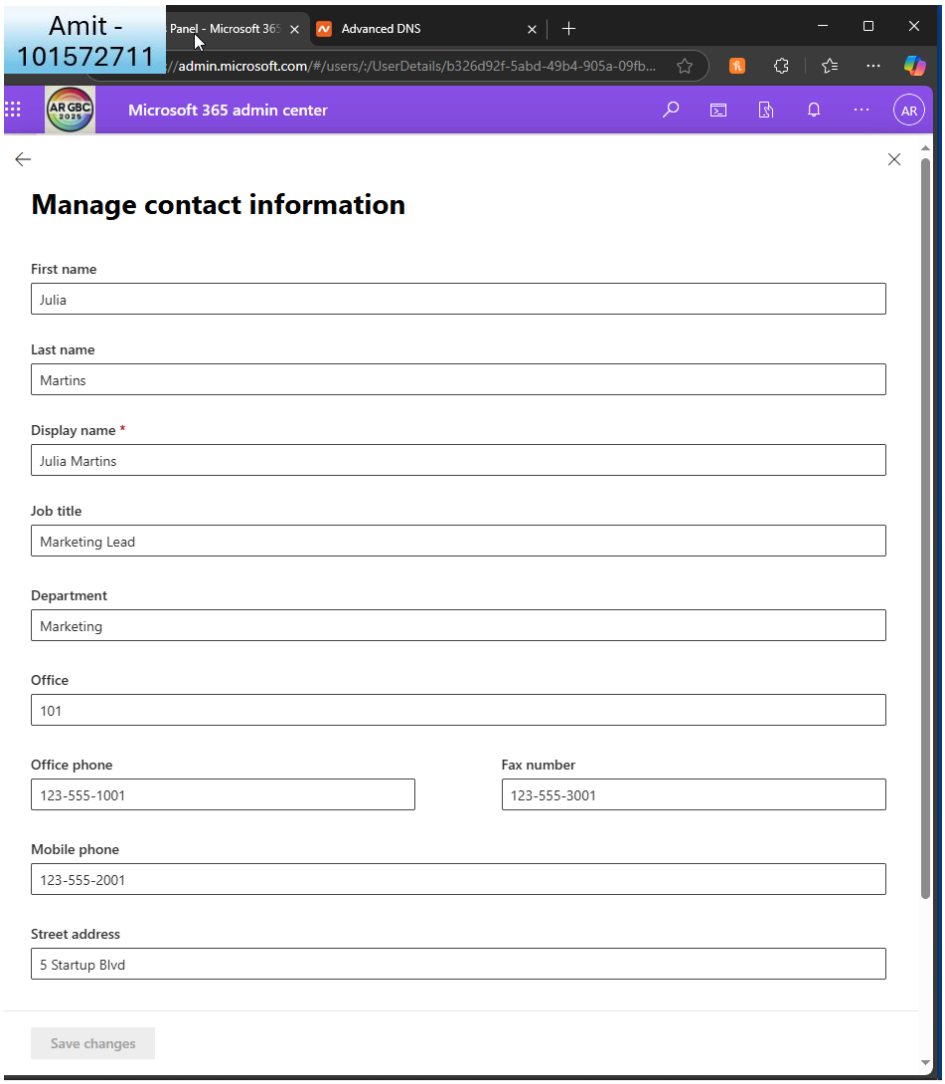
Student Name: ……. Term: ……..
Student ID: ……..



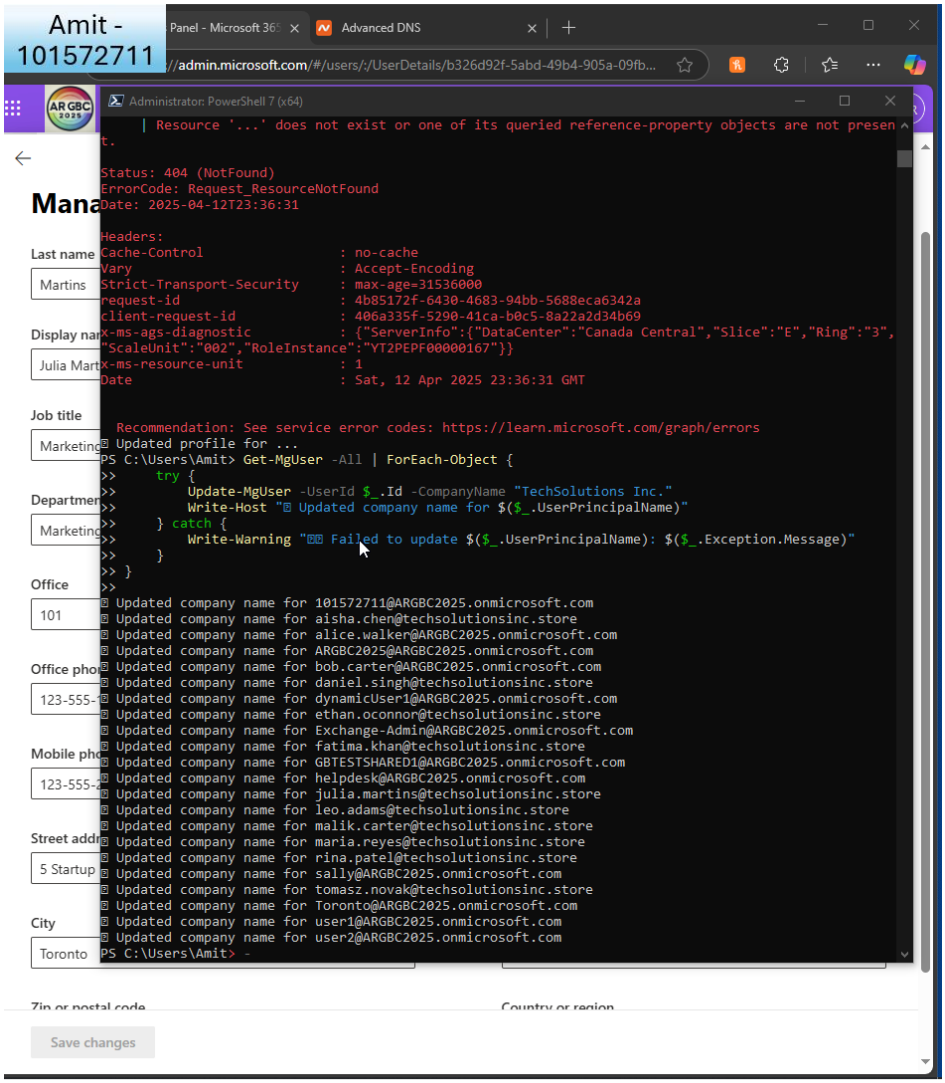
Here’s the confirmation

Student Name: ……. Term: ……..
Student ID: ……..

- Configure user settings to include organization-specific information.



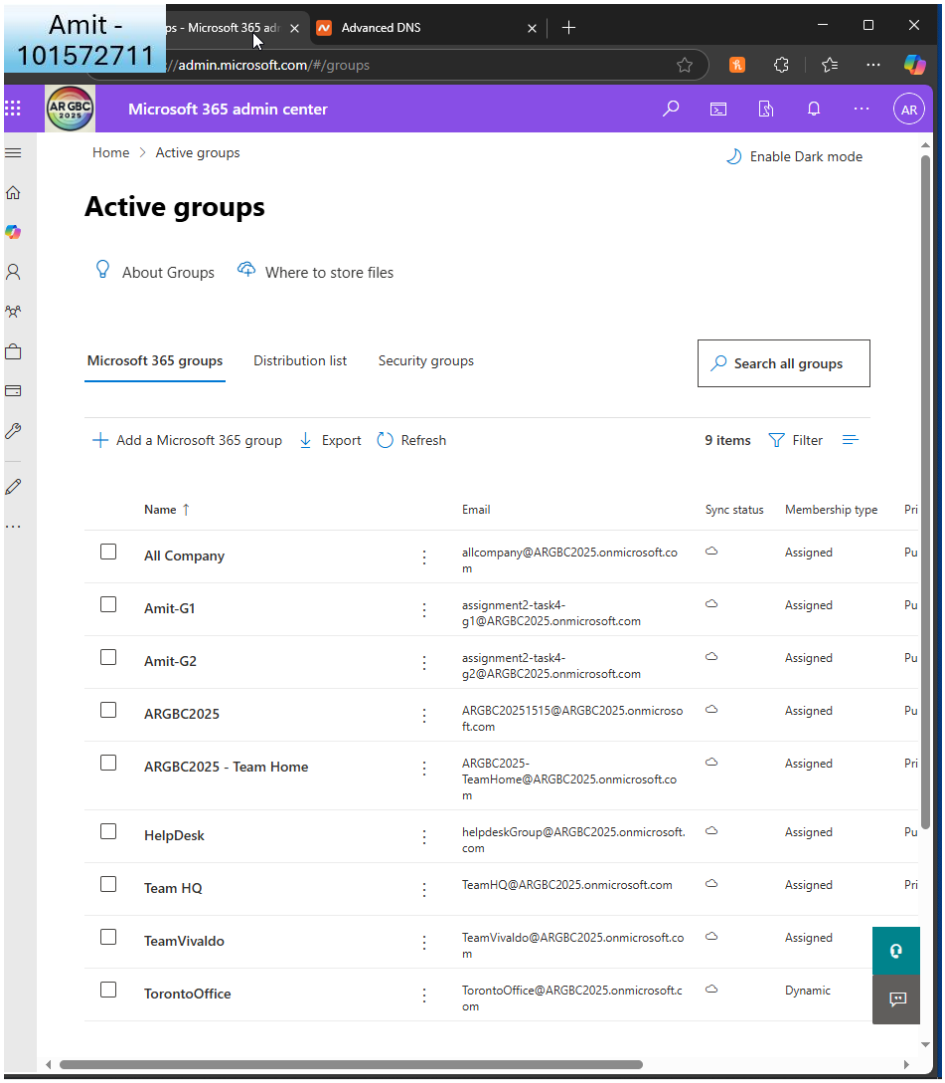
Student Name: ……. Term: ……..
Student ID: ……..



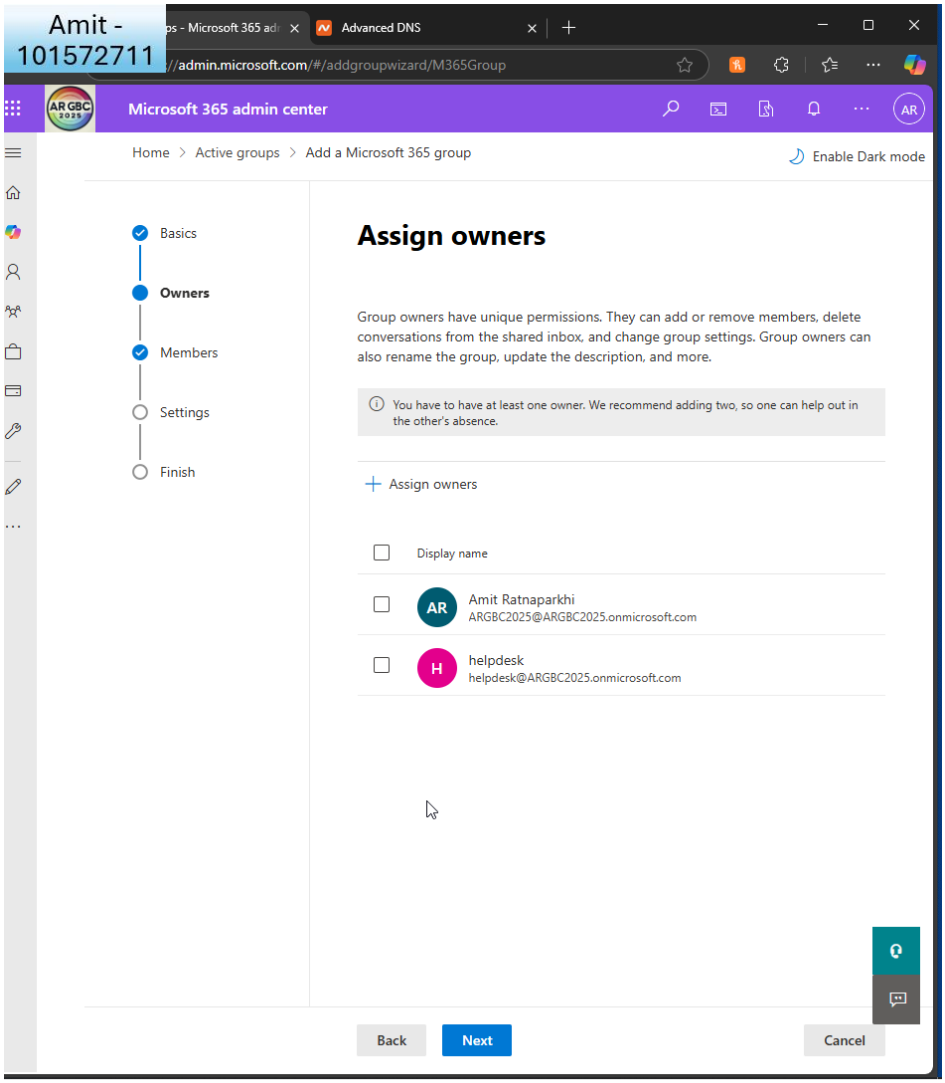
I also used powershell to update the company name

3. **Create Office 365 Groups**:
    - Create three Office 365 groups for different departments: IT, HR, and Marketing.

Student Name: ……. Term: ……..
Student ID: ……..



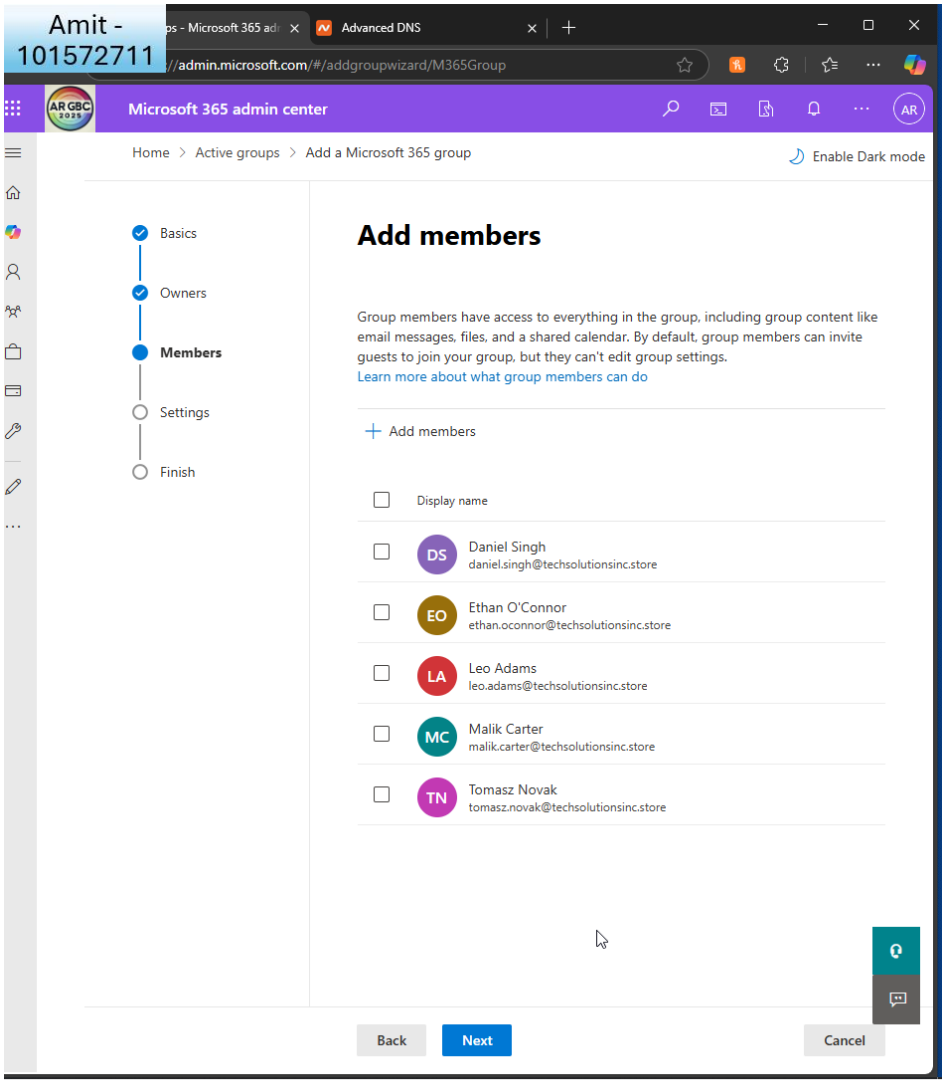
Student Name: ……. Term: ……..
Student ID: ……..



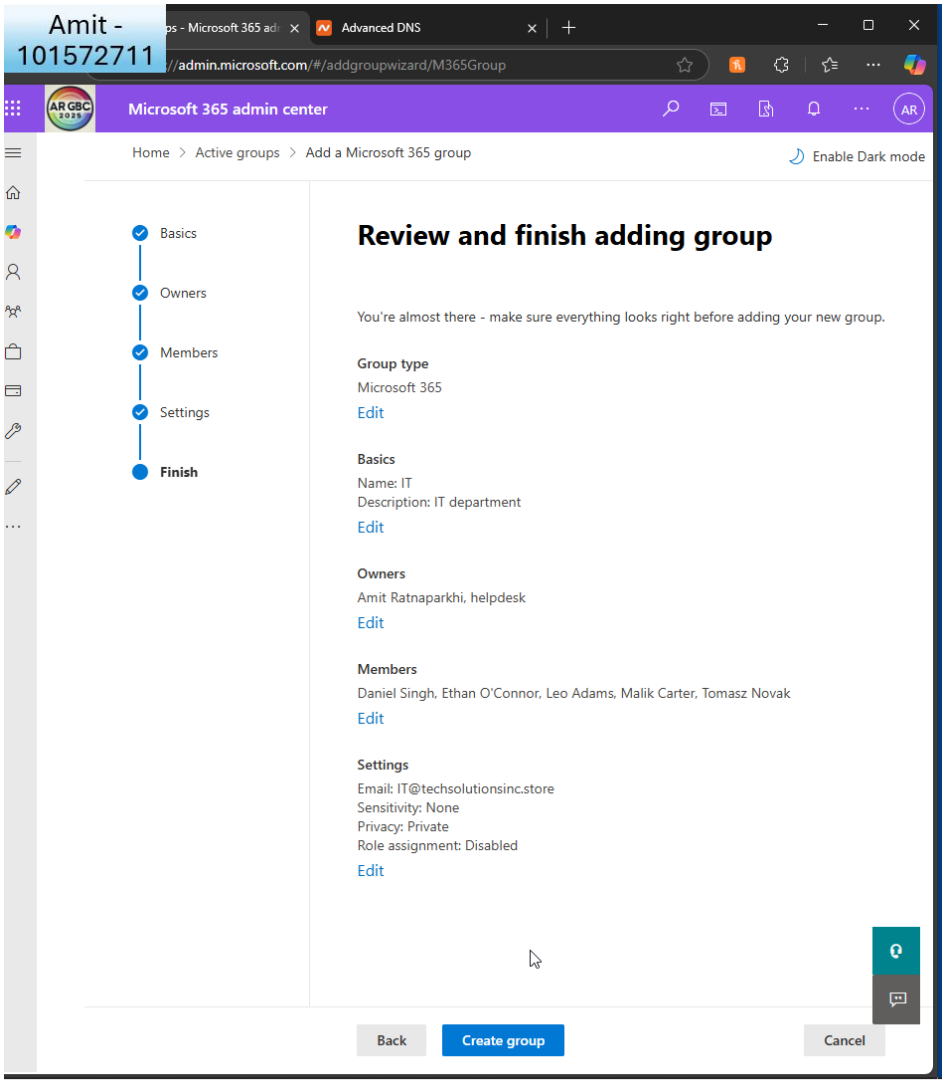
I add 2 owners per group (GA and helpdesk)

- Add users to their respective groups.

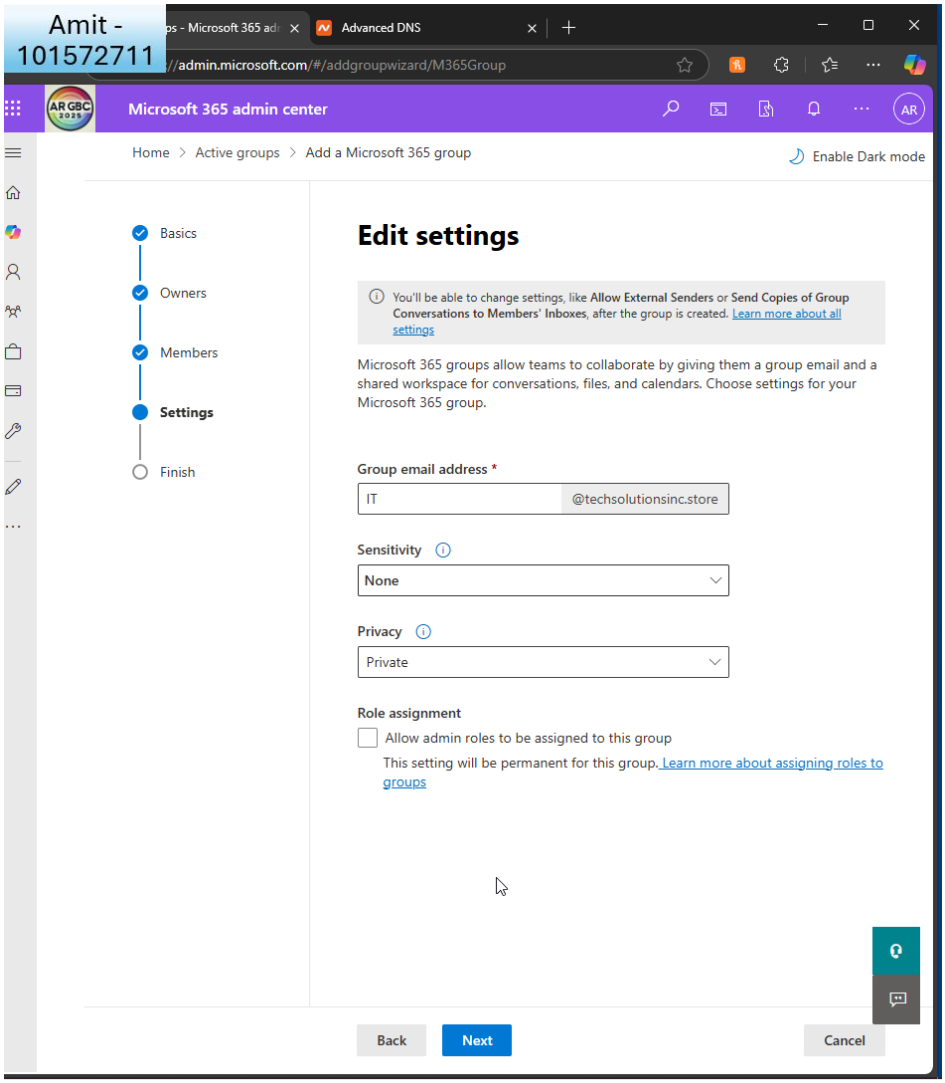
Student Name: ……. Term: ……..
Student ID: ……..



Student Name: ……. Term: ……..
Student ID: ……..

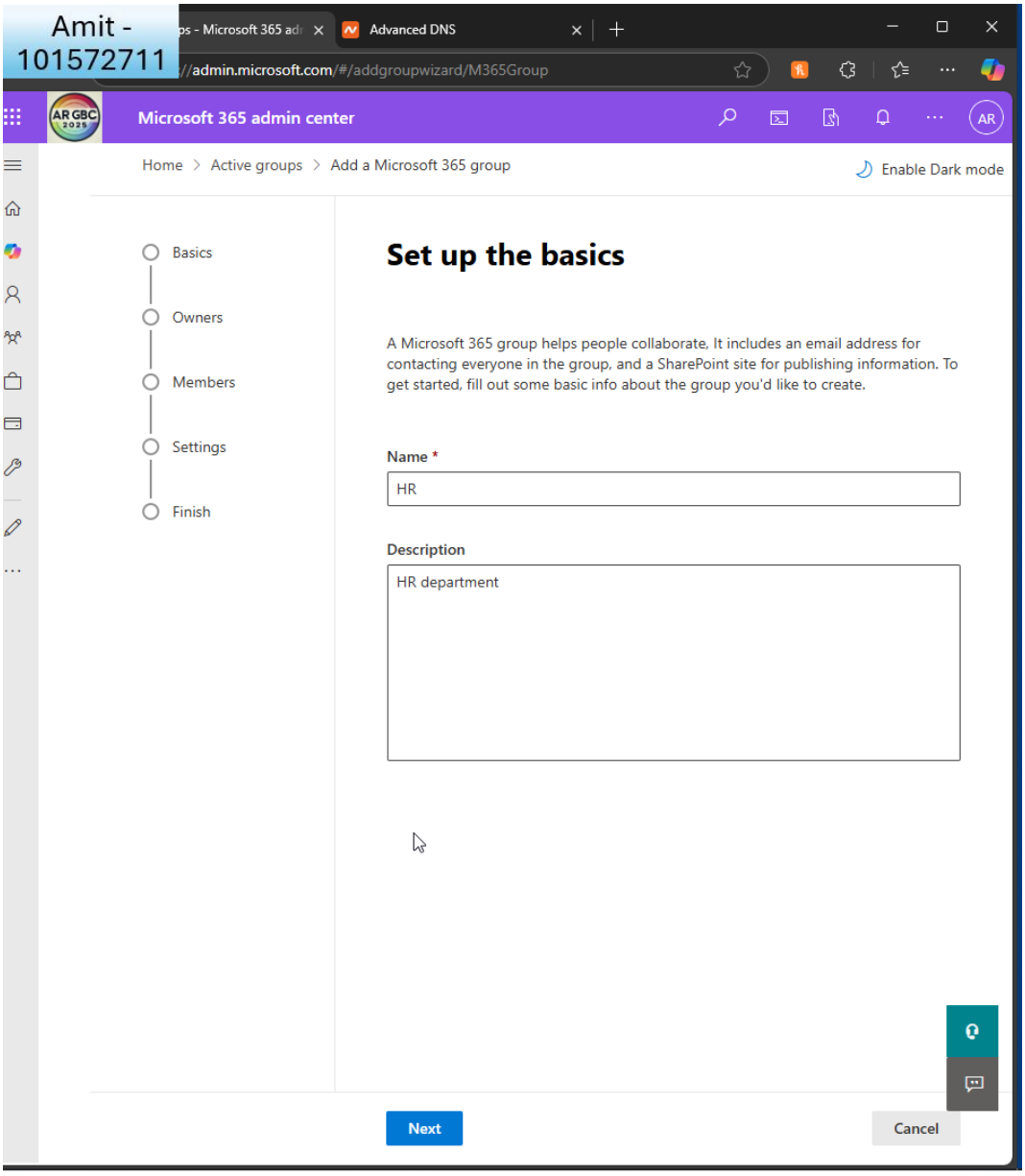


Student Name: ……. Term: ……..
Student ID: ……..

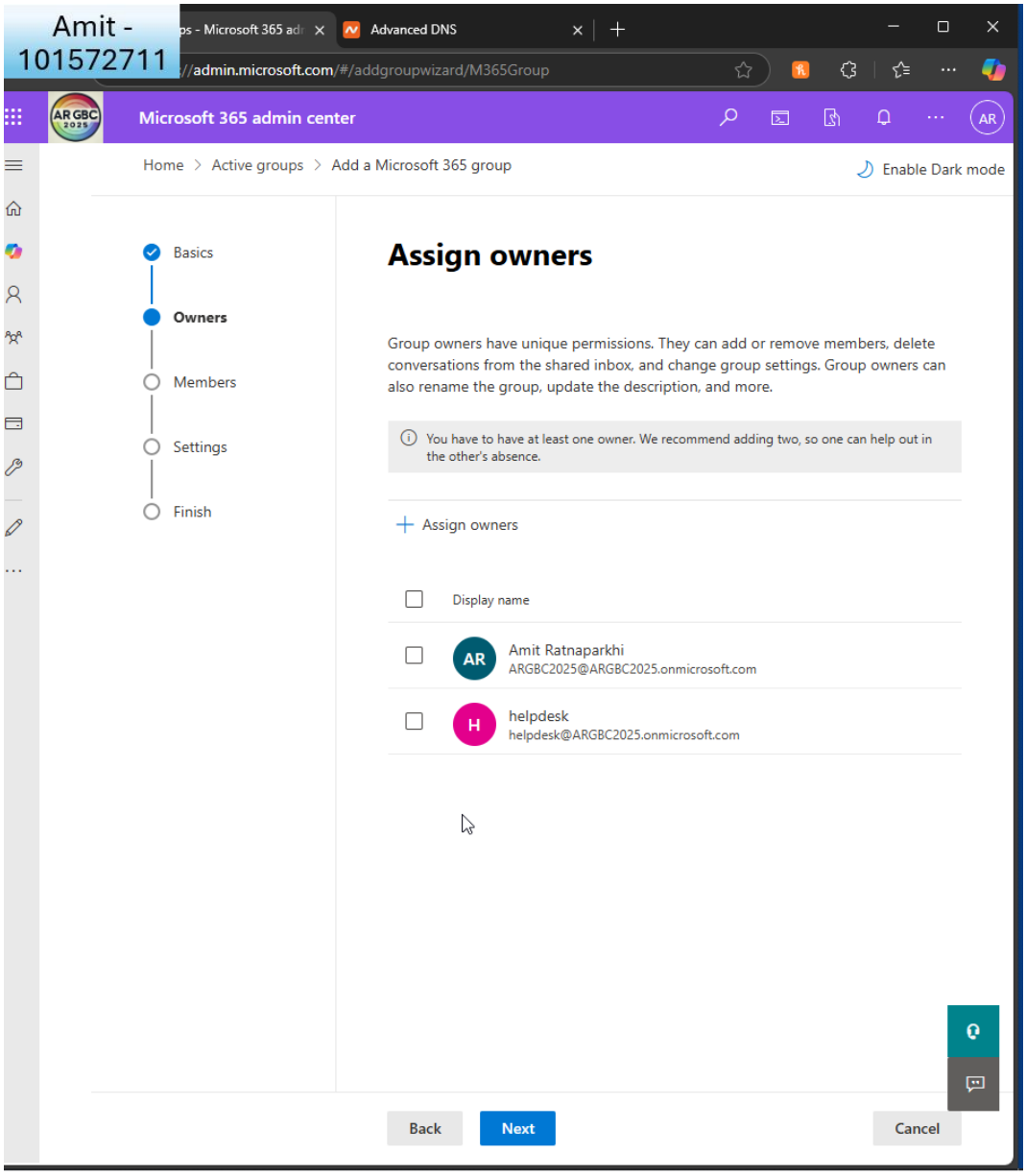


This is the IT department

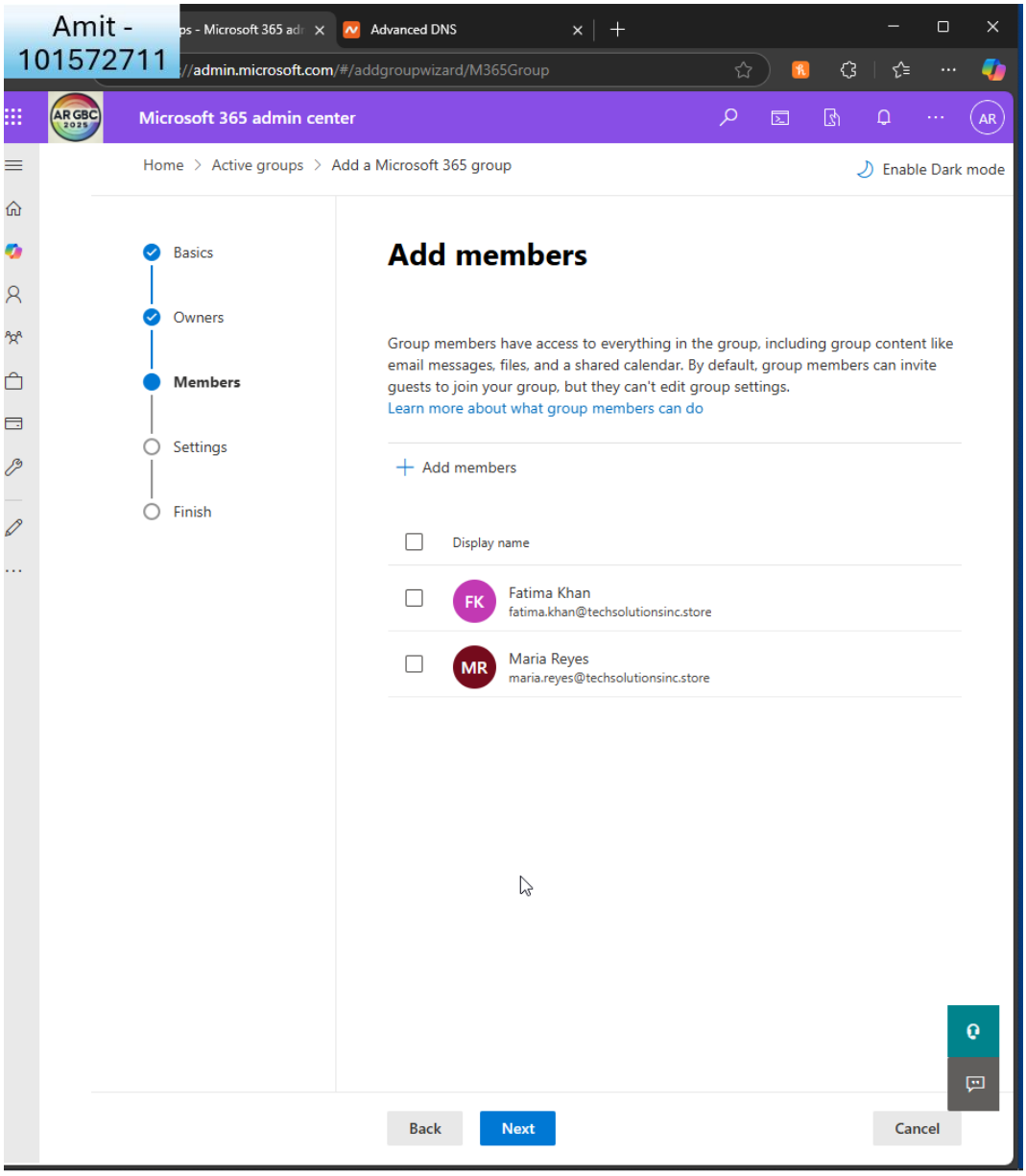
Student Name: ……. Term: ……..
Student ID: ……..



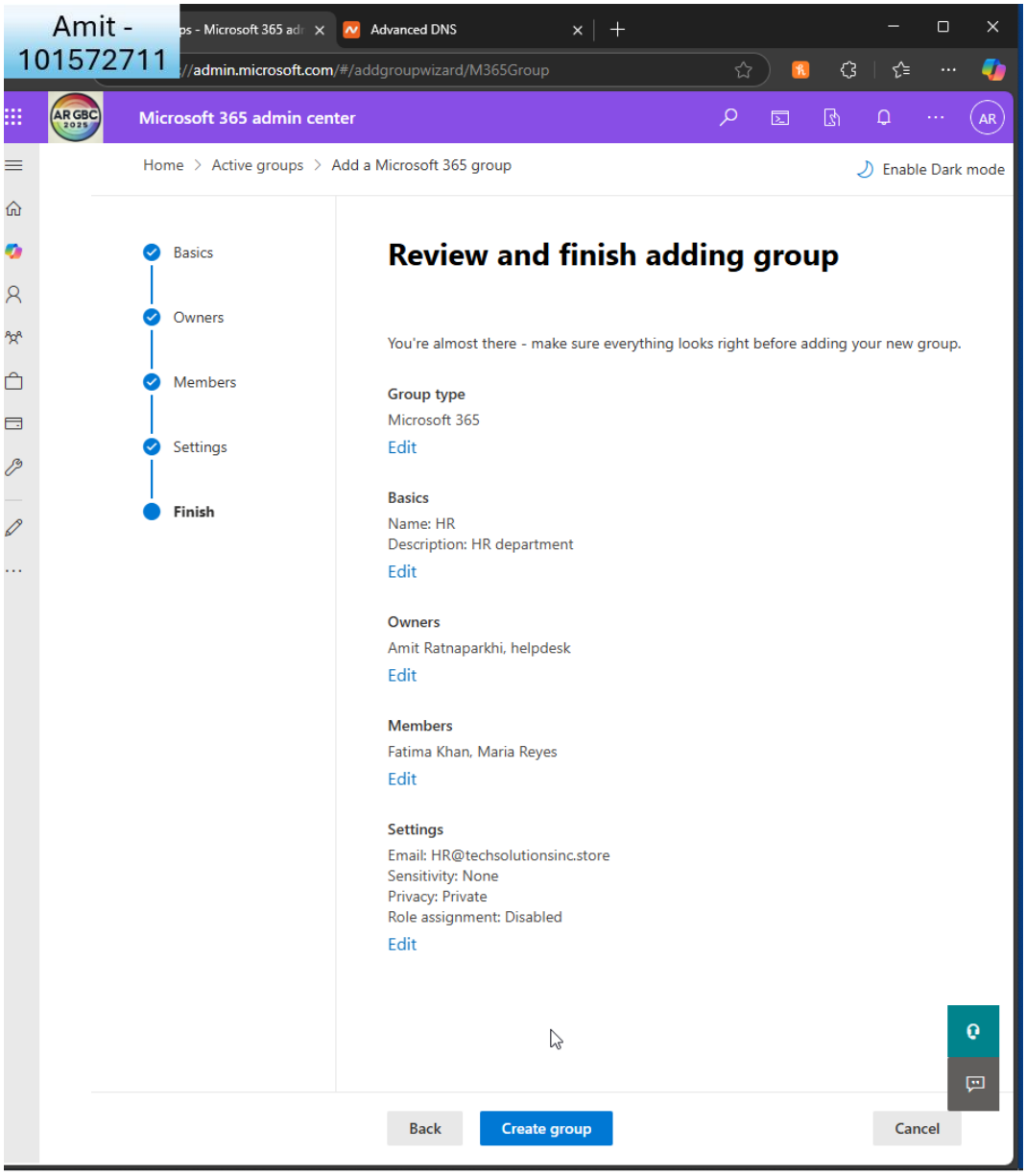
Student Name: ……. Term: ……..
Student ID: ……..



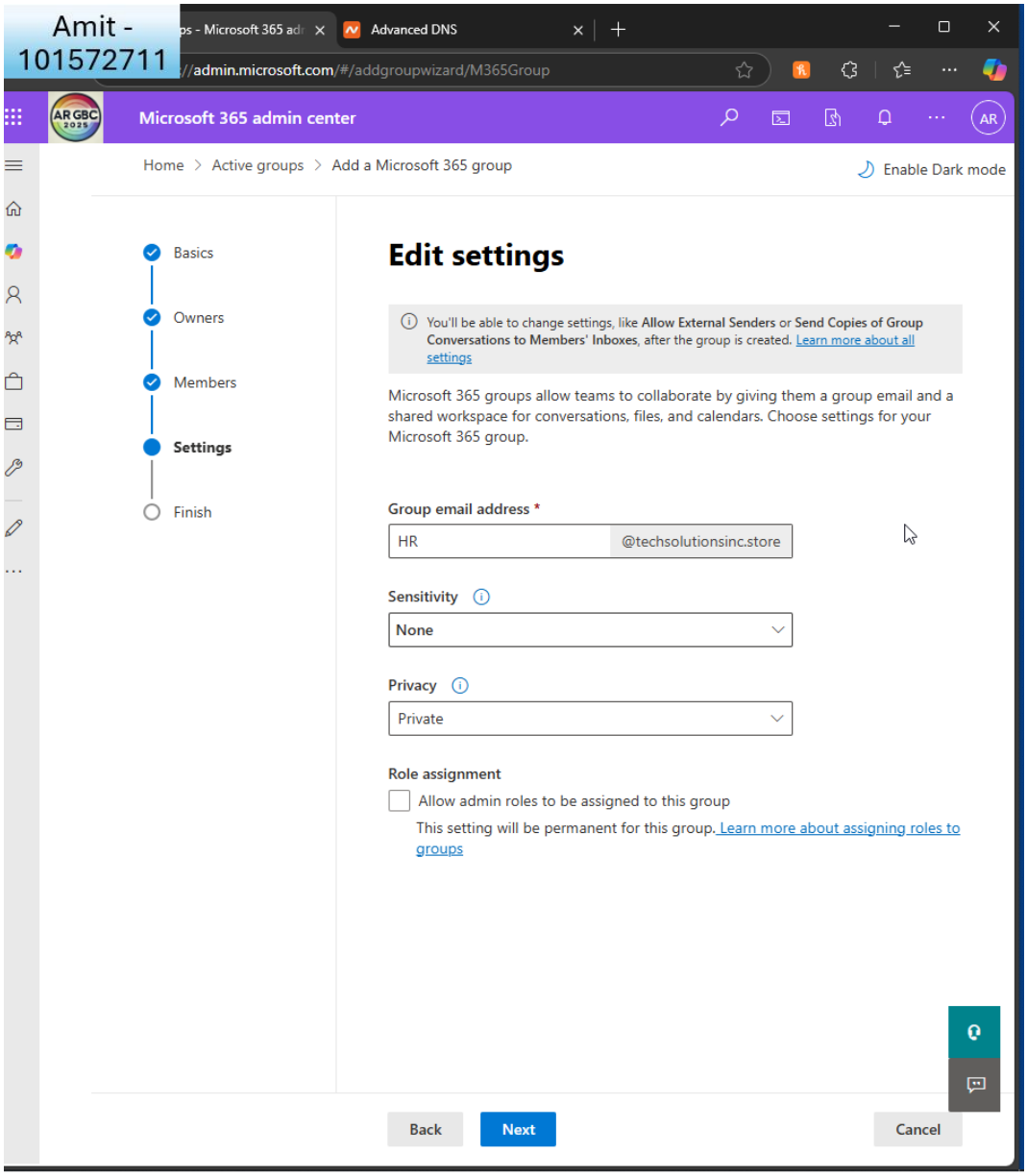
Student Name: ……. Term: ……..
Student ID: ……..



Student Name: ……. Term: ……..
Student ID: ……..

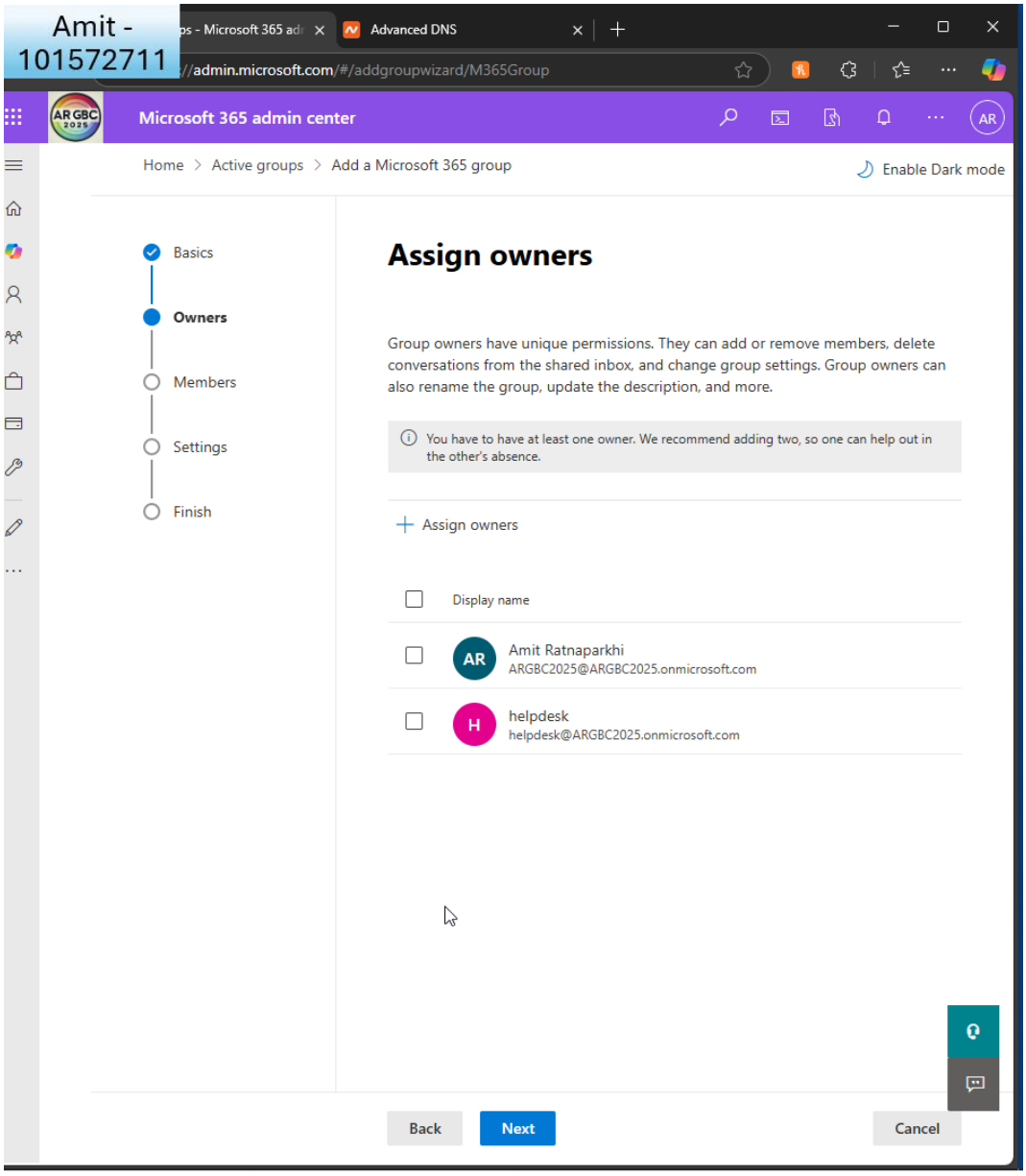


Student Name: ……. Term: ……..
Student ID: ……..

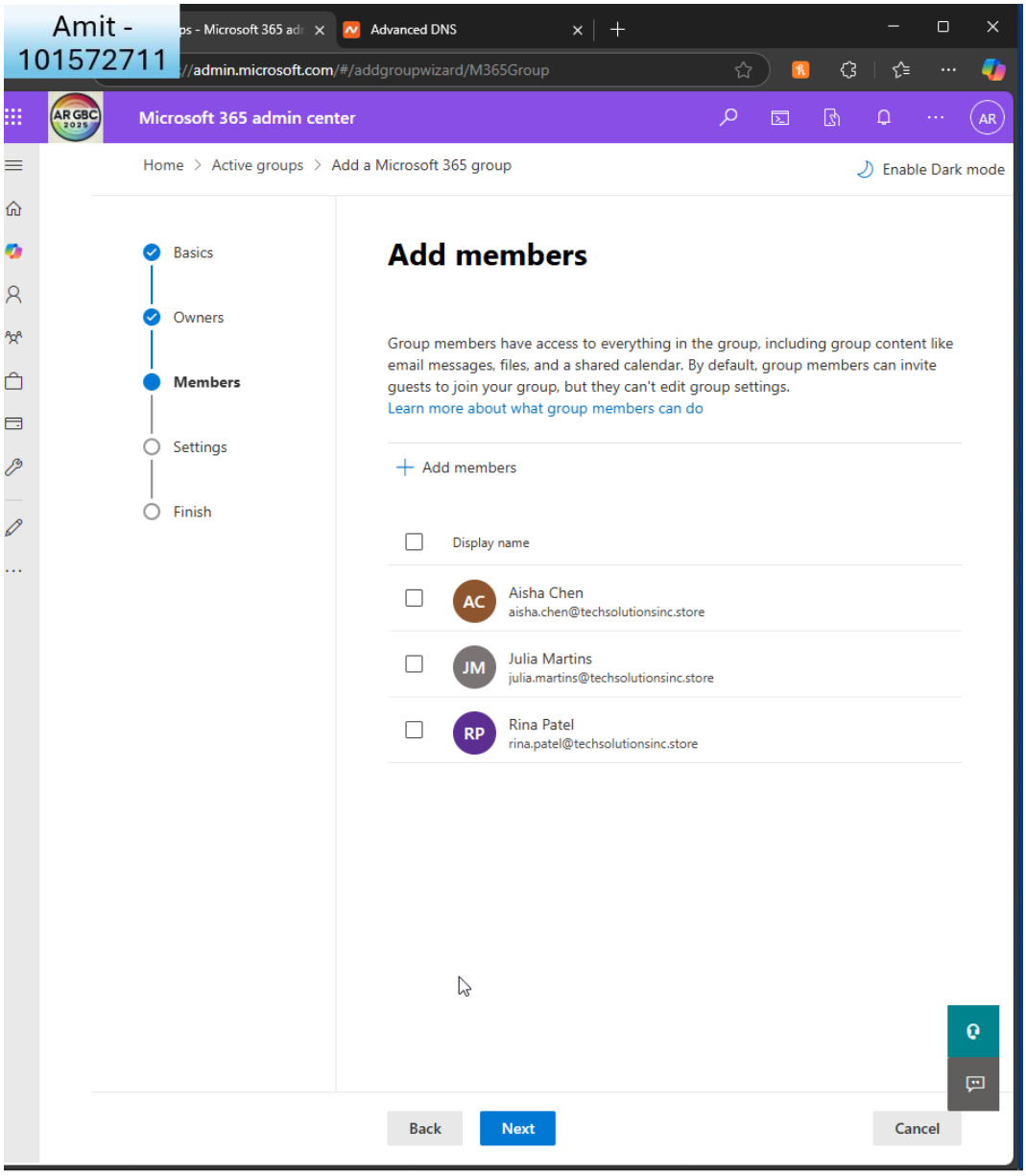


This is the HR department

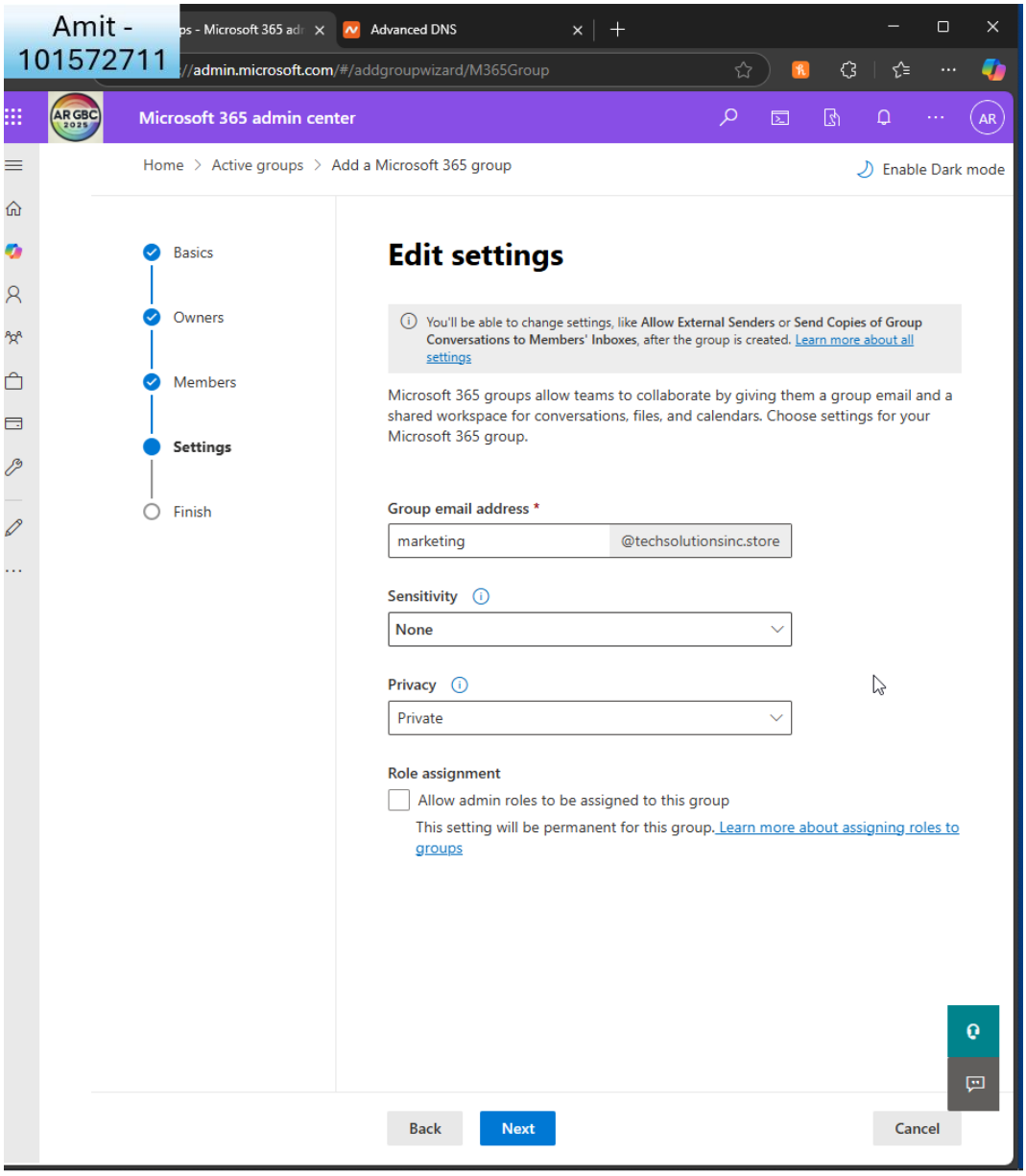
Student Name: ……. Term: ……..
Student ID: ……..



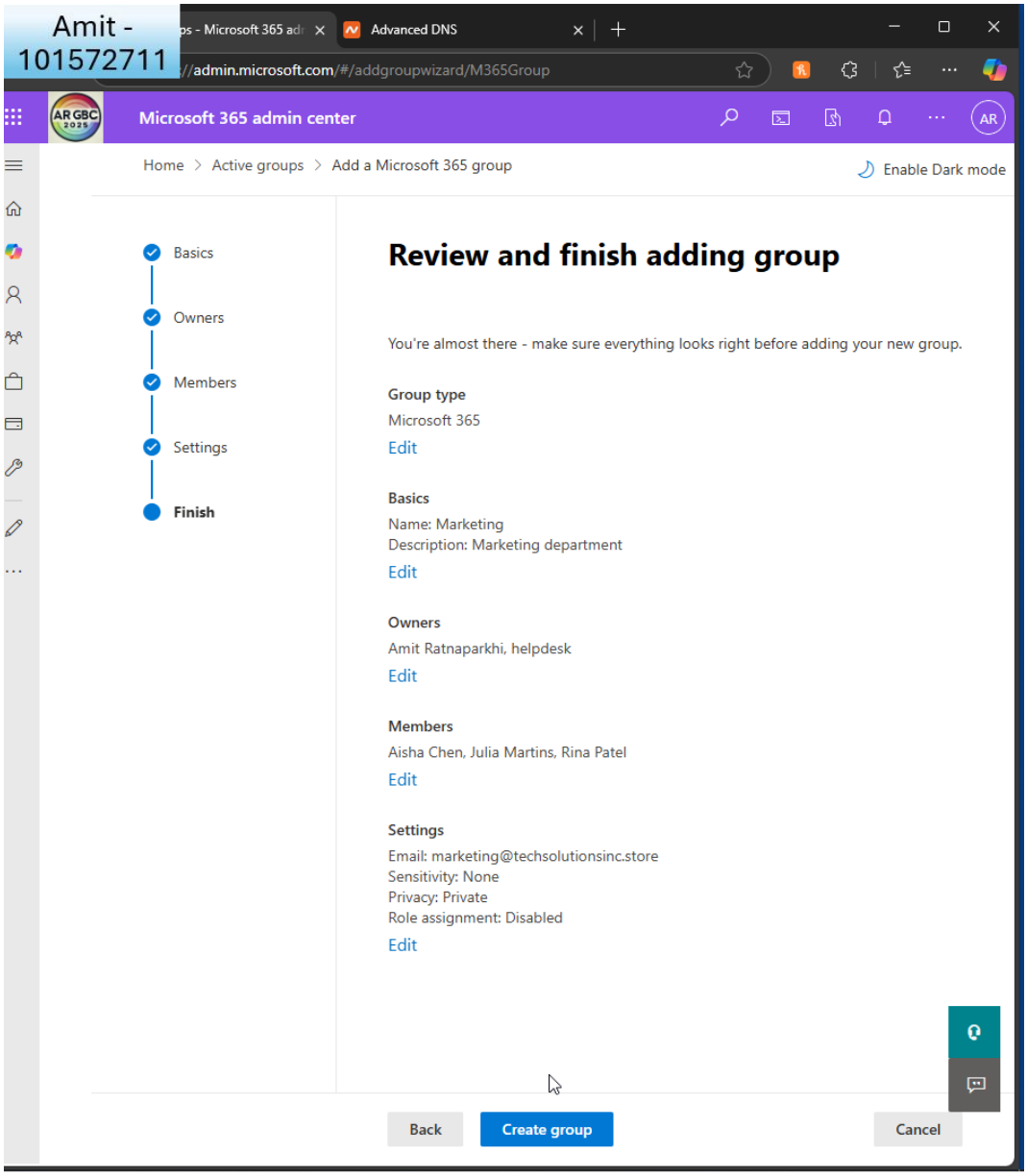
Student Name: ……. Term: ……..
Student ID: ……..



Student Name: ……. Term: ……..
Student ID: ……..

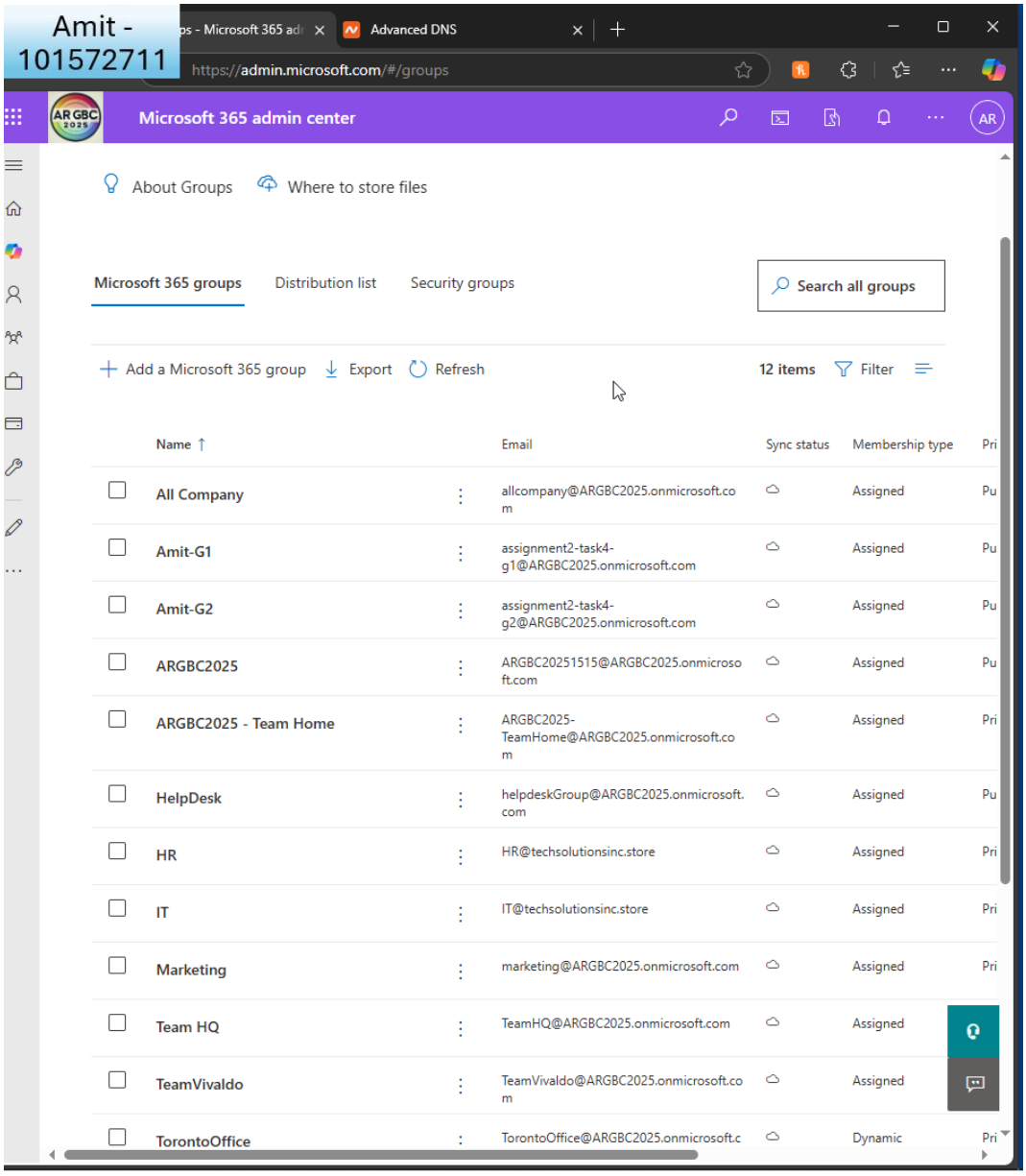


Student Name: ……. Term: ……..
Student ID: ……..



This is the marketing department

Student Name: ……. Term: ……..
Student ID: ……..

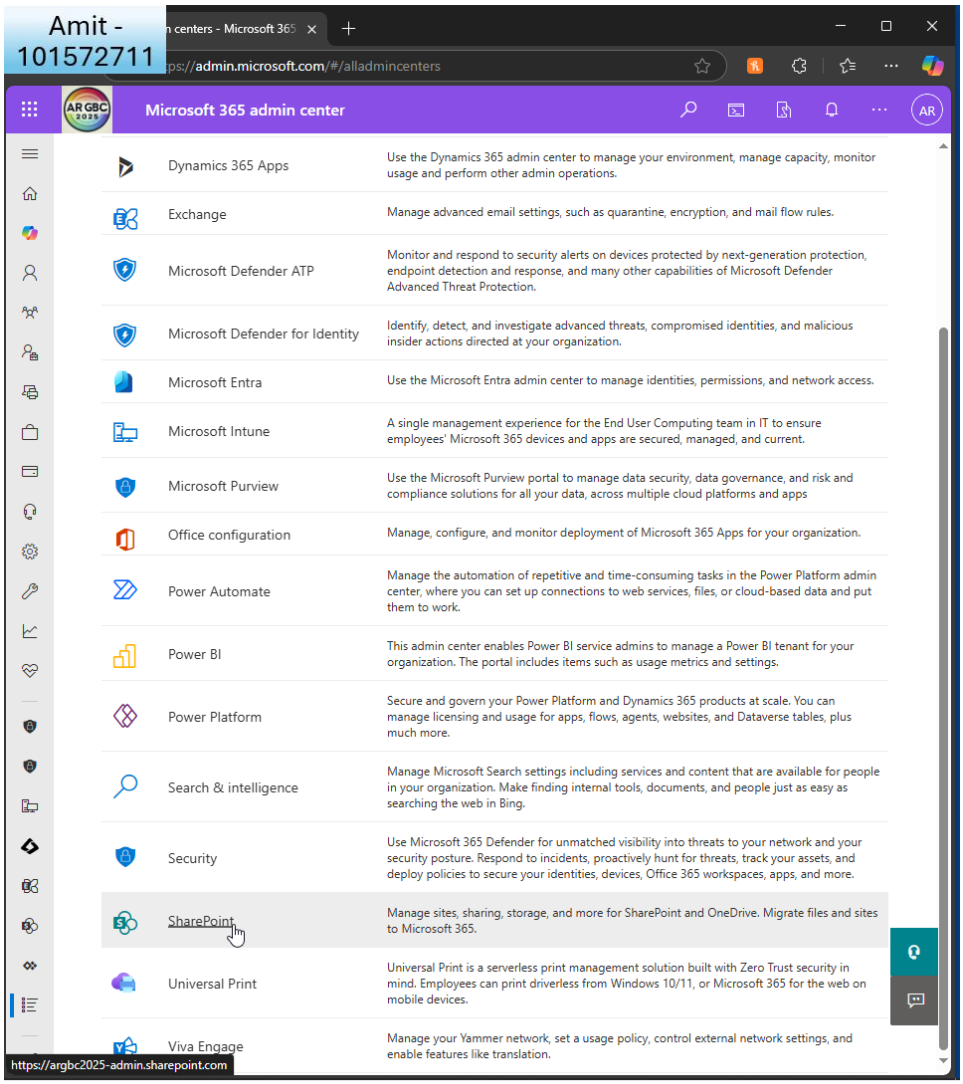


Confirmation of groups creation

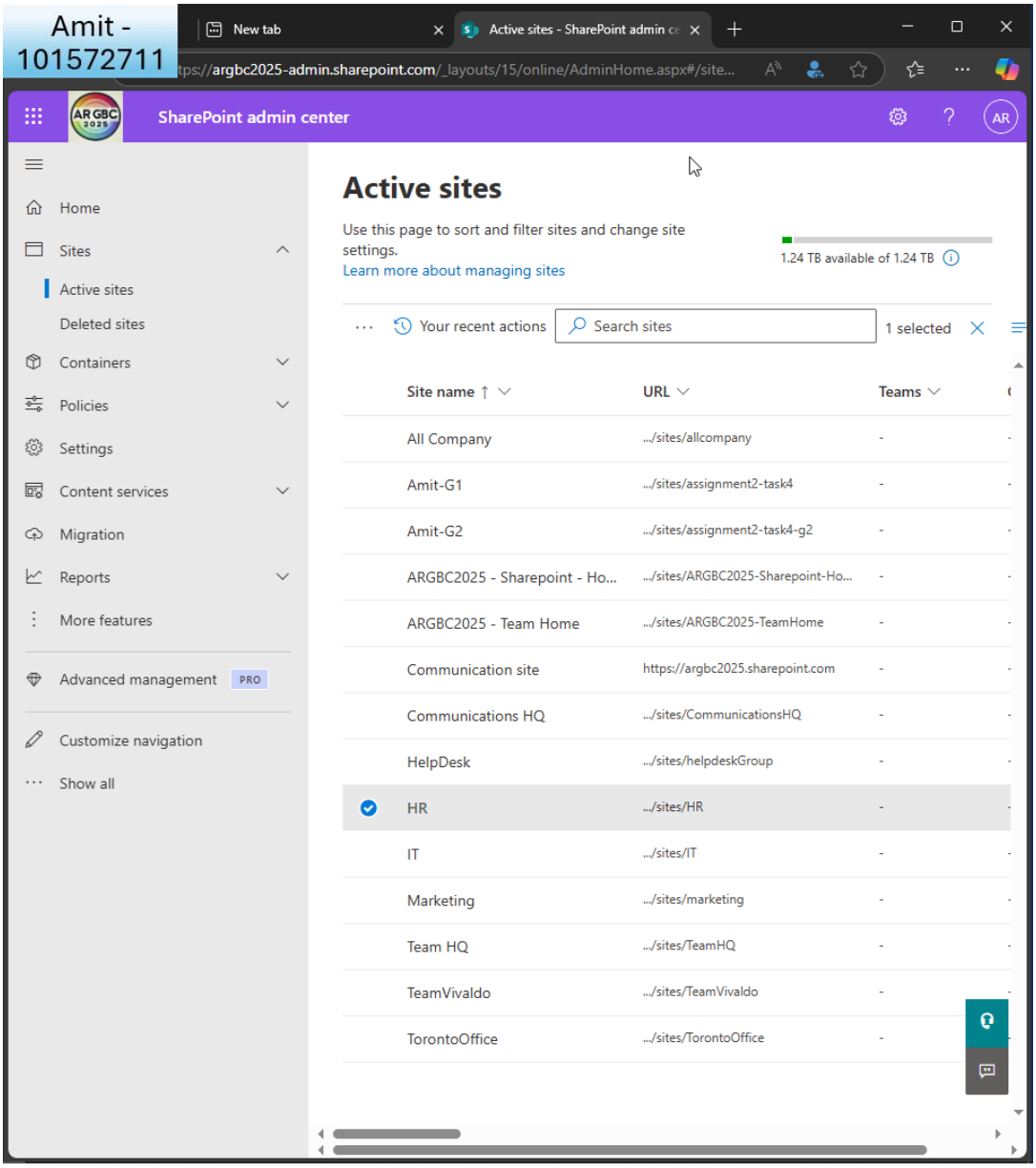
4. **Configure User Permissions**:

Student Name: ……. Term: ……..
Student ID: ……..

- Assign specific permissions to the HR group to access sensitive HR documents in SharePoint.

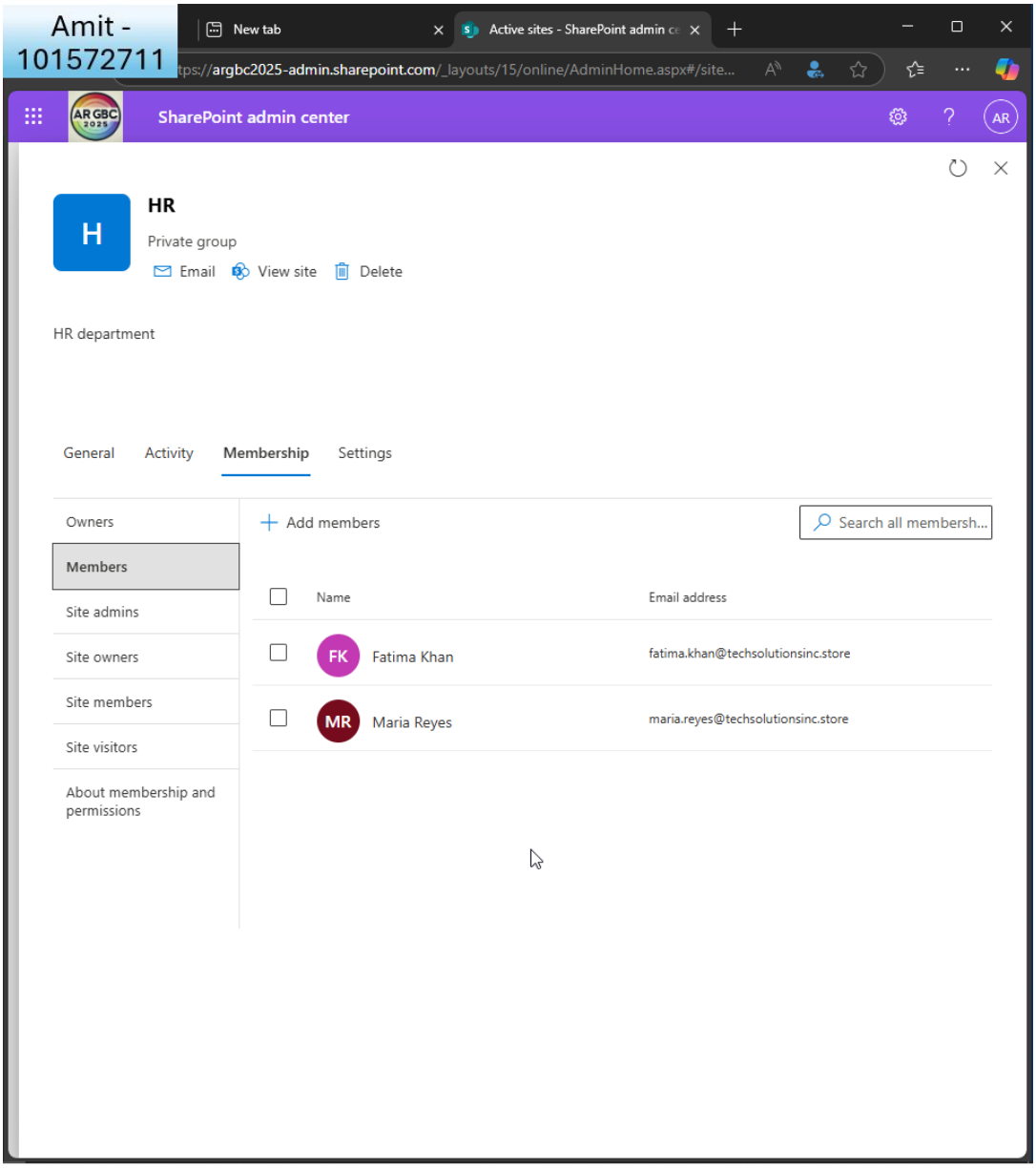


Student Name: ……. Term: ……..
Student ID: ……..



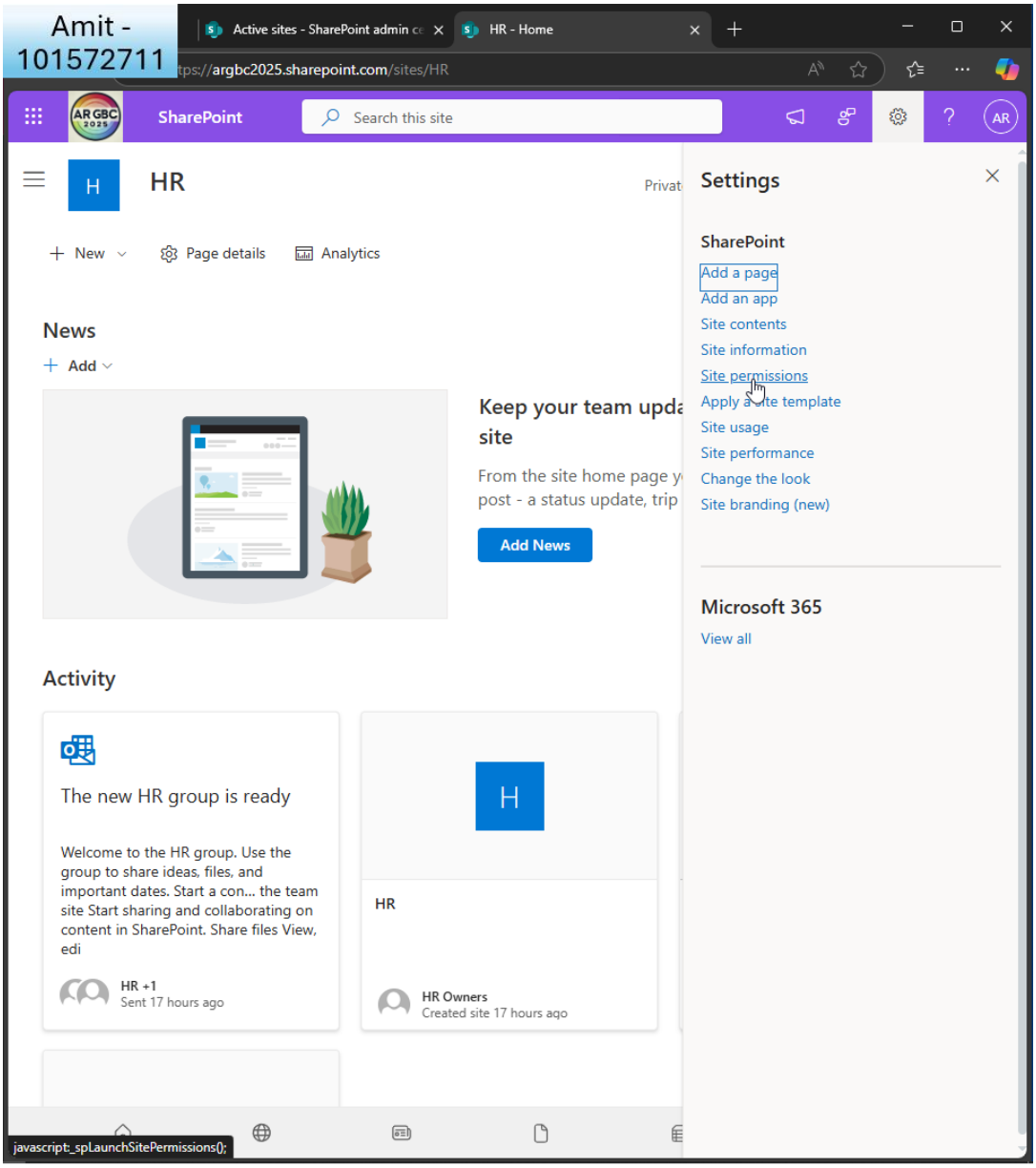
I choose the HR sharepoint site

Student Name: ……. Term: ……..
Student ID: ……..



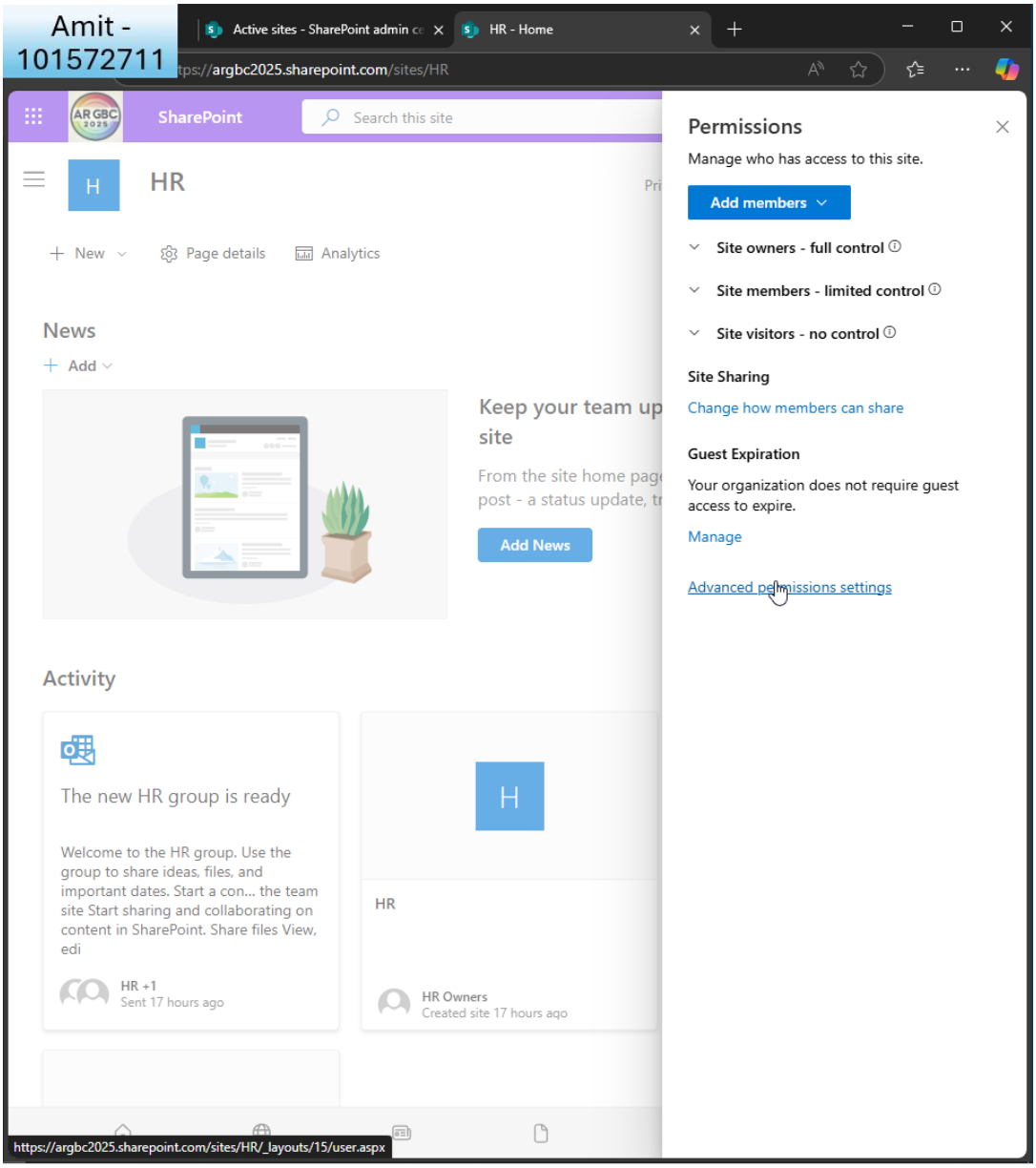
I see the members of the group

Student Name: ……. Term: ……..
Student ID: ……..



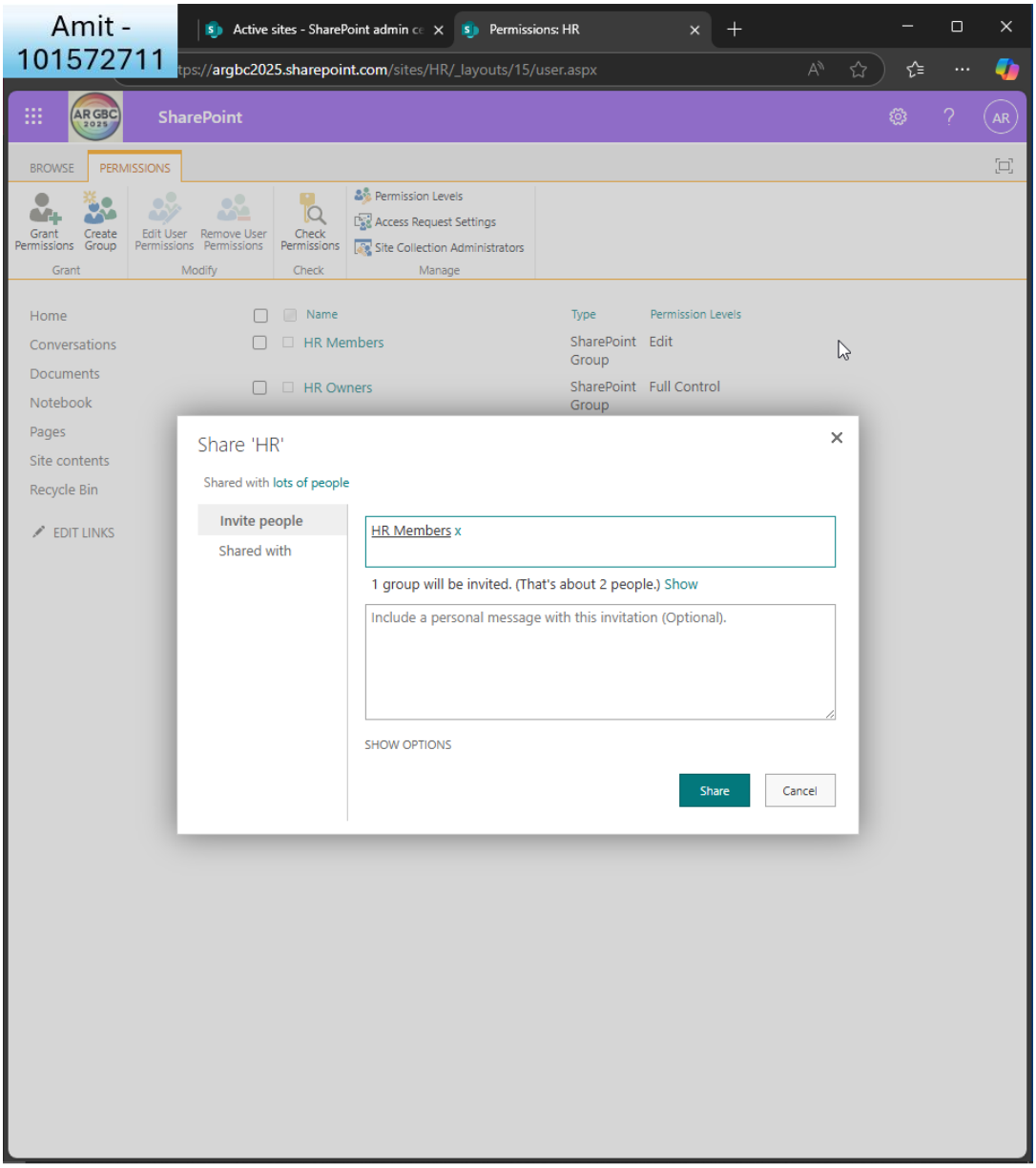
I change site permissions

Student Name: ……. Term: ……..
Student ID: ……..



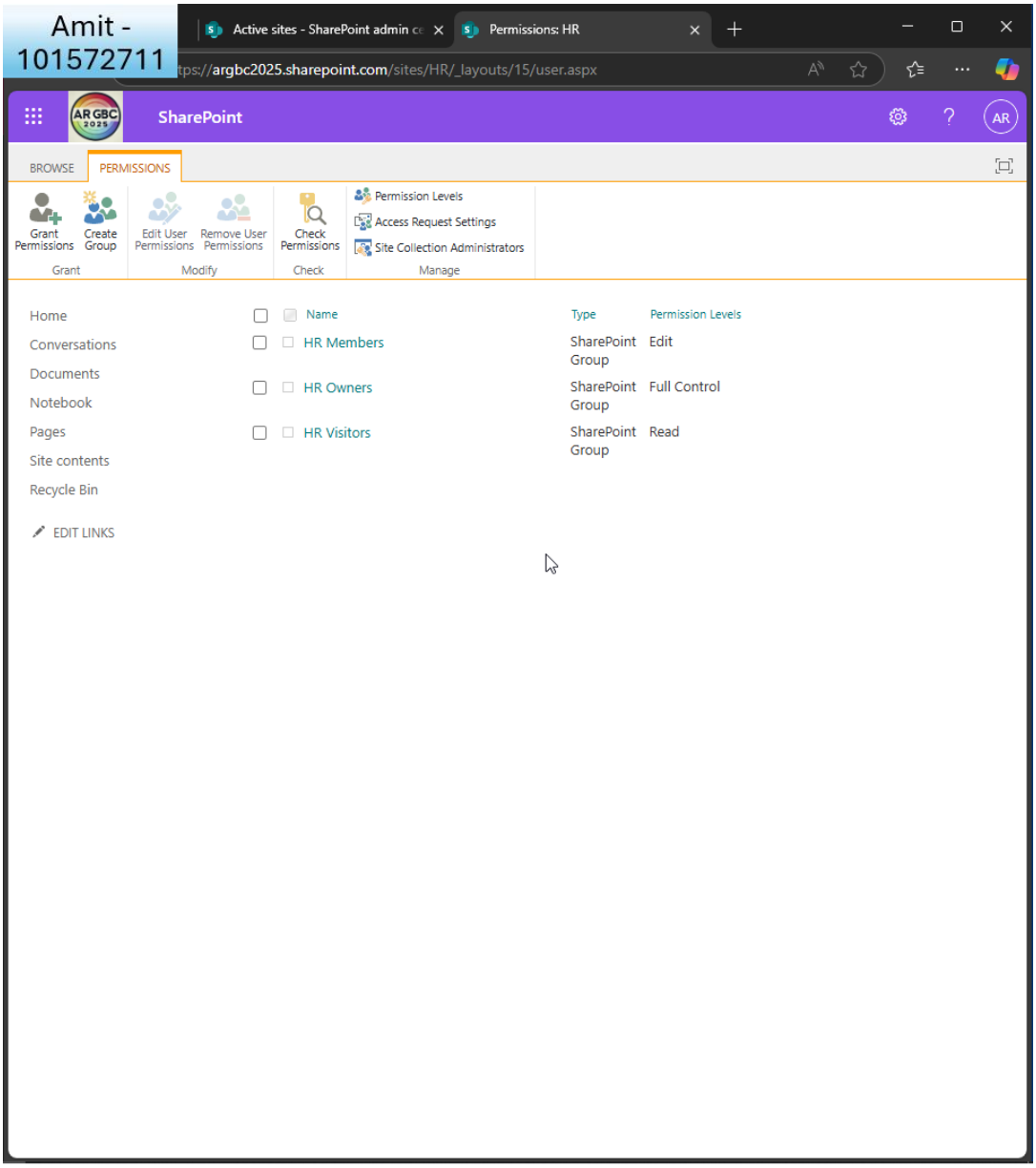
I click 'advanced permissions settings'

Student Name: ……. Term: ……..
Student ID: ……..



I choose HR group

Student Name: ……. Term: ……..
Student ID: ……..



I can see the different levels of permissions

- Ensure the Marketing group has permission to create and manage Microsoft Teams.

Part B:

What a task! I found it a little complicated at first but once it was done, it was nice to have that feeling of accomplishment!

Task 1 gave me hands-on experience with creating a Microsoft 365 environment for practical and realistic purposes. As a first step, I actually went ahead and registered a live domain techsolutionsinc.store with Namecheap and paired it with Microsoft 365. Setting up DNS records like MX, TXT, and CNAME records was an exercise, to be sure, but one that highlighted how domain control is critical to both email and identity functionality within a cloud configuration.

It was not too difficult to mass-import users (I learnt using Powershell), but configuring their profiles was a tad hard! I learnt how to personalise user fields like job titles, offices, and Departments, and I even mass-added profile pictures to all users. I wanted to give it a realistic feel so I used ChatGPT to create their photos! It entailed learning to script, debugging file paths, and manipulating authentication scopes with Microsoft Graph. It was rewarding to have an entire directory of staff at the end.

Enablement of Microsoft 365 for HR, Marketing, and IT helped to cement how role-based access and collaboration work across the Microsoft platform. Provision of controlled access to SharePoint to the HR team gave me direct experience with how permissions can be scoped finely for confidential data.

Overall, I found Microsoft 365 to be powerful but at times frustrating to navigate through the process. Certain settings were difficult to locate, occasionally the UI was not great! (particularly between new vs. legacy admin portals), and group/team relationships were not as clear as required. I wish that Microsoft would make group-level permissions more intuitive, particularly moving between Teams, SharePoint, and Entra. It feels like there's a lack of consistency.

In total, I was able to learn how to provision a professional Microsoft 365 estate from scratch, and the exercise did help me increase my confidence with regards to working with live tenants.

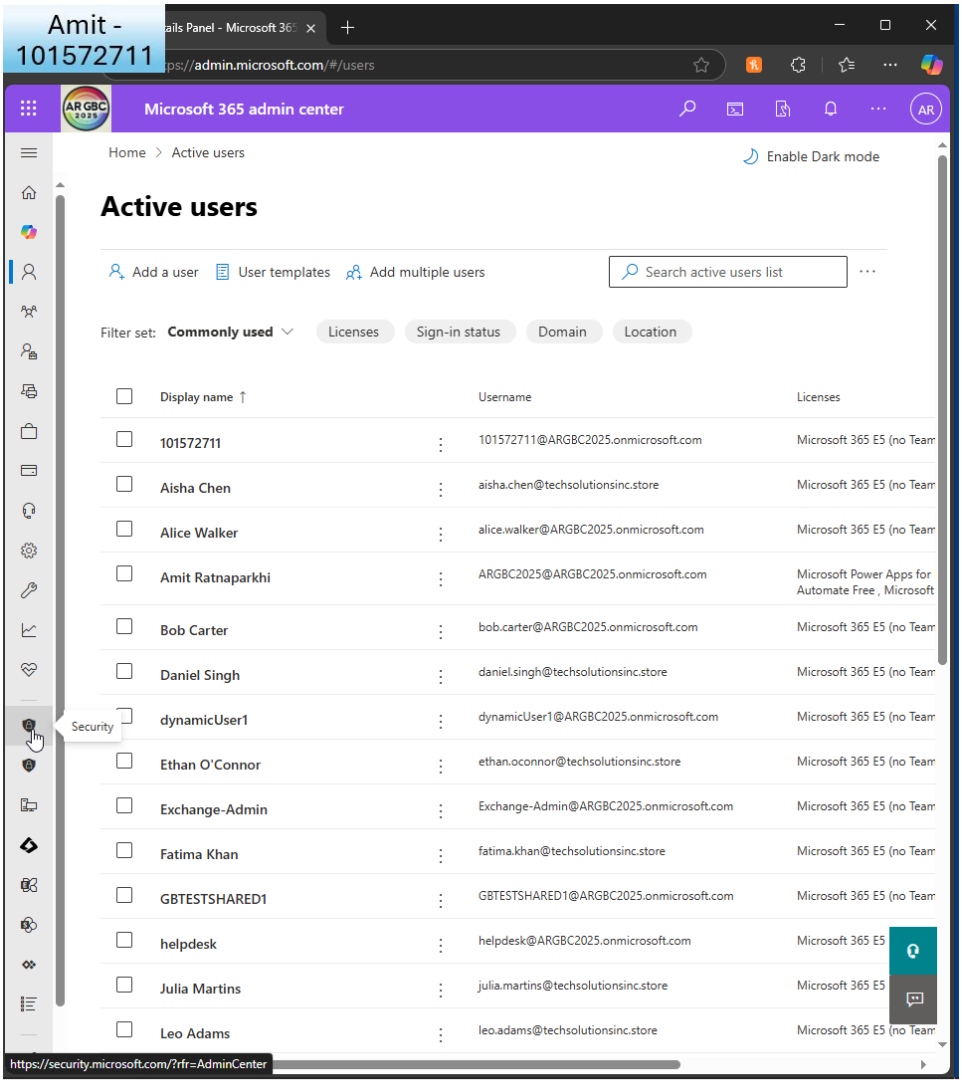
Task 2: Implementing Security Measures

1. **Set Up and Configure Microsoft Defender for Office 365**:

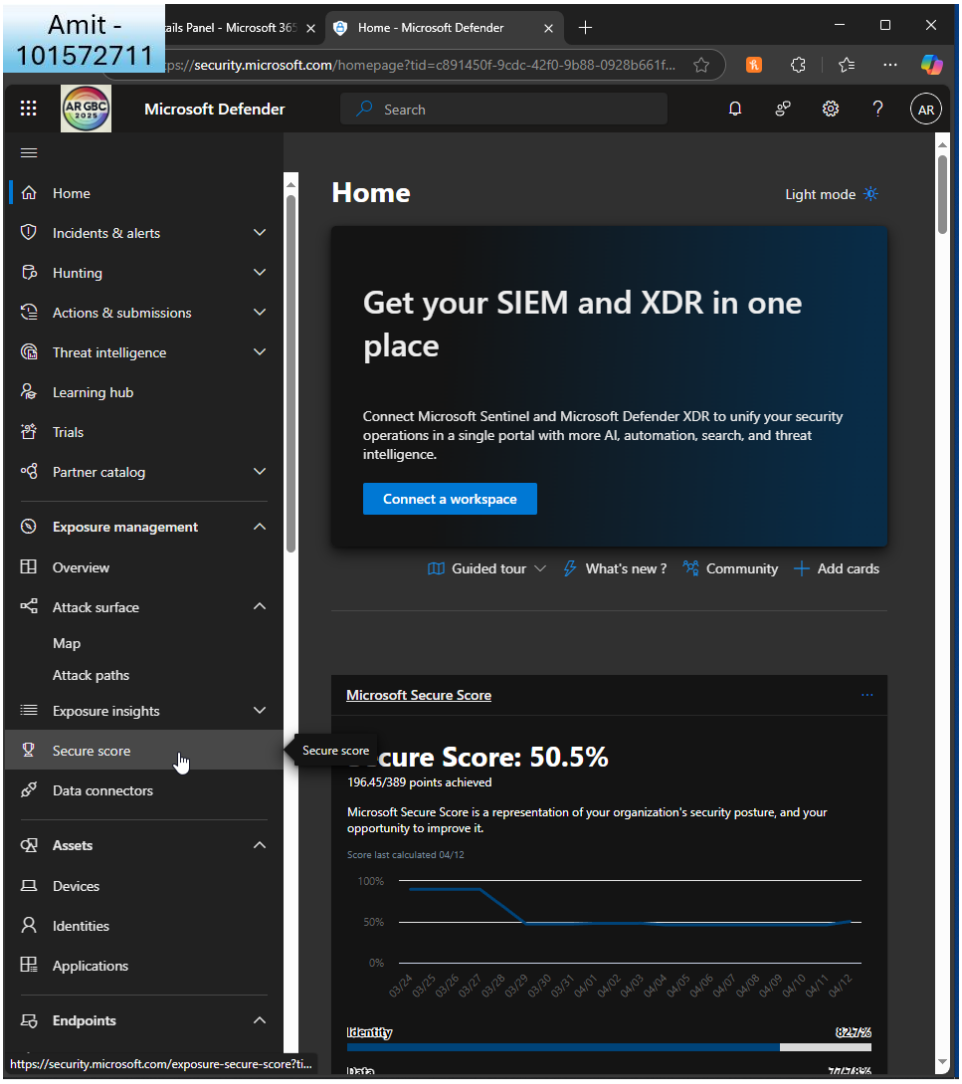
   Part A:

   - Access the MS Defender and navigate to Secure Score.

Student Name: ……. Term: …….
Student ID: ……..

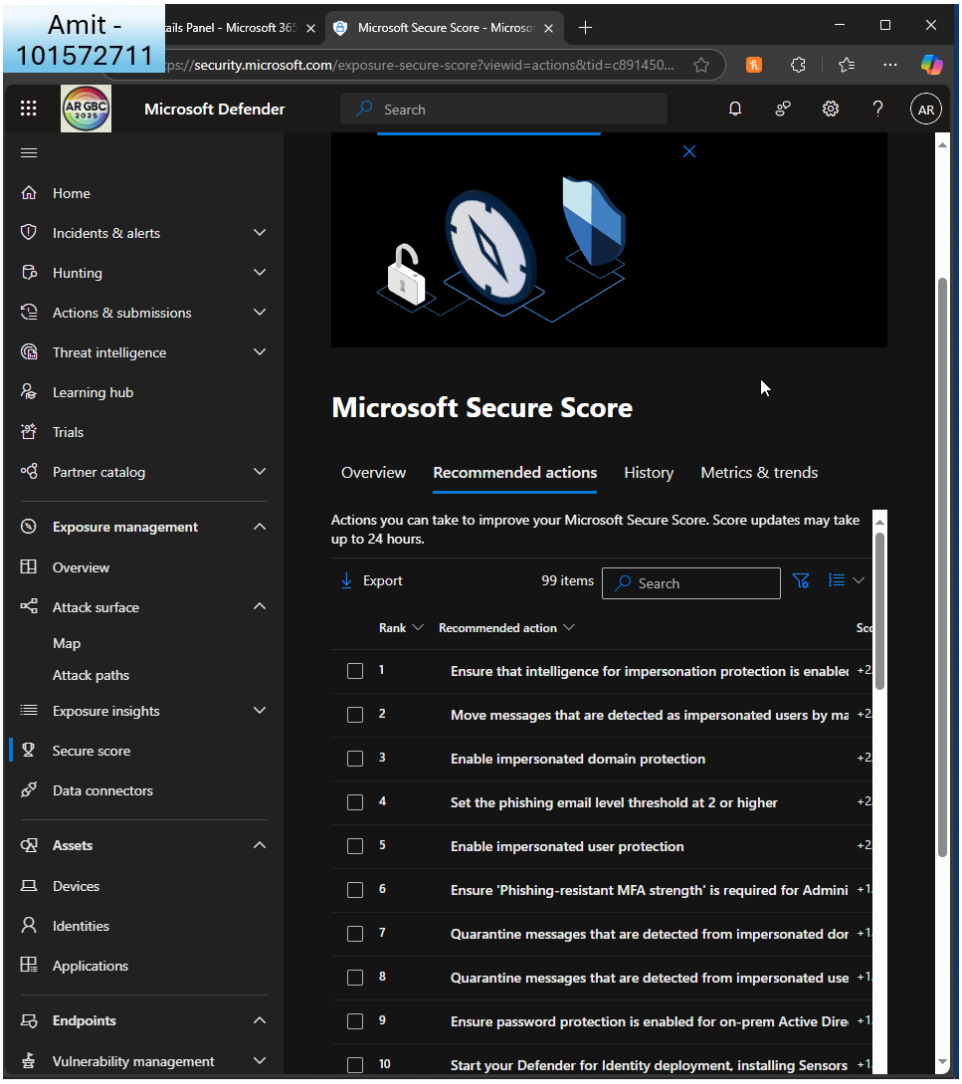


Student Name: ……. Term: ……..
Student ID: ……..



Here I can see my score of 50.5%

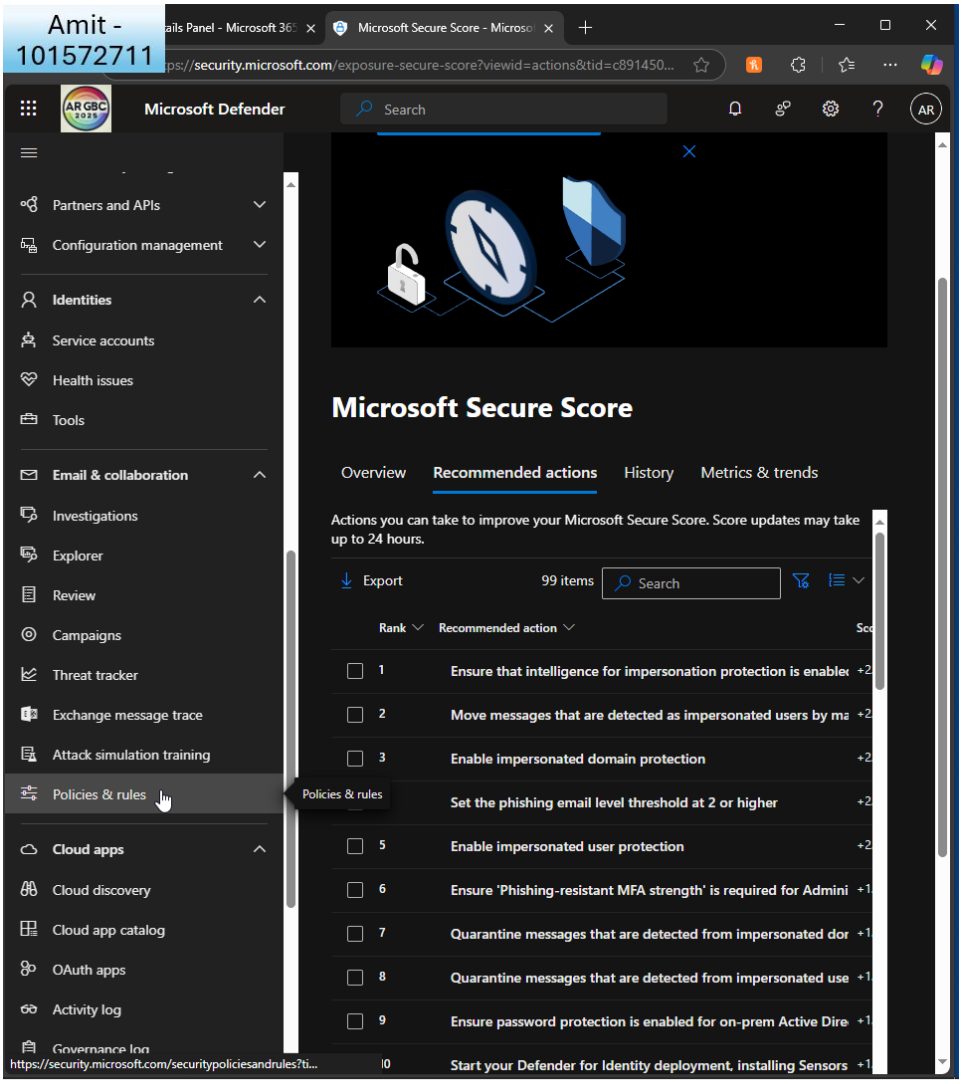
Student Name: ……. Term: …….
Student ID: …….



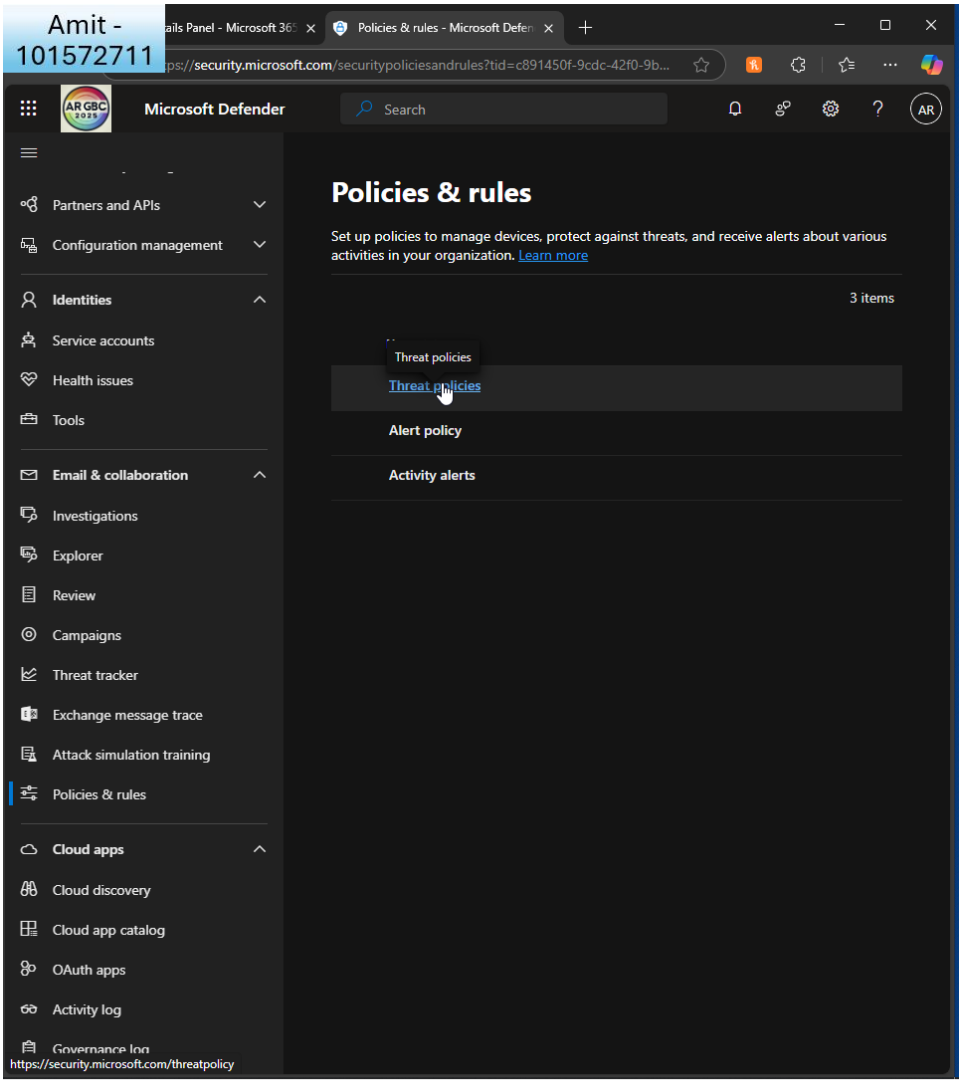
Here I see a list of recommendations

- Ensure that Safe Links and Safe Attachments have been enabled for all users.

Student Name: ……. Term: ……..
Student ID: ……..

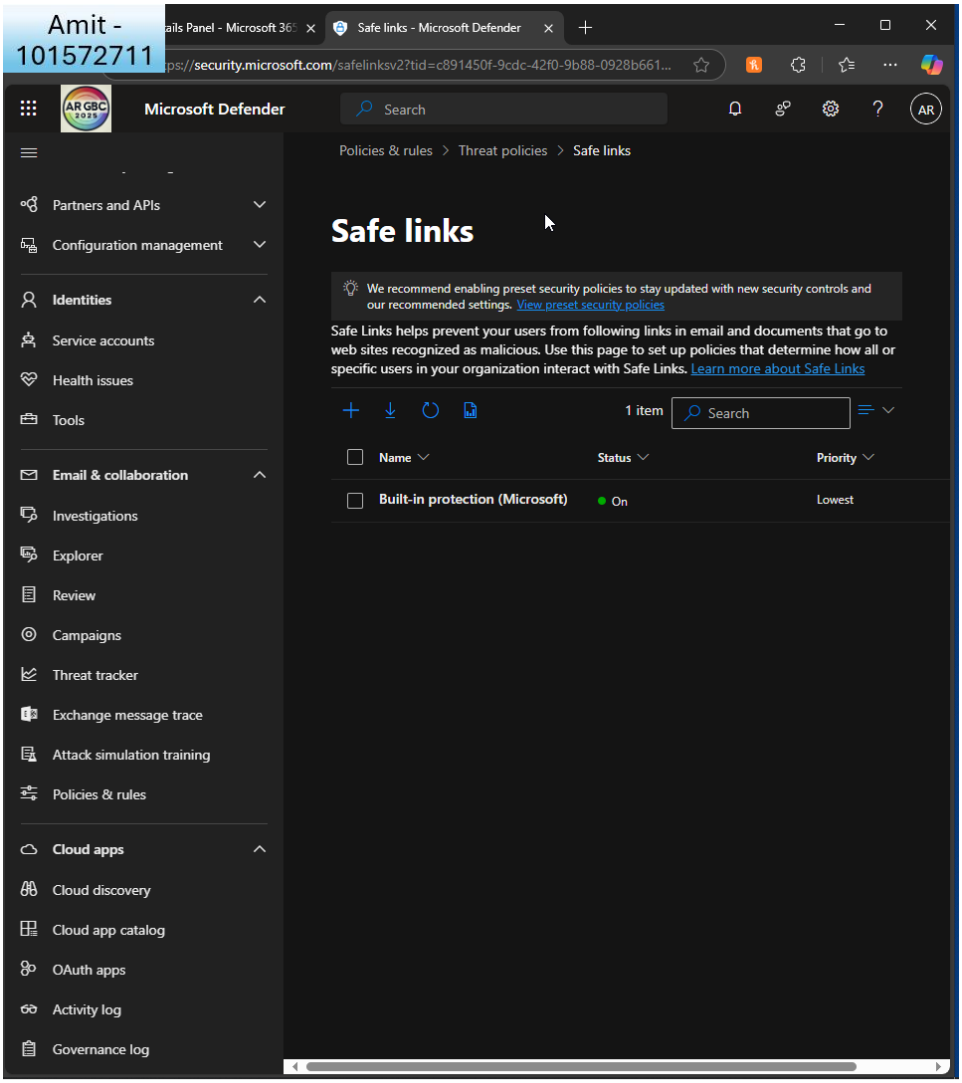


Student Name: ……. Term: ……..
Student ID: ……..



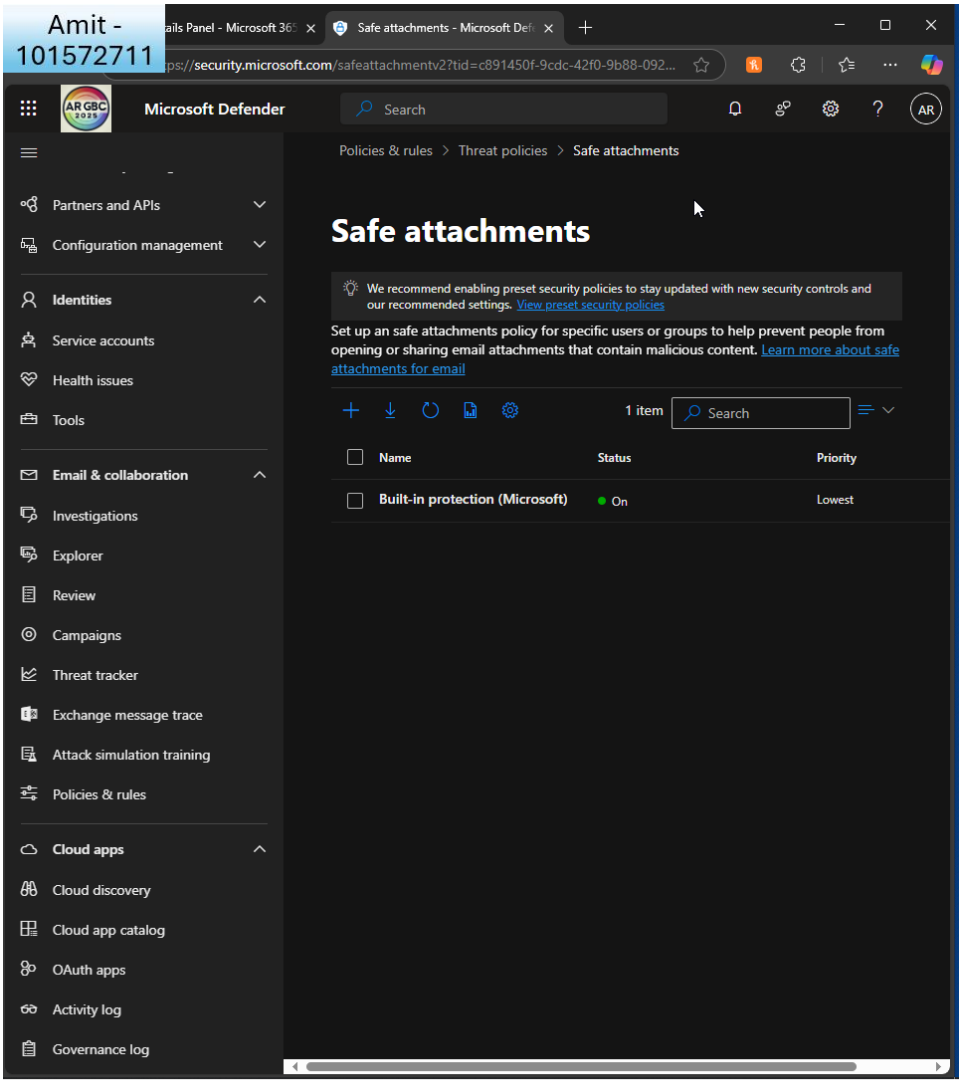
I check the current threat policies

Student Name: ……. Term: ……..
Student ID: ……..



I can see safe links is already enabled

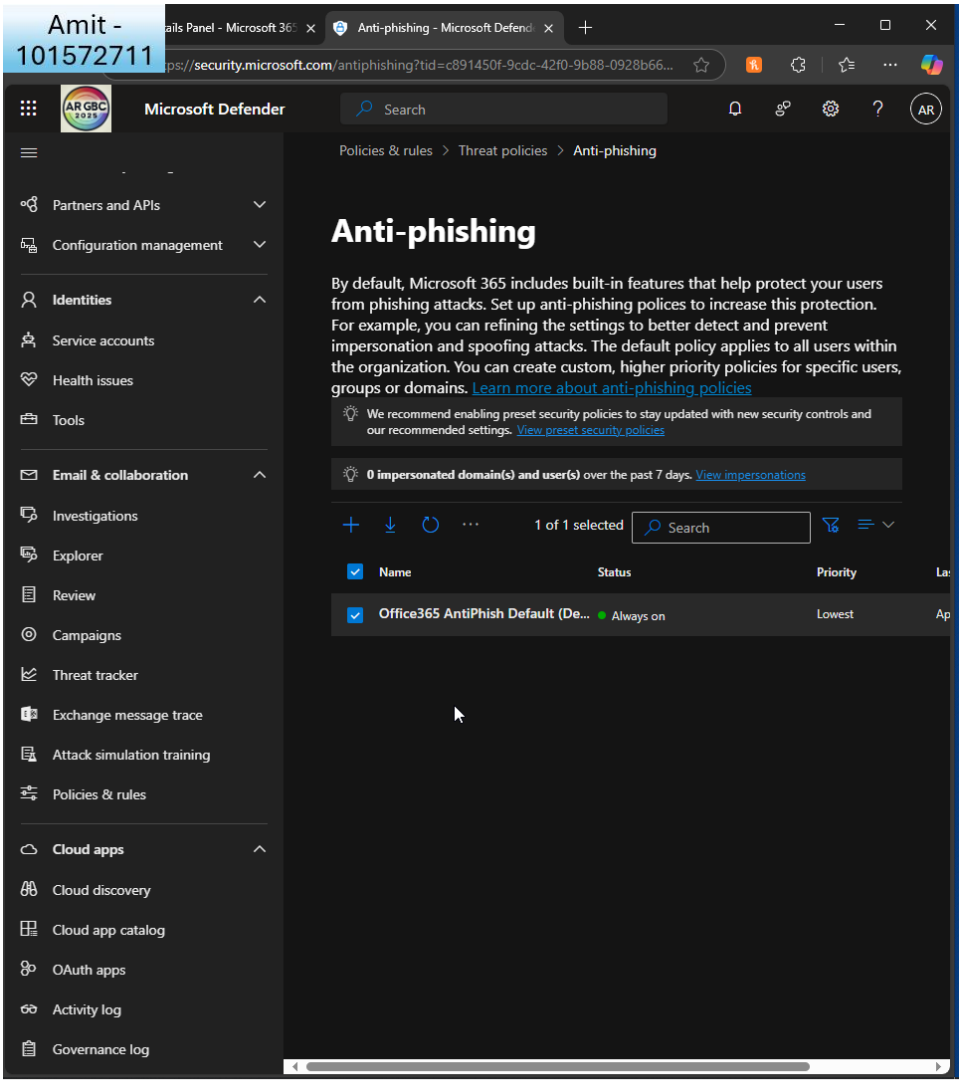
Student Name: ……. Term: ……..
Student ID: ……..



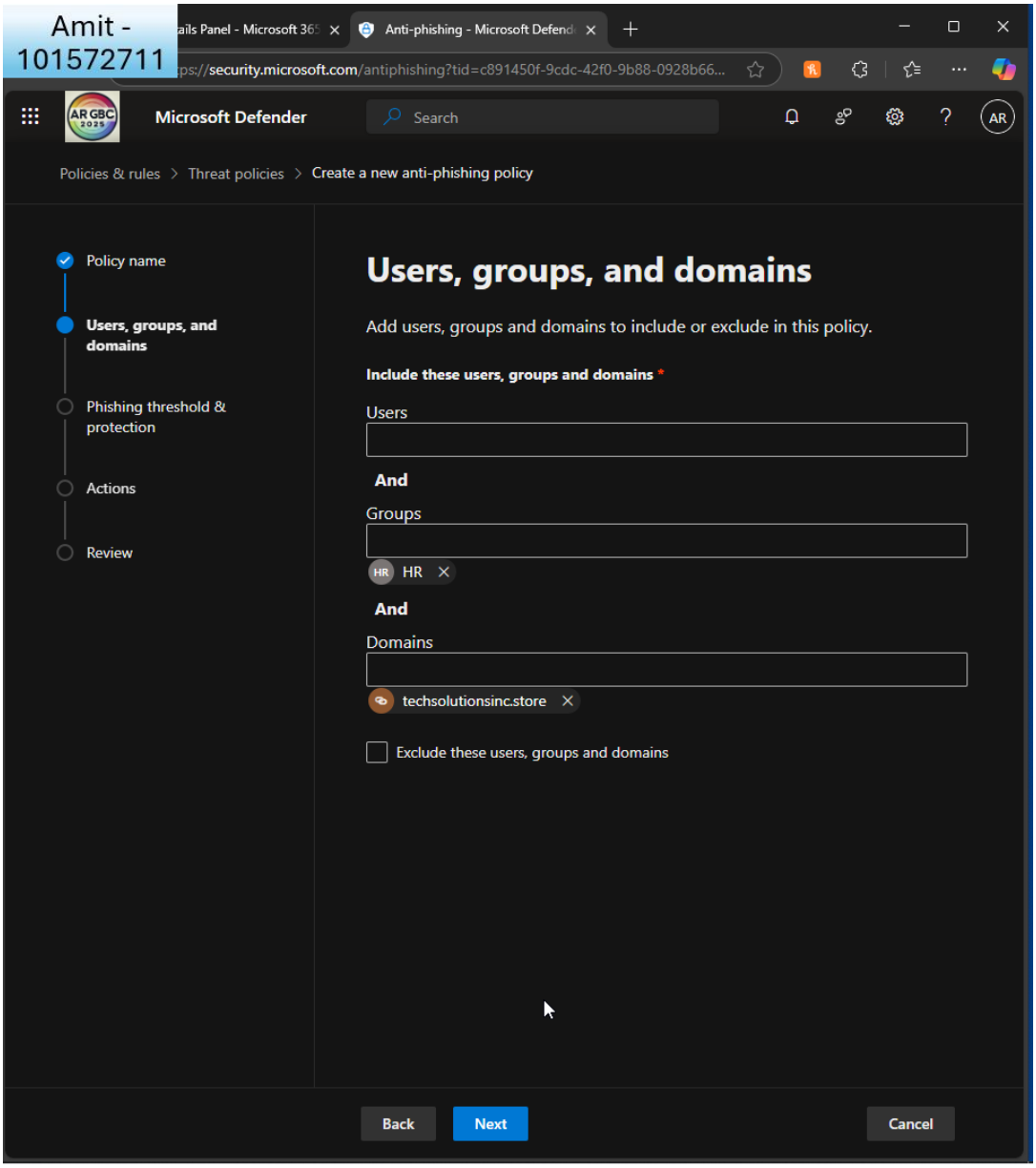
As is safe attachments

- Navigate to Policies and rules, then configure at least one policy to protect against phishing, malware, or spam.

Student Name: ……. Term: ……..
Student ID: ……..

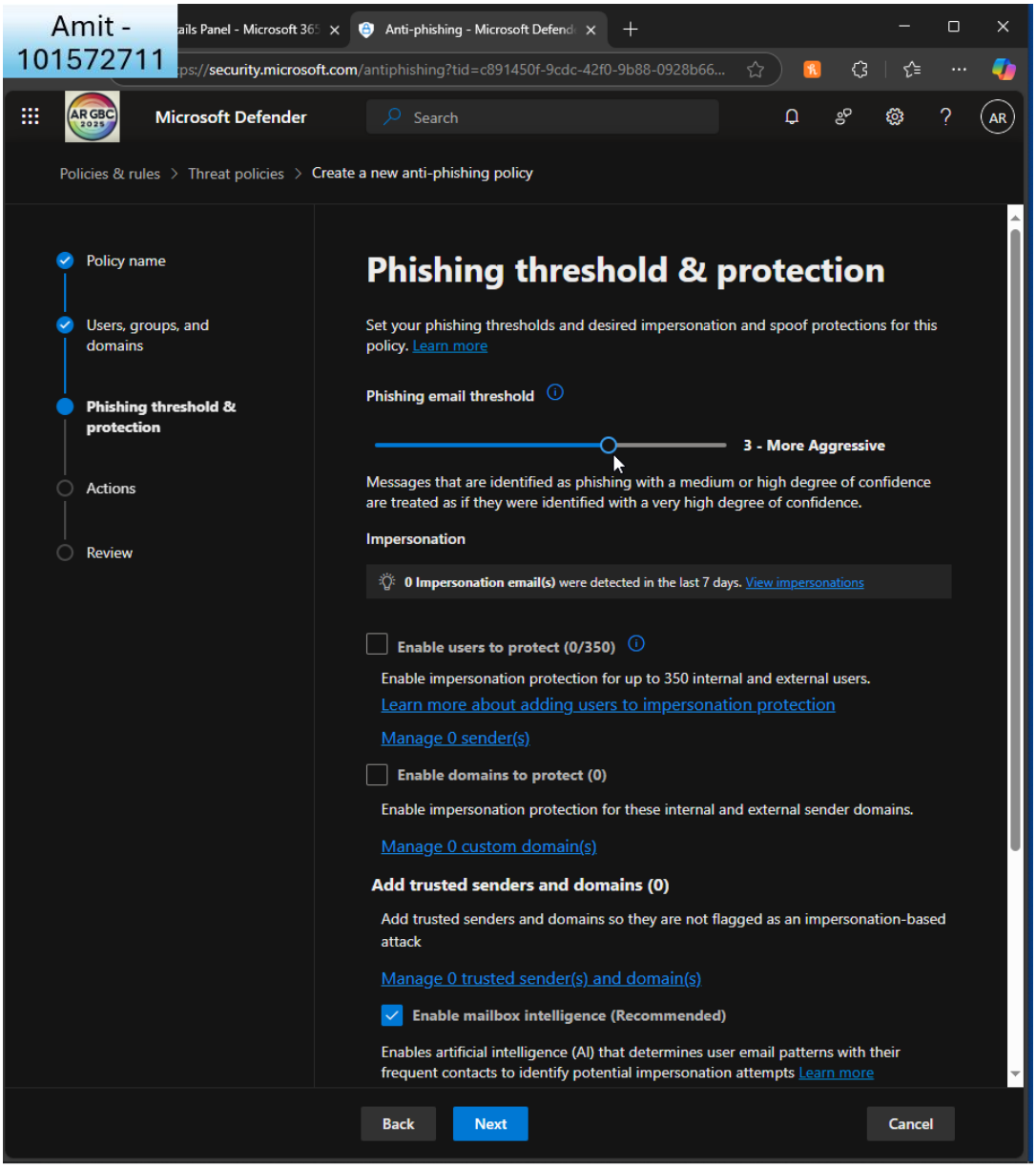


Student Name: ……. Term: ……..
Student ID: ……..



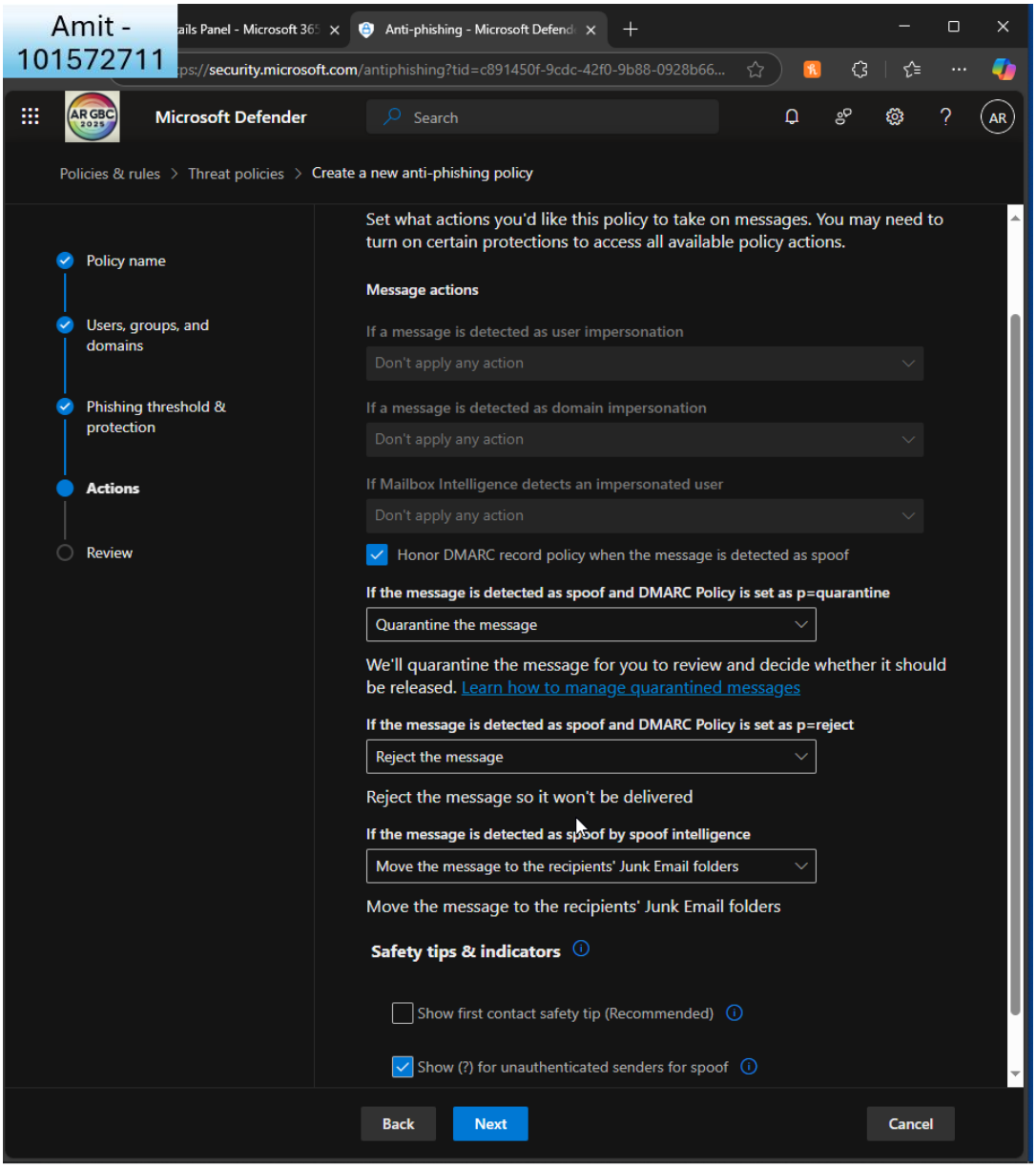
I create a new anti-phishing policy to apply to my HR group on techsolutions domain

Student Name: ……. Term: ……..
Student ID: ……..



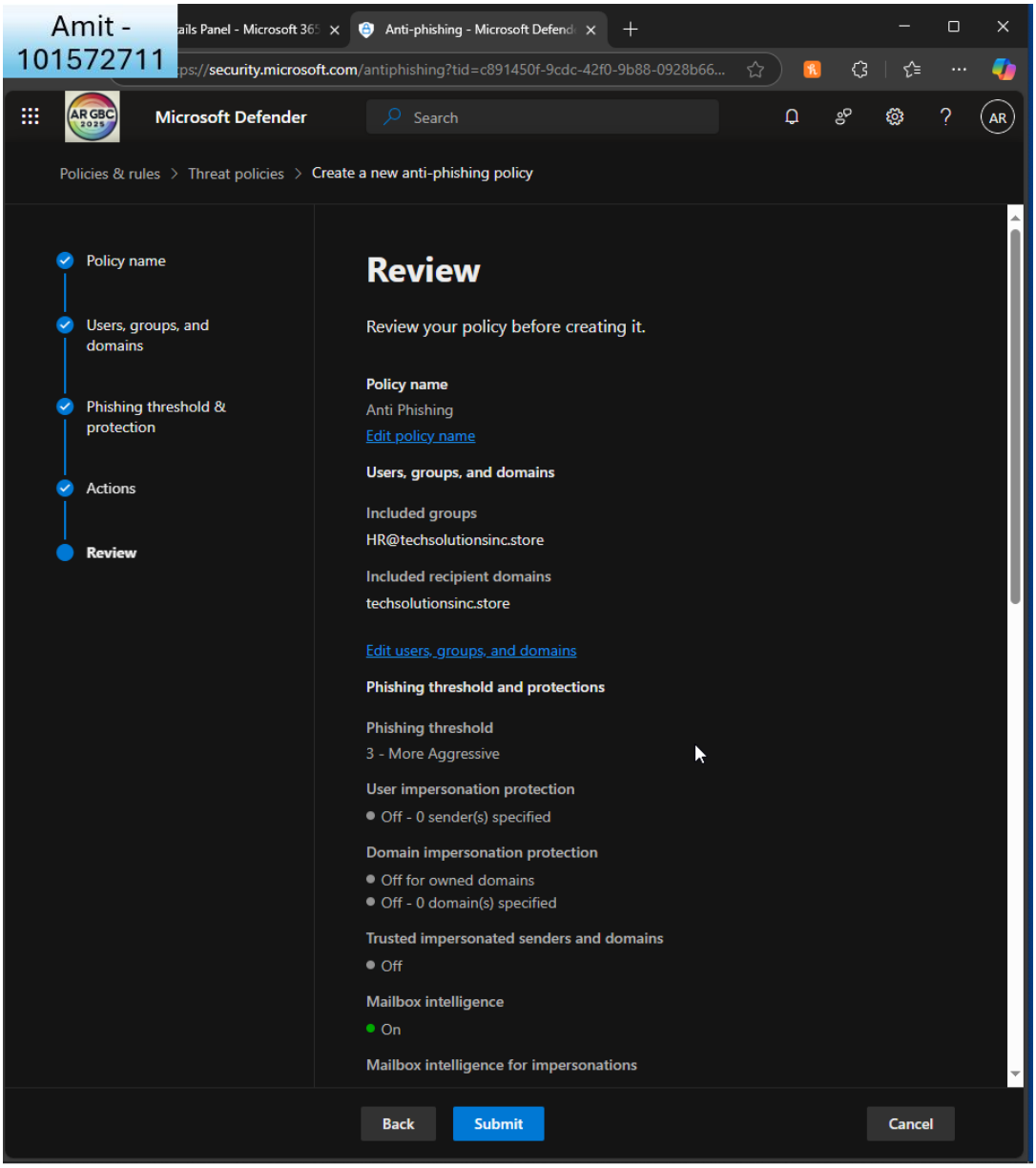
I choose a more aggressive threshold

Student Name: ……. Term: ……..
Student ID: ……..



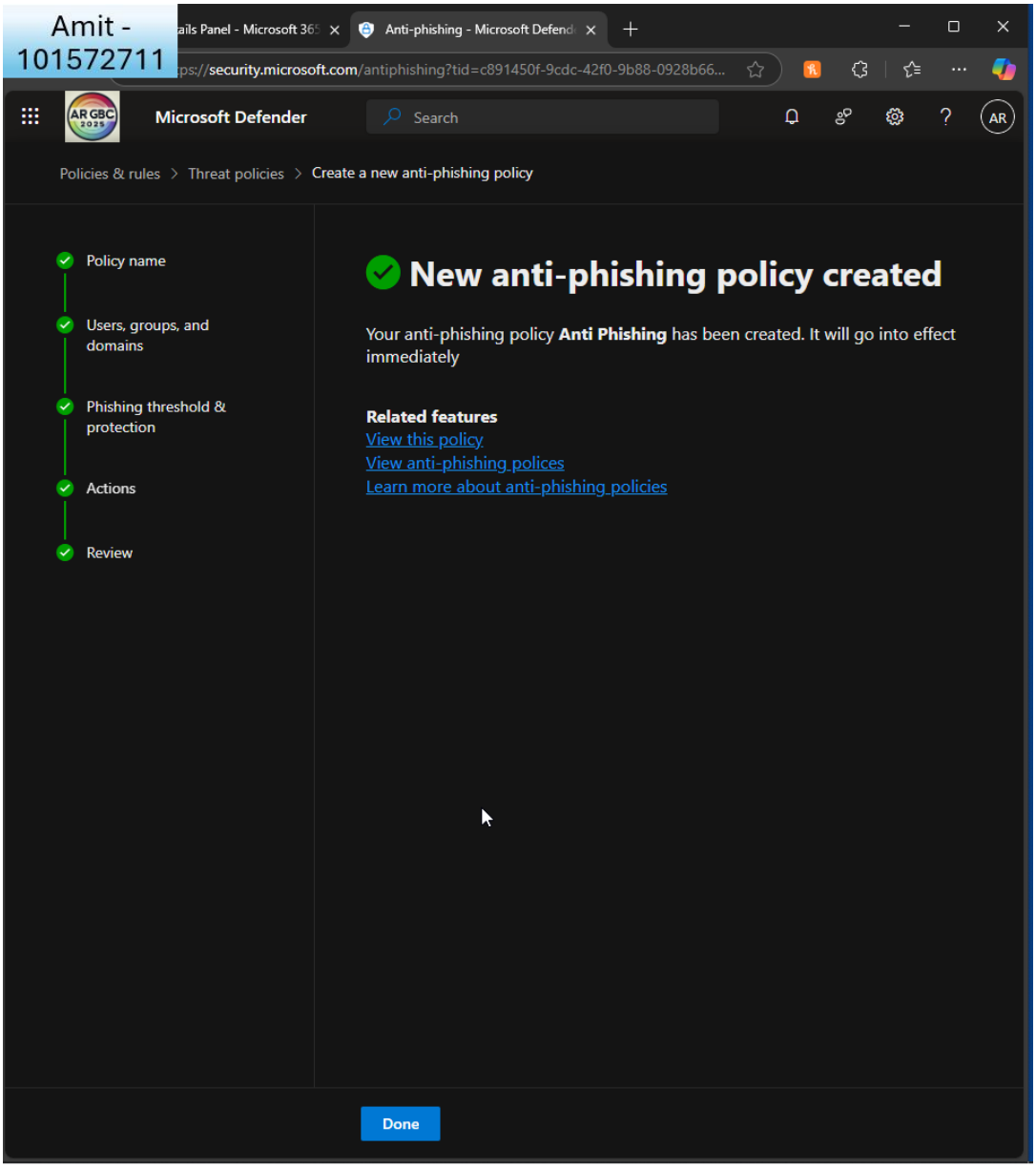
I keep default settings

Student Name: ……. Term: ……..
Student ID: ……..



I review the policy

Student Name: ……. Term: ……..
Student ID: ……..



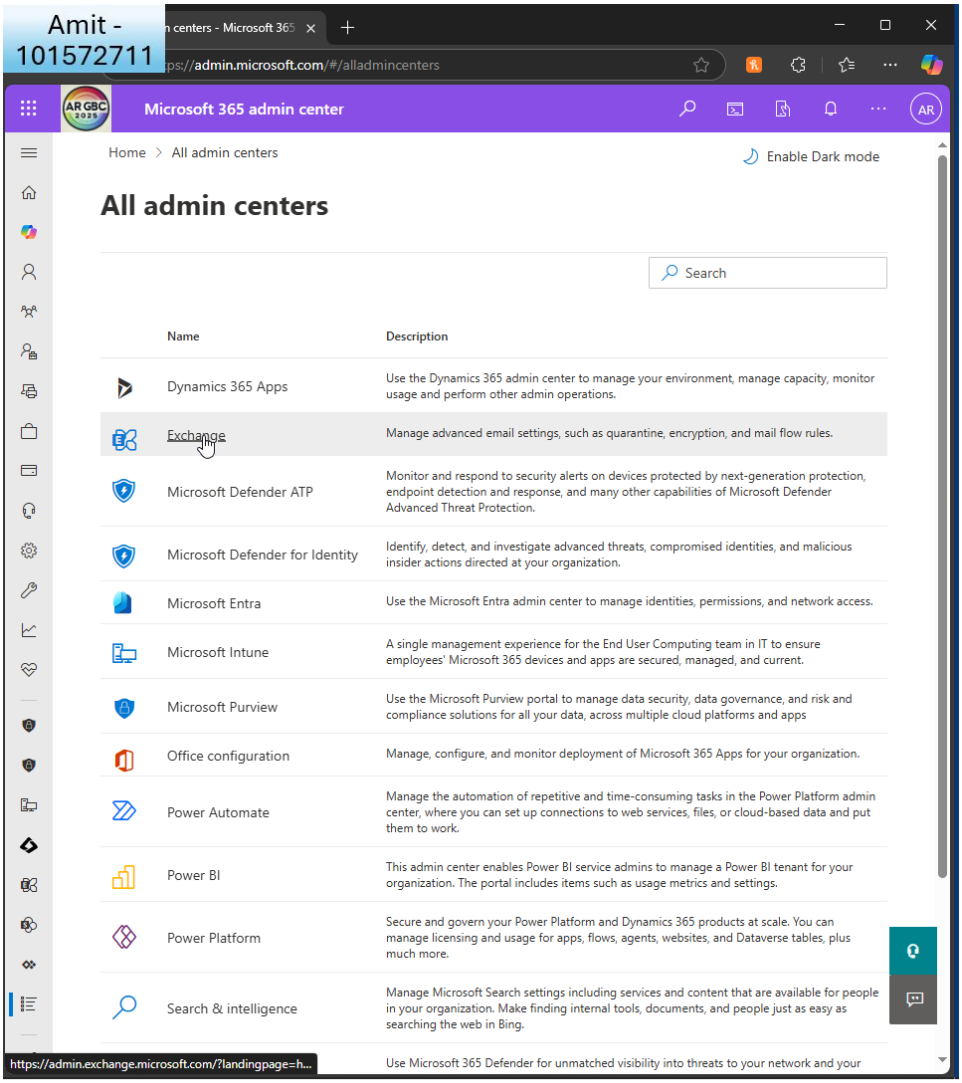
I see the confirmation

Student Name: ……. Term: ……..
Student ID: ……..

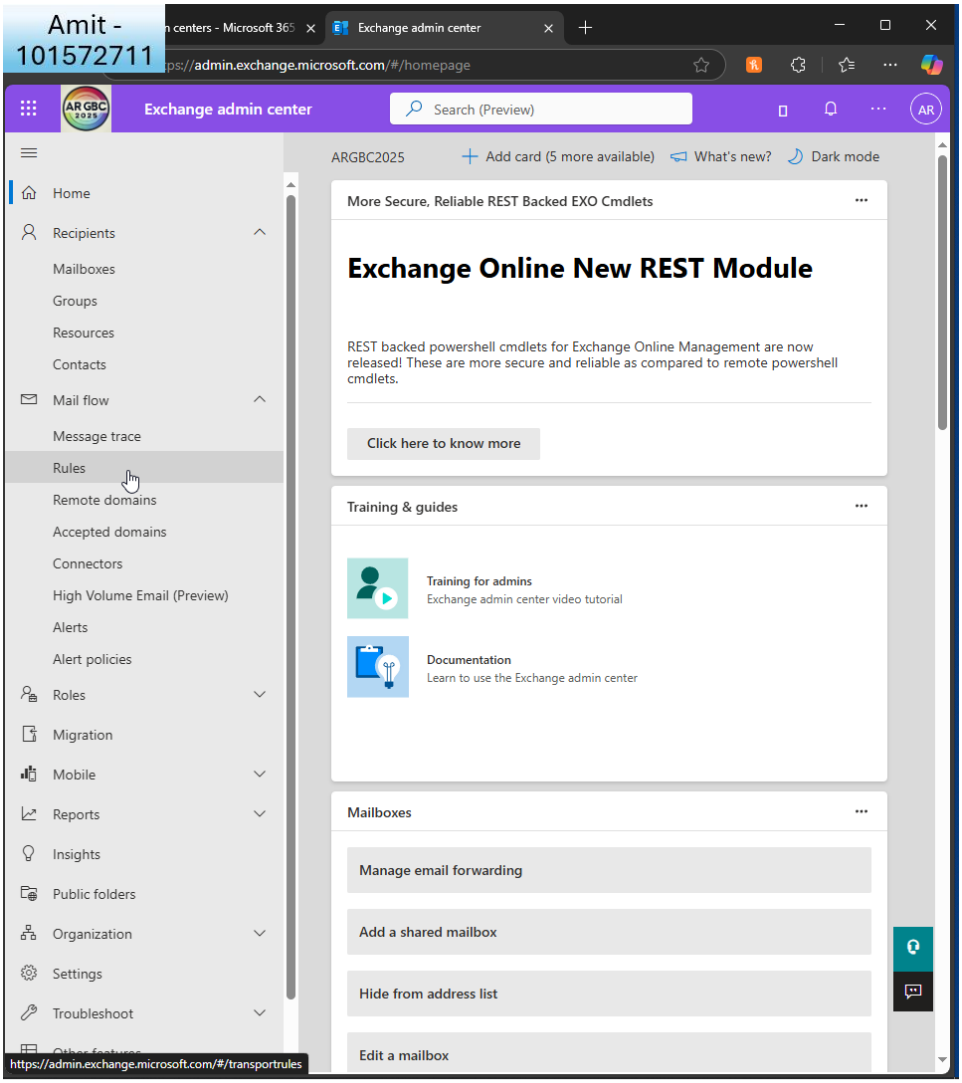
2. **Set Up Data Encryption**:

Part A:

- Configure Microsoft 365 Message Encryption.
- Ensure that emails from inside the organization are automatically encrypted. (Hints: Navigate to Exchange admin center, and then Rules)

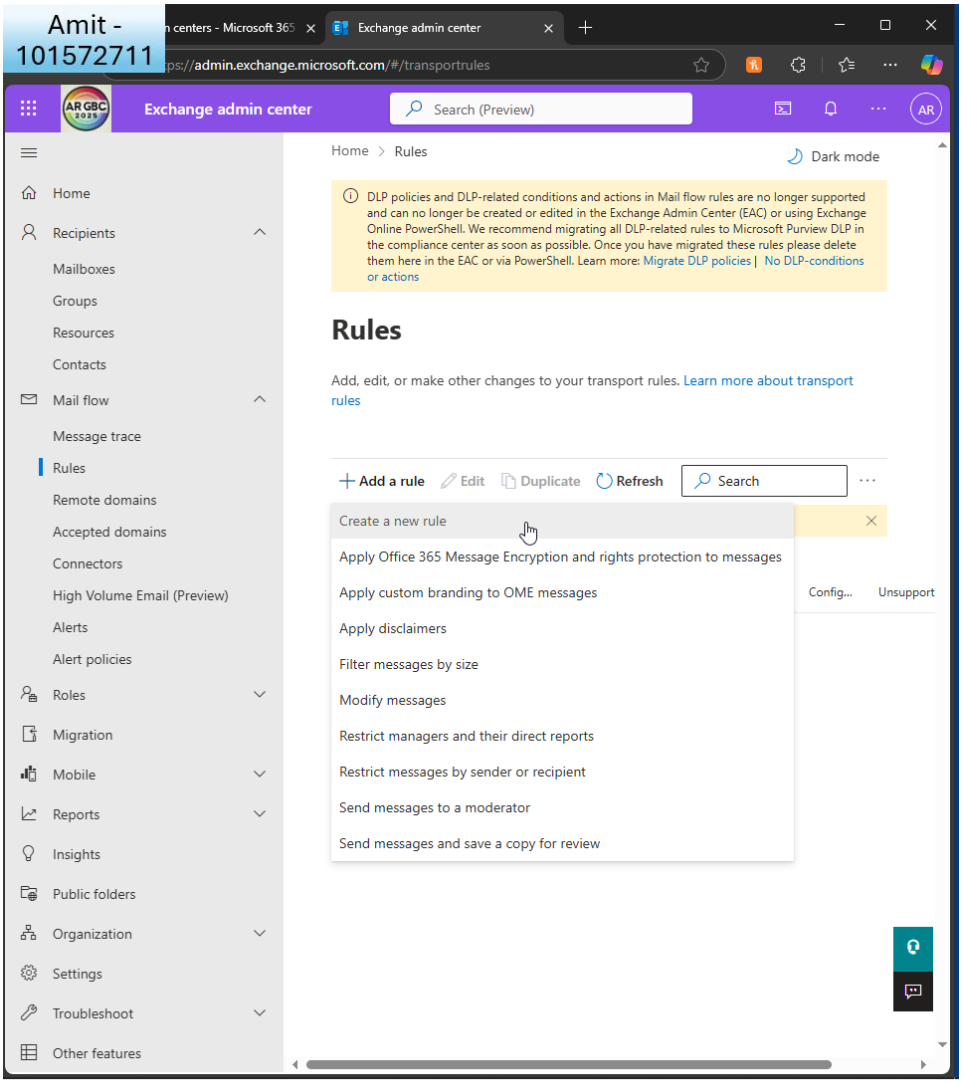


Student Name: ……. Term: ……..
Student ID: ……..



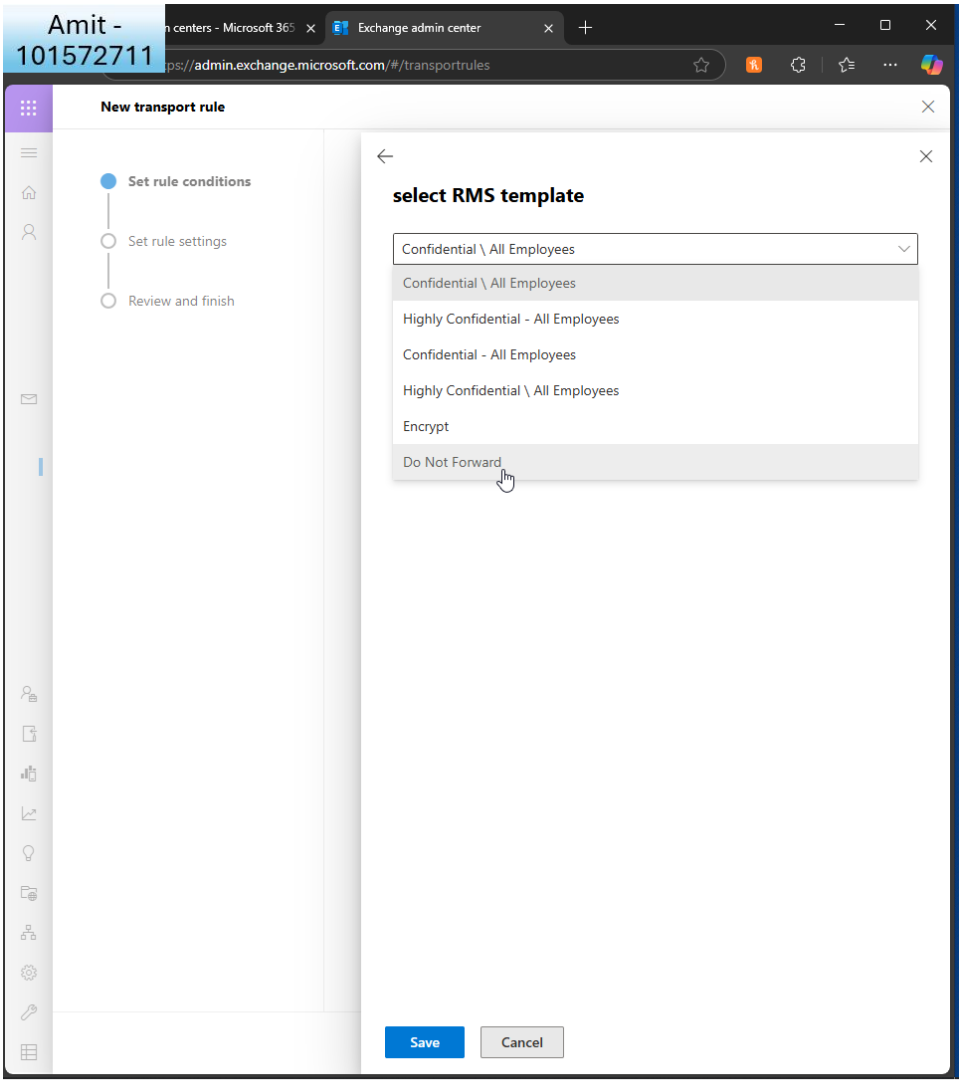
I click ’rules’ in Exchange admin centre

Student Name: ……. Term: ……..
Student ID: ……..



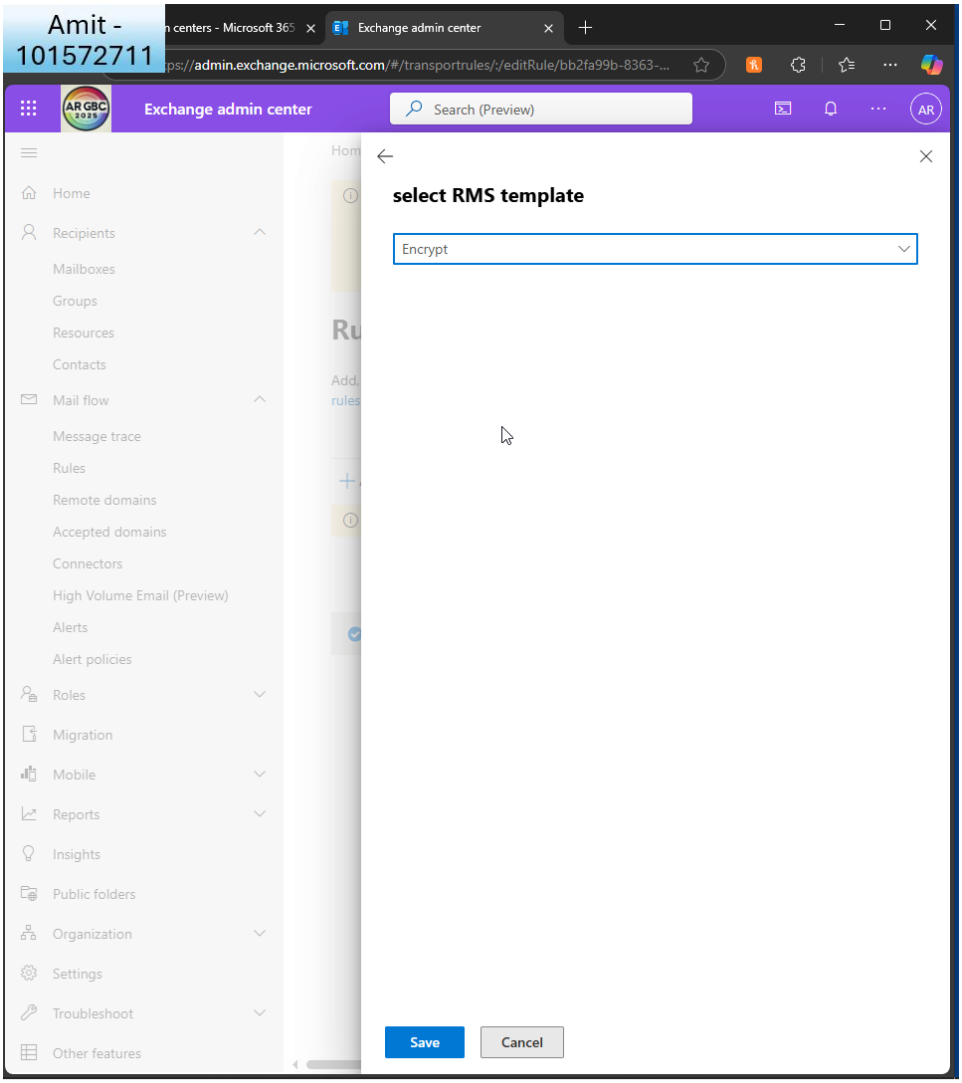
I create a new rule

Student Name: ……. Term: ……..
Student ID: ……..

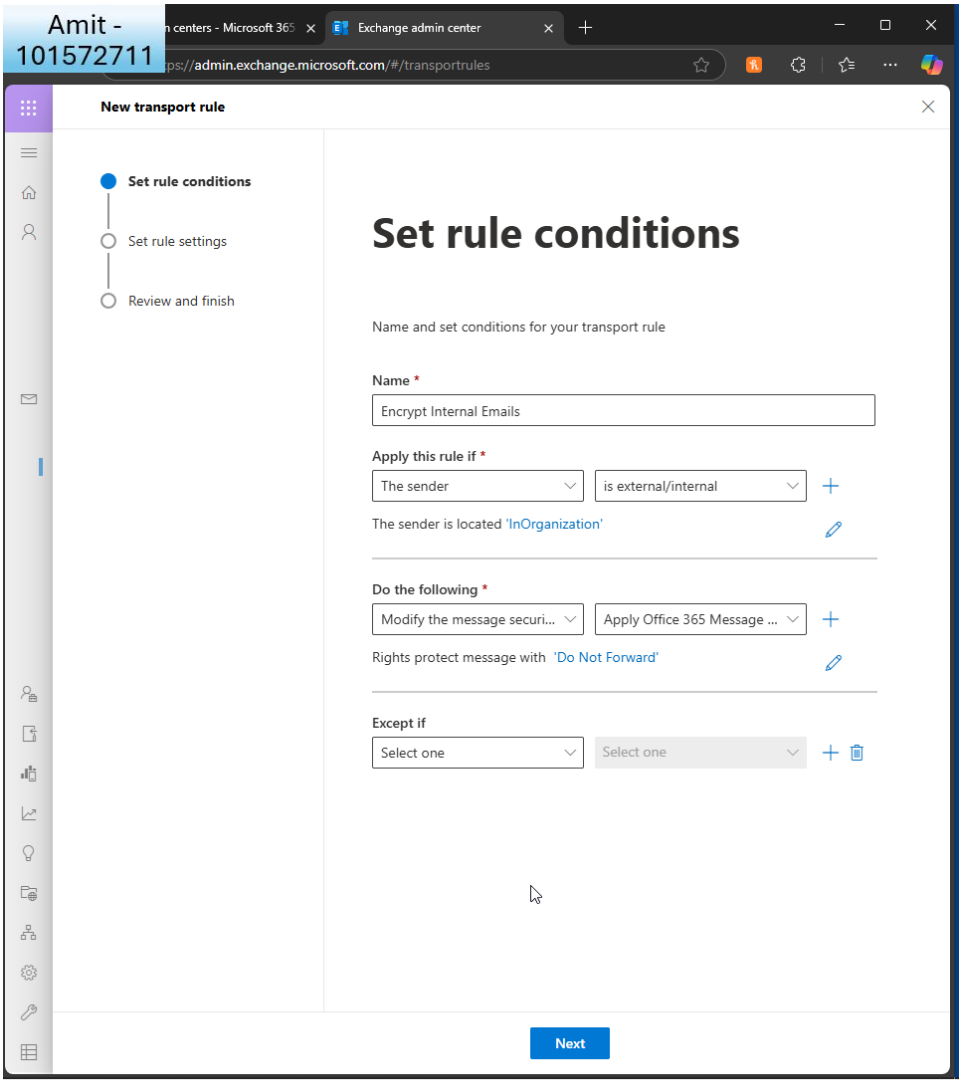


I set it so it doesn't forward (then changed it to 'encrypt' as per assignment rules - below)

Student Name: ……. Term: ……..
Student ID: ……..

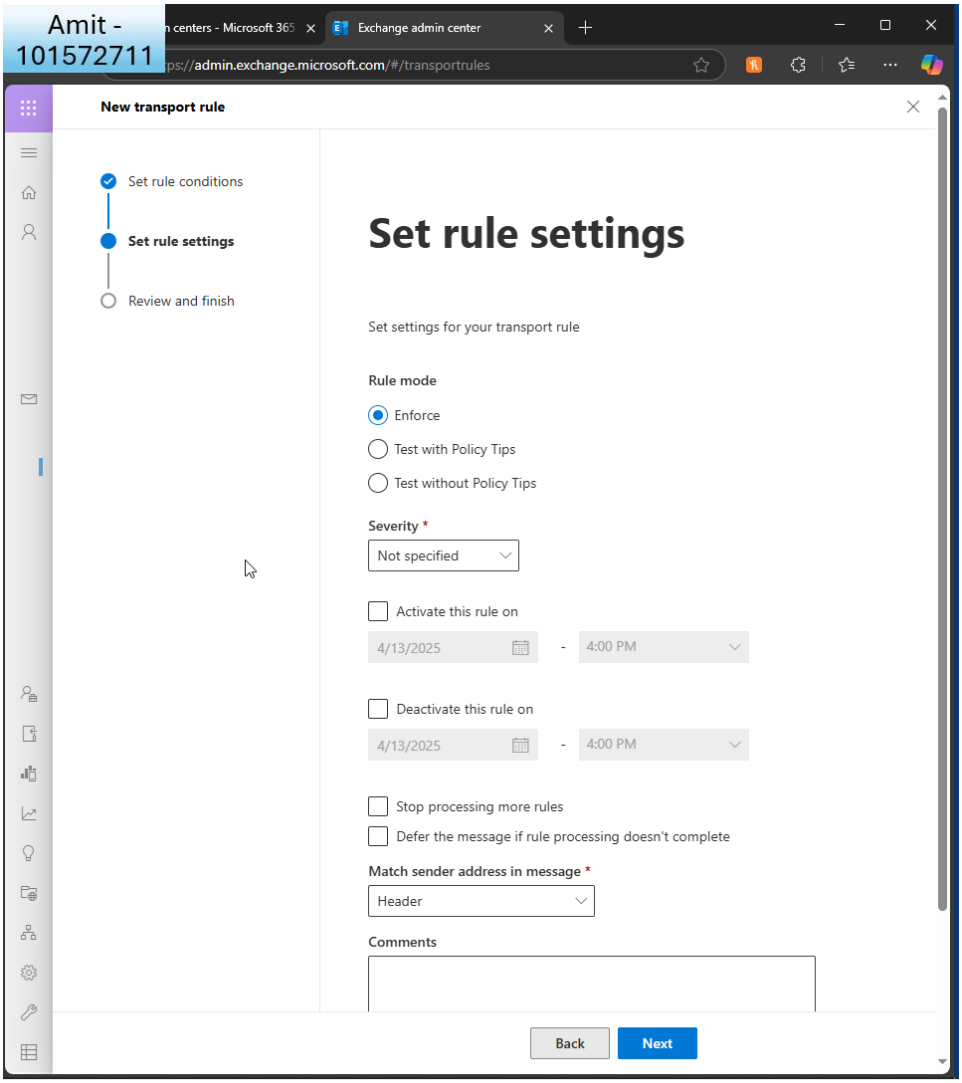


Student Name: ……. Term: ……..
Student ID: ……..



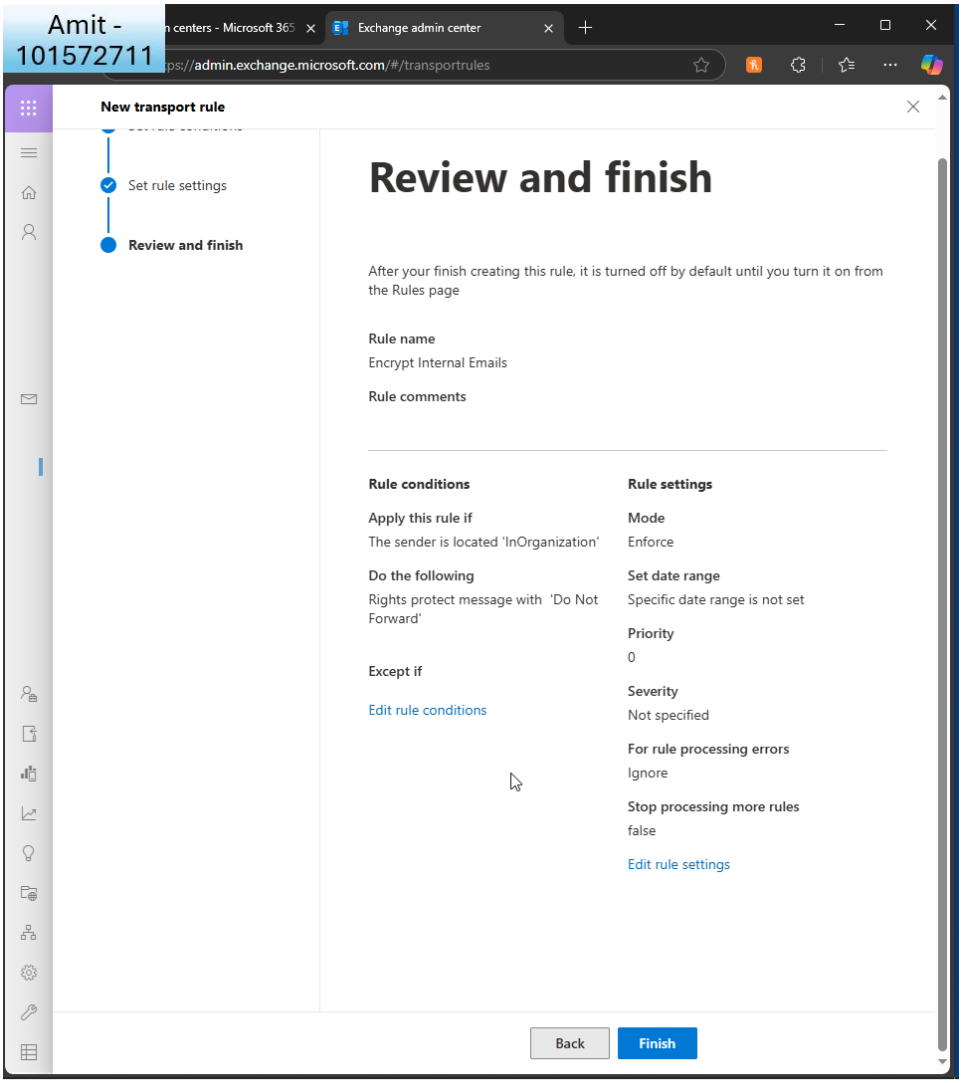
I set the conditions so if the sender is inside the organisation

Student Name: ……. Term: ……..
Student ID: ……..



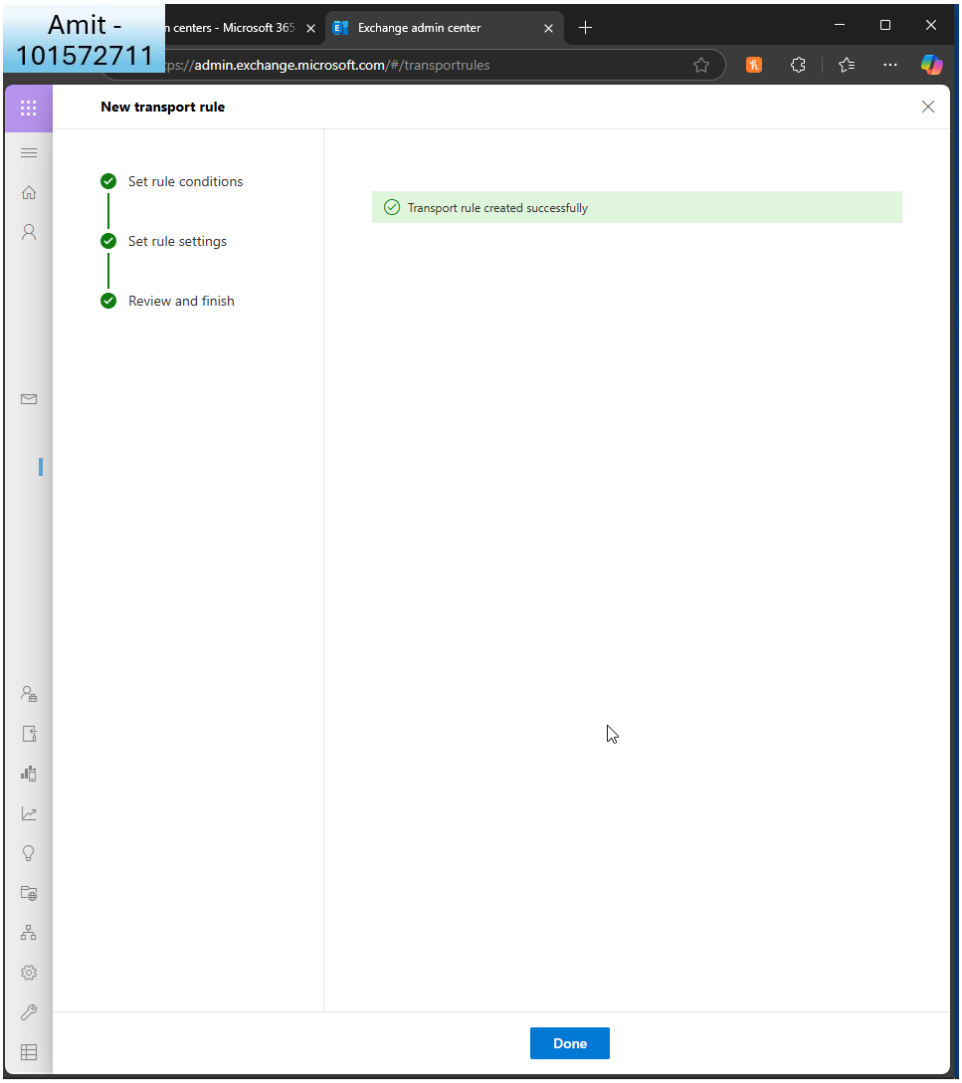
I enforce the policy

Student Name: ……. Term: ……..
Student ID: ……..



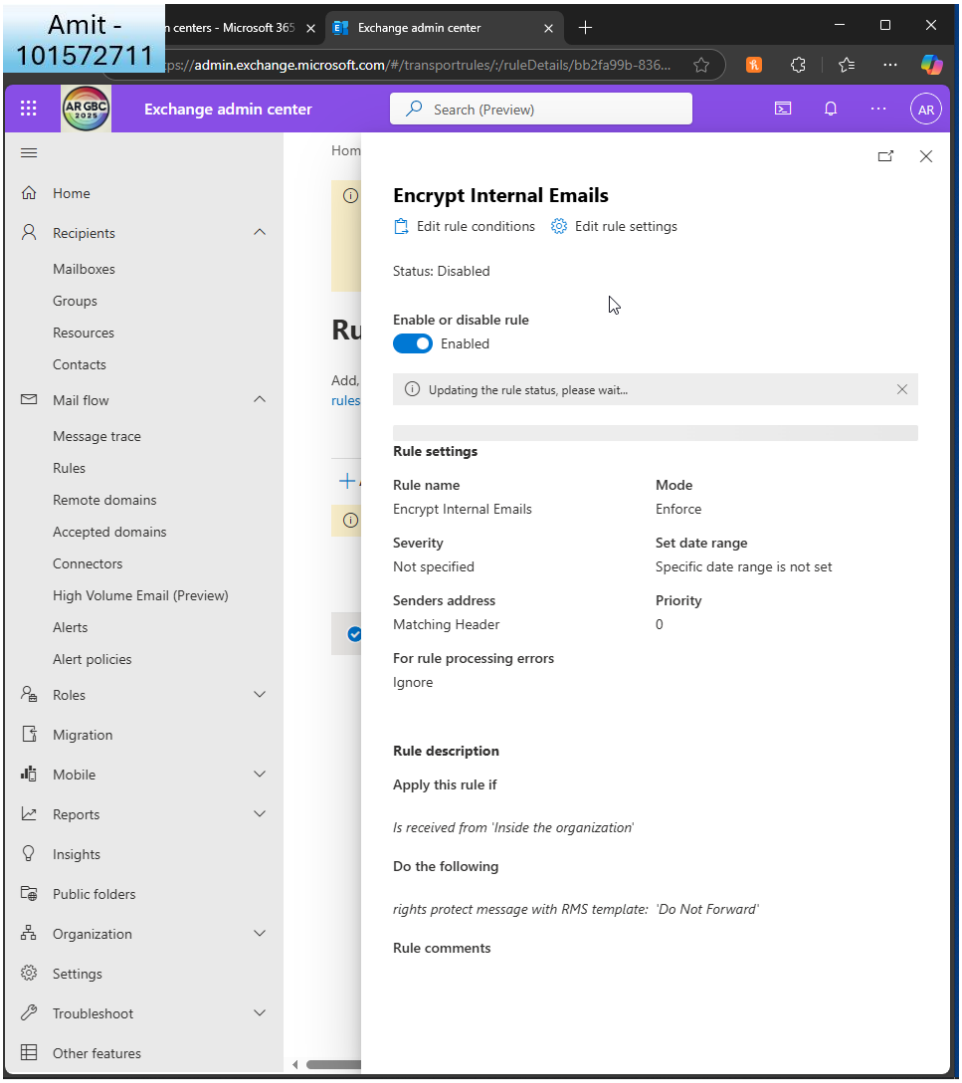
I review and finish

Student Name: ……. Term: ……..
Student ID: ……..



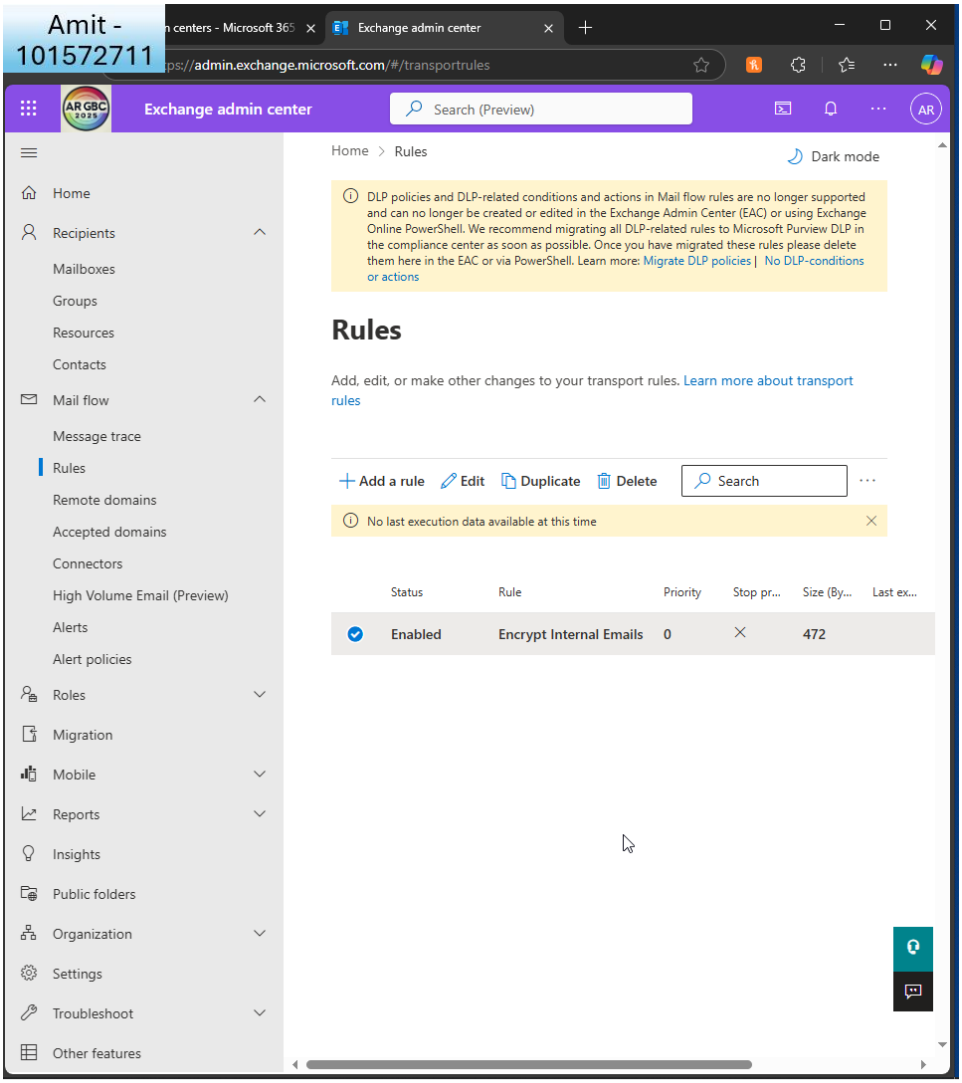
I see the confirmation

Student Name: ……. Term: ……..
Student ID: ……..



I enable the rule

Student Name: ……. Term: ……..
Student ID: ……..



I see the confirmation it's enabled.

Part B:

Task 2 involved enabling security features, and it was so cool to see how secure Microsoft 365 is! I started with Microsoft Defender and proceeded to enable Safe Links and Safe Attachments for all. I realised that a single malicious link or attachment could put the entire company at risk! This proves how important this part is.

Student Name: ……. Term: ……...
Student ID: ……..

Microsoft 365 Message Encryption was a nice first step. I created a rule to encrypt automatically all messages that went to others within the company, ensuring private messages remain secure without requiring users to do anything. It was nice to realise that changing rules a few times could provide good security for an entire company.

I liked the explanation that MS365 gives when it comes to creating policies in terms of how aggressive the policy needs to be. It's on a sliding scale, which is nice and user friendly.

There were a few issues with the exercise. The user interface is difficult to comprehend since the same settings are used for other admin user interfaces as well. It can be improved to make it easier for administrators to understand. I also noticed that when you create a rule, you have to manually enable it, it's not enabled by default.

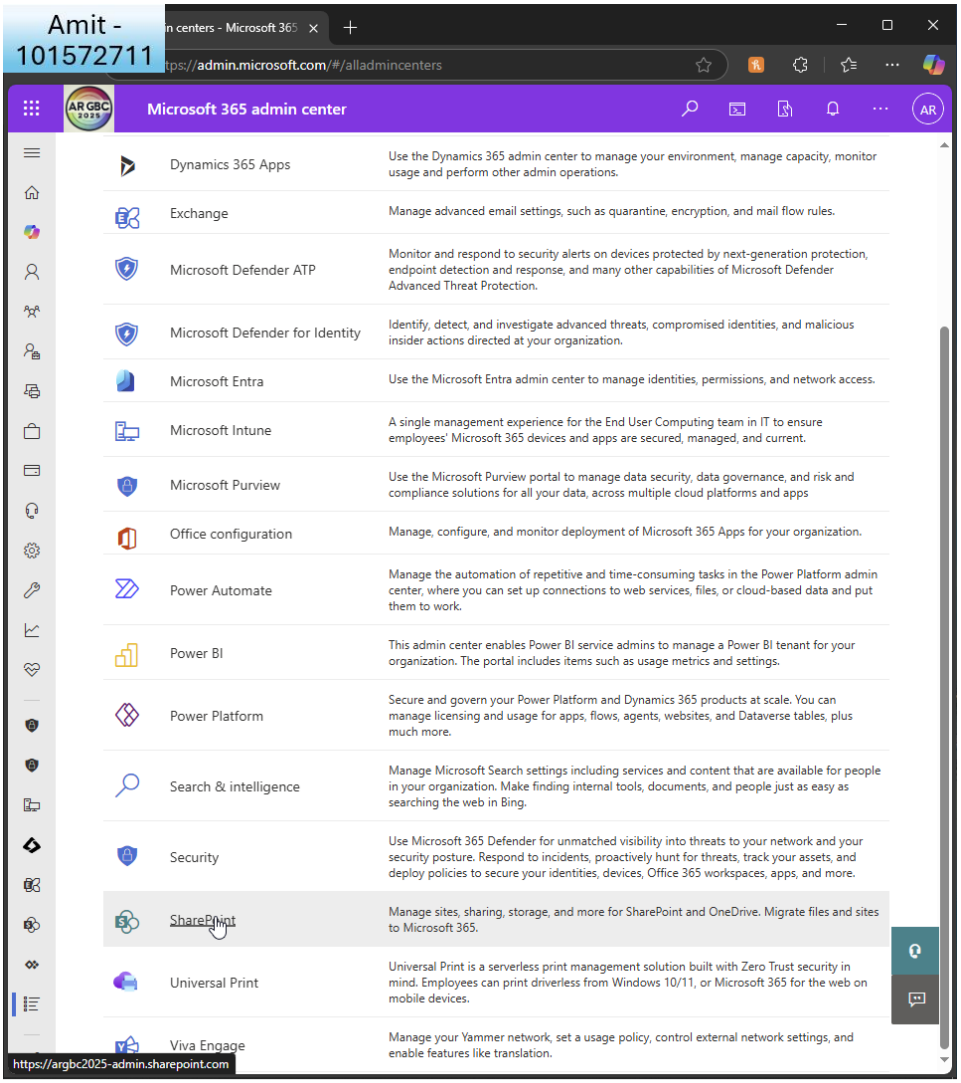
Nevertheless, through this exercise, I got to see how large corporations make and maintain security rules. I got to see how critical it is to safeguard communication and how wonderful it is to realise that one administrator could do this. The power!

Student Name: ……. Term: ……..
Student ID: ……..

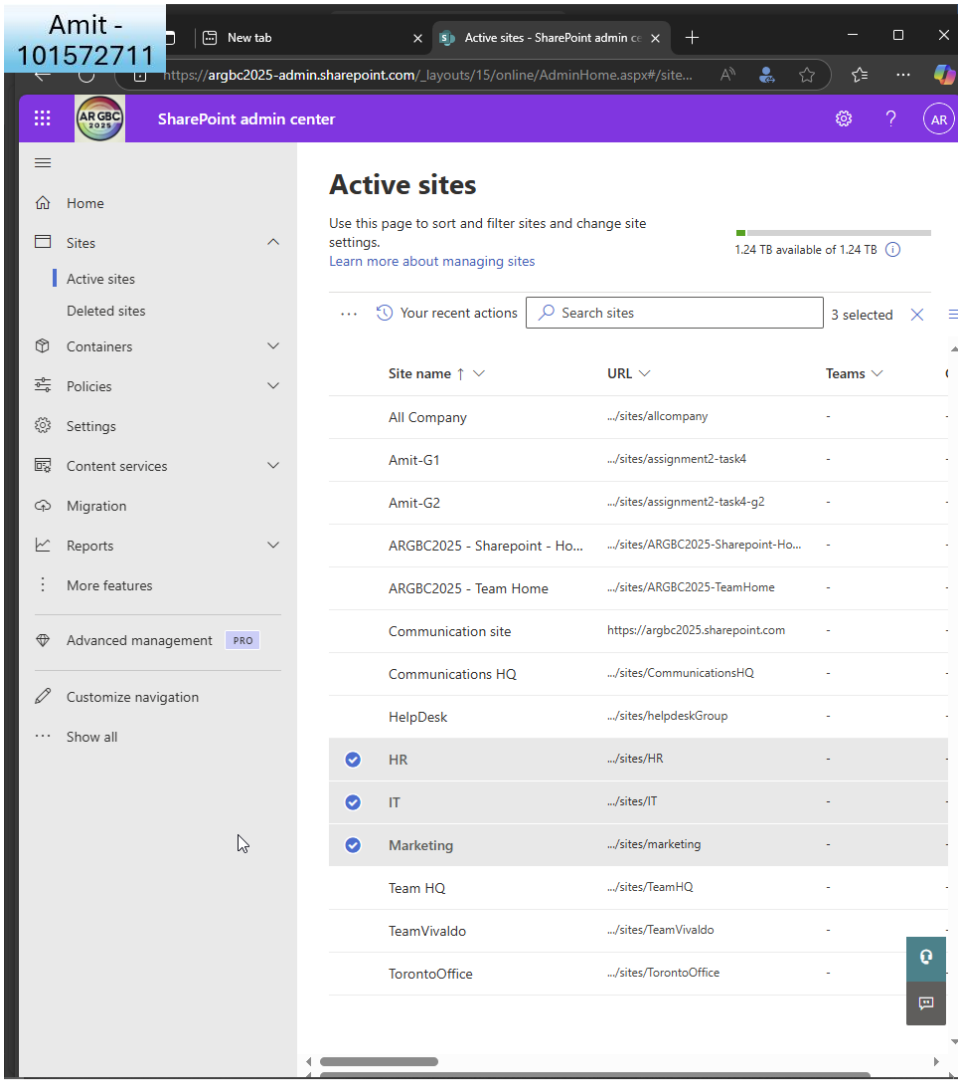
Task 3: Configuring and Managing Collaboration Tools

1. **Set Up SharePoint Online**:

   Create an online SharePoint site for each department (IT, HR, Marketing).

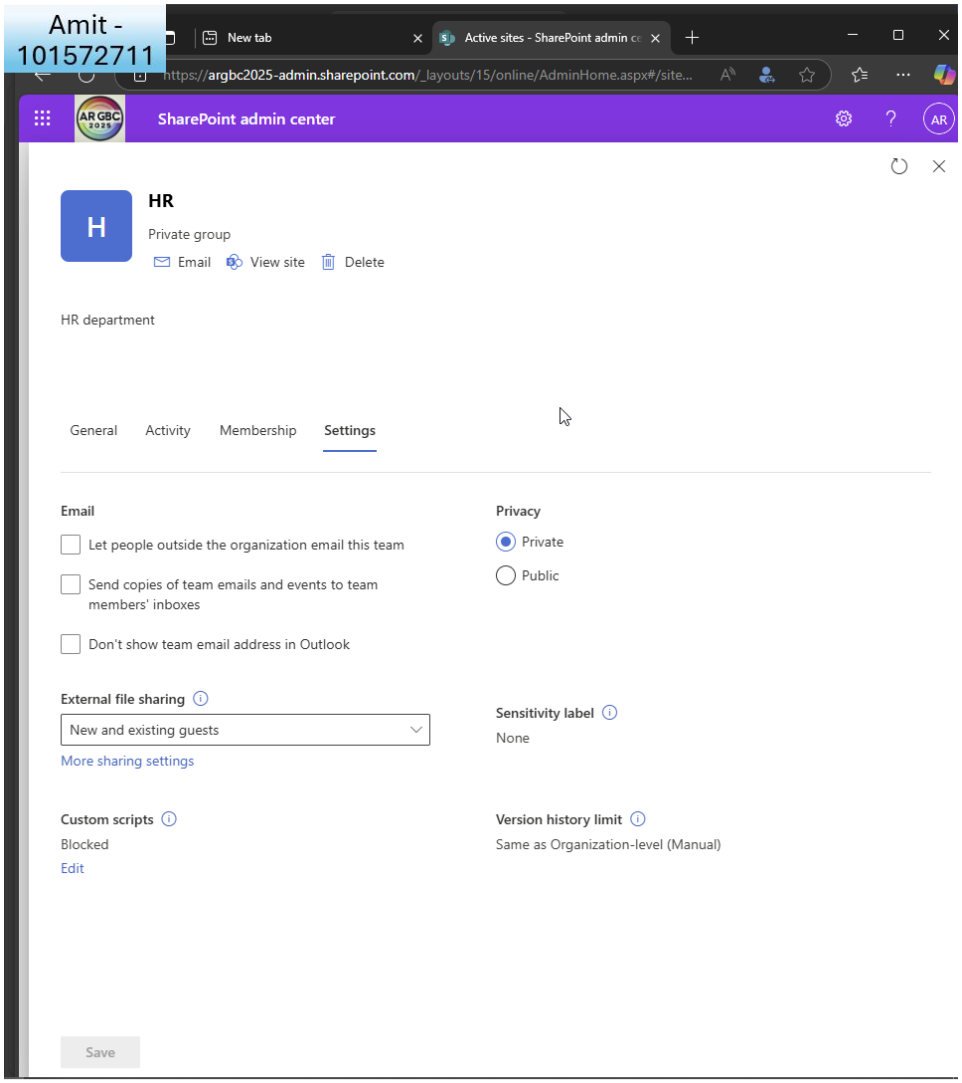


Student Name: ……. Term: ……..
Student ID: ……..



I create 3 sites in sharepoint to reflect the 3 different departments (HR, IT, Marketing)

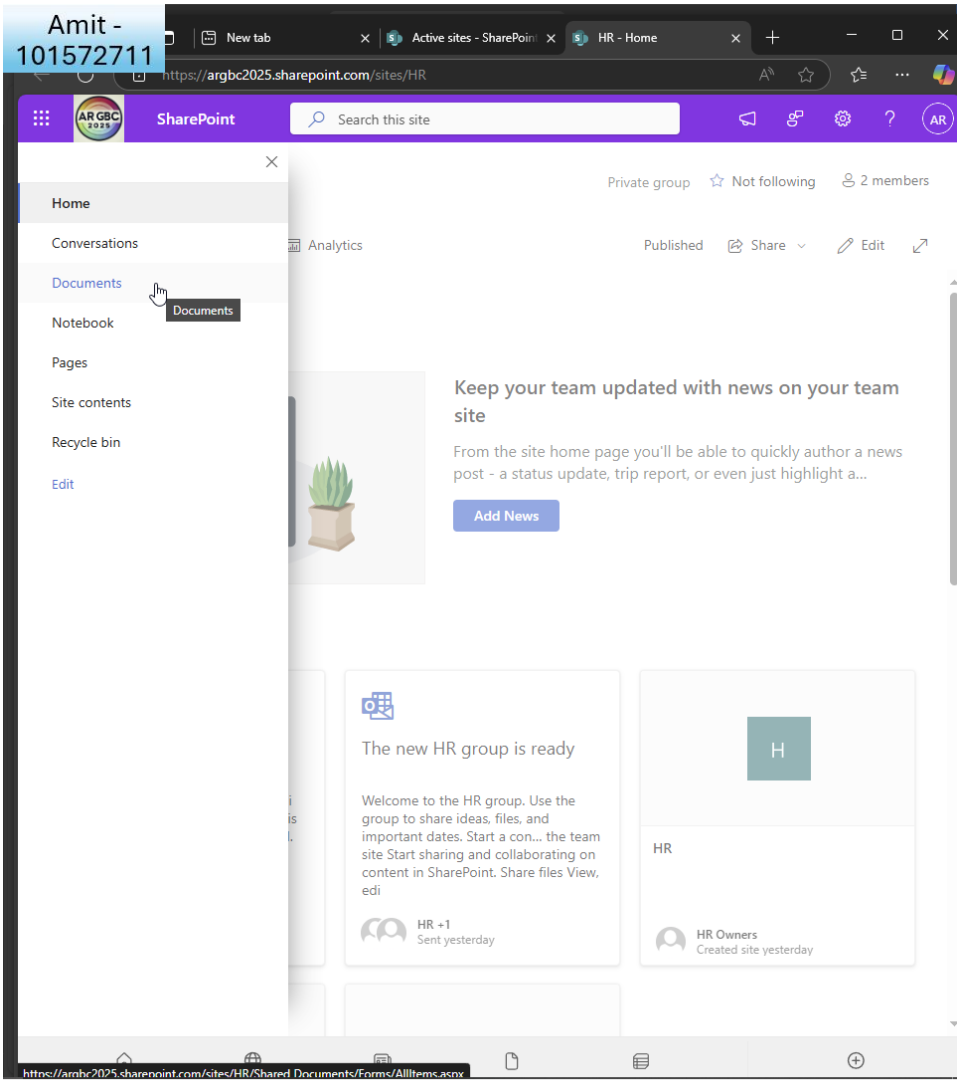
Student Name: ……. Term: ……..
Student ID: ……..



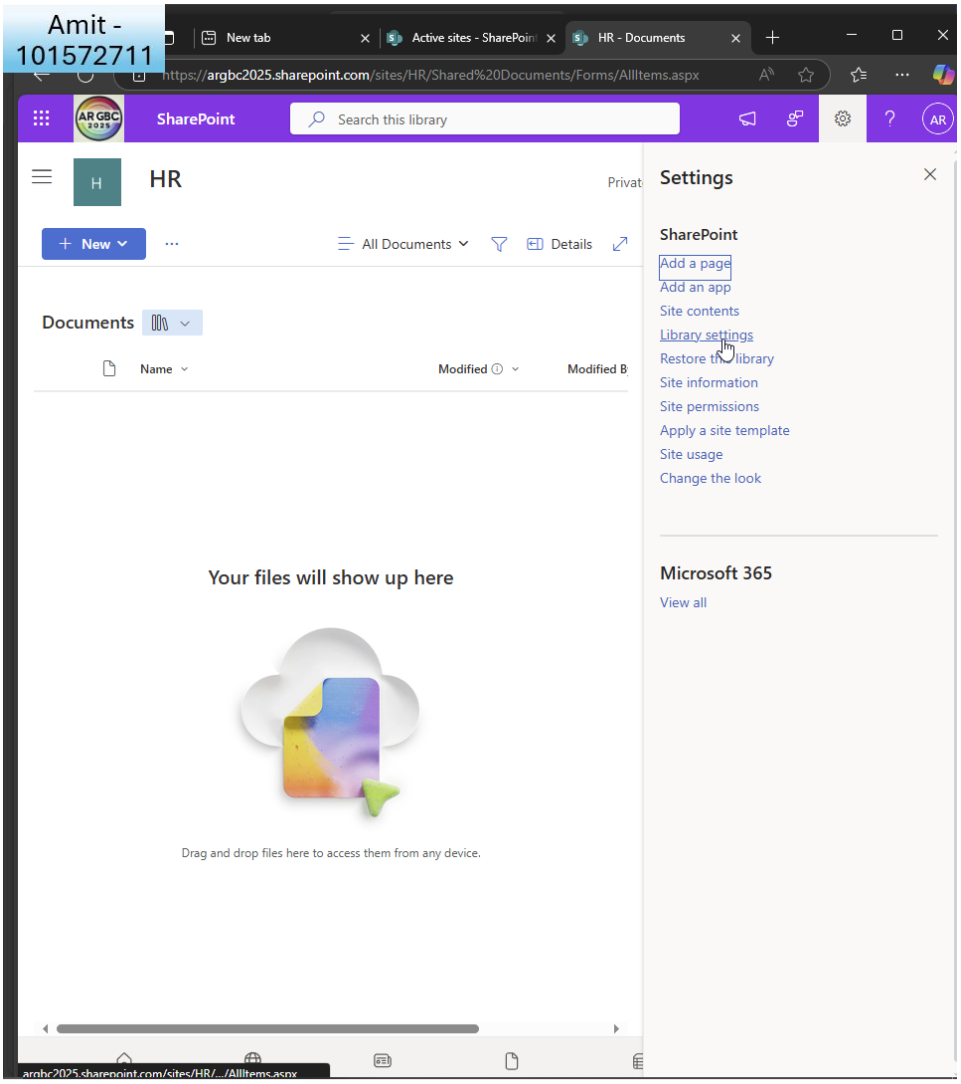
HR site

- Configure document libraries and permissions for each site.

Student Name: ……. Term: ……..
Student ID: ……..

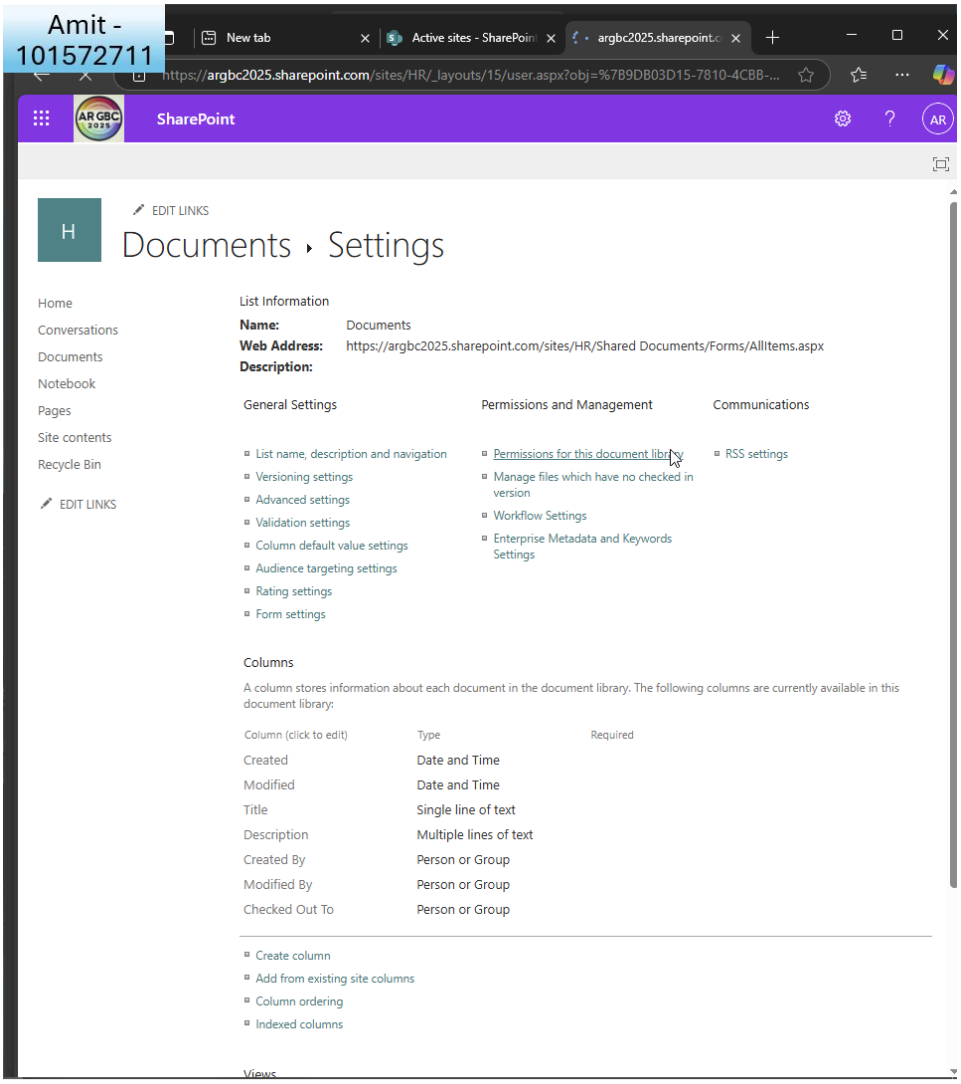


Student Name: ……. Term: ……..
Student ID: ……..



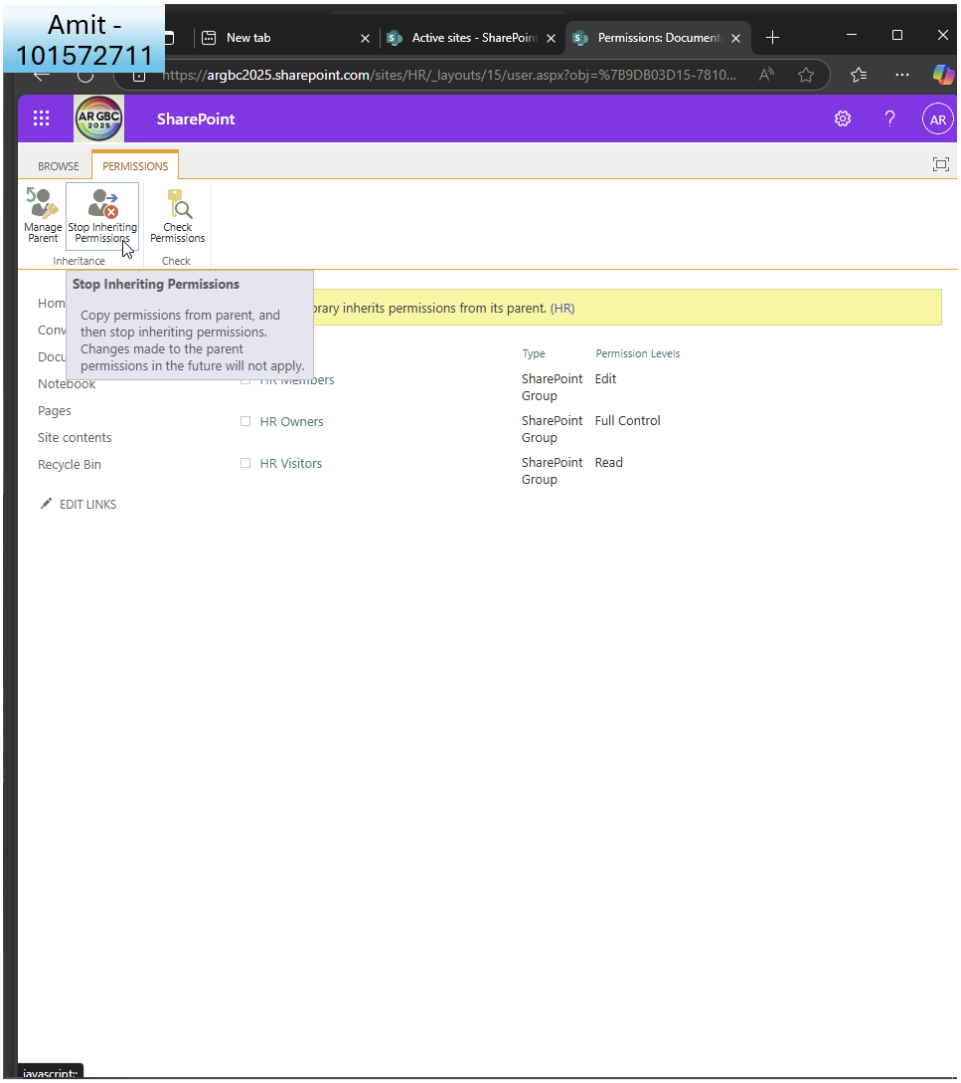
I click library settings within documents of the sharepoint site

Student Name: ……. Term: ……..
Student ID: ……..



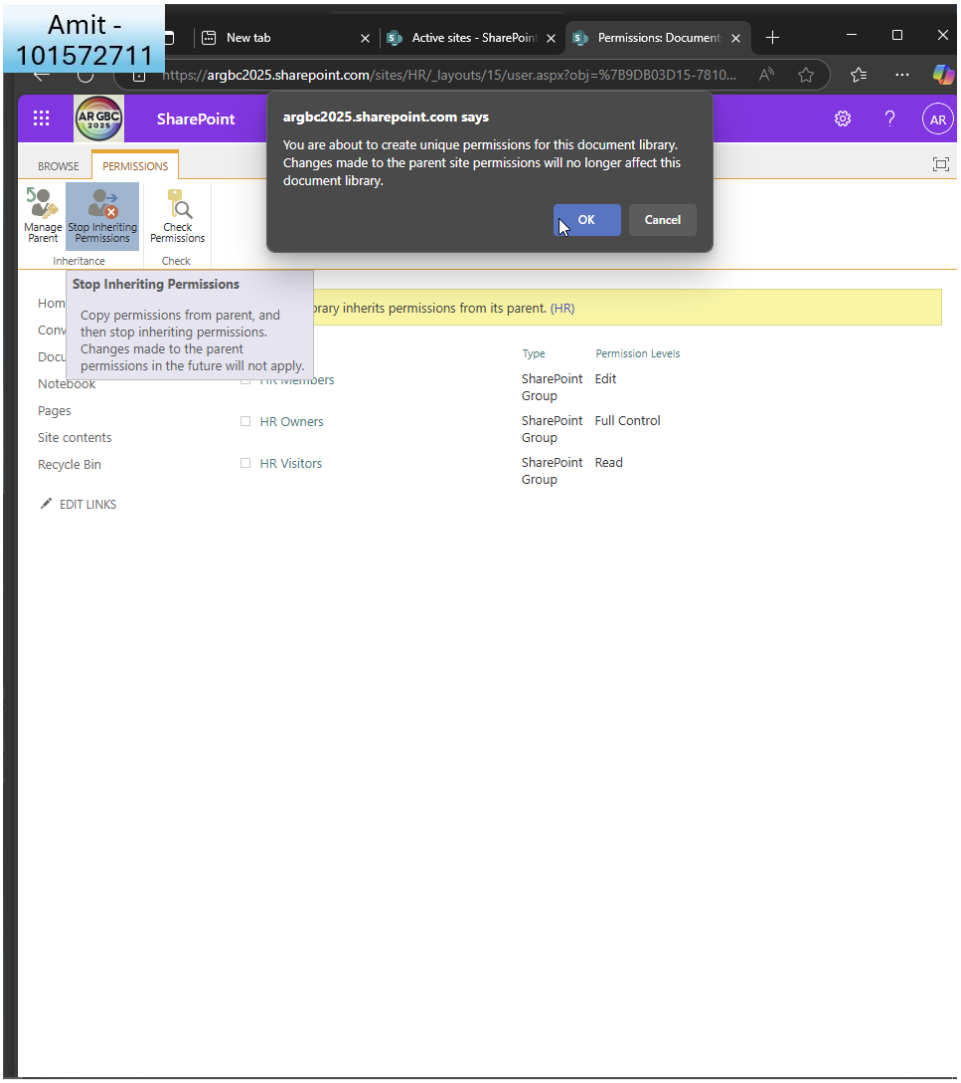
I click the permissions to edit them

Student Name: ……. Term: ……..
Student ID: ……..



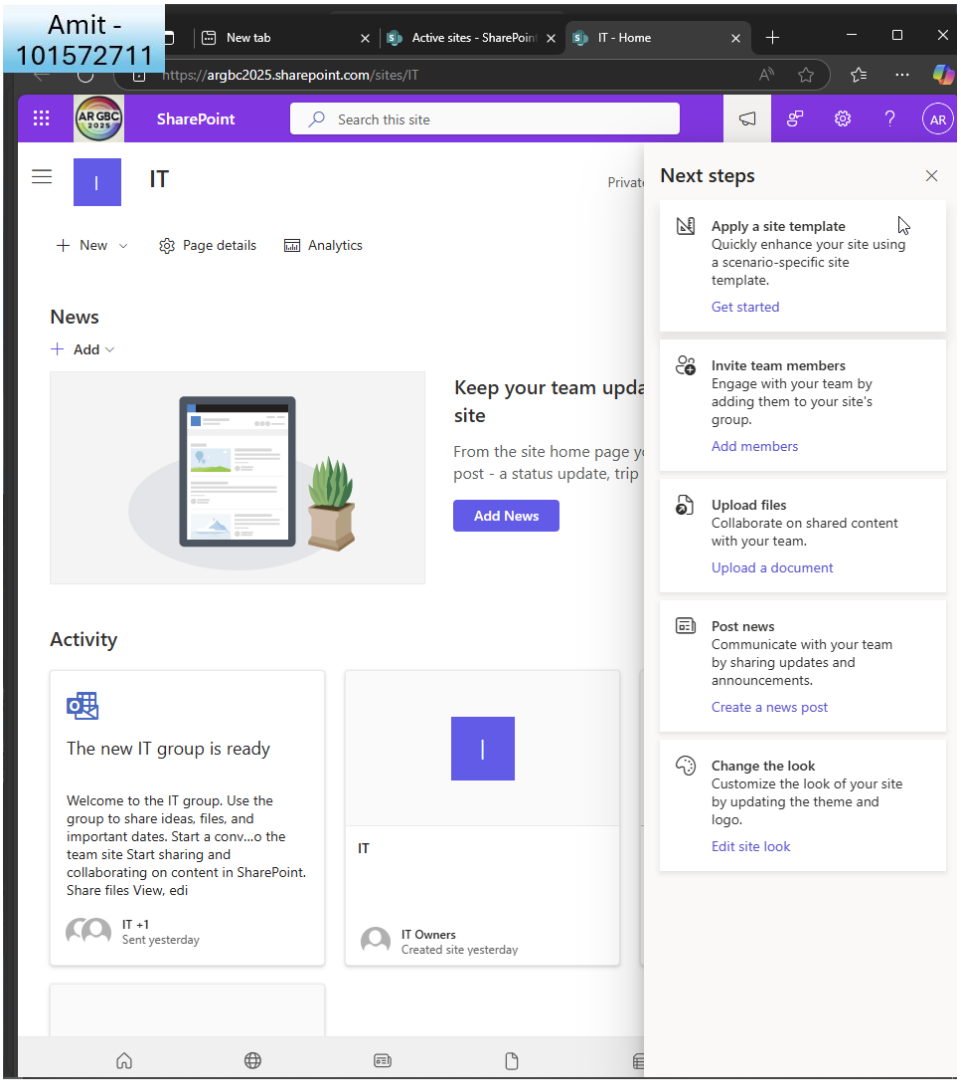
I click to step inheriting permissions

Student Name: ……. Term: ……..
Student ID: ……..



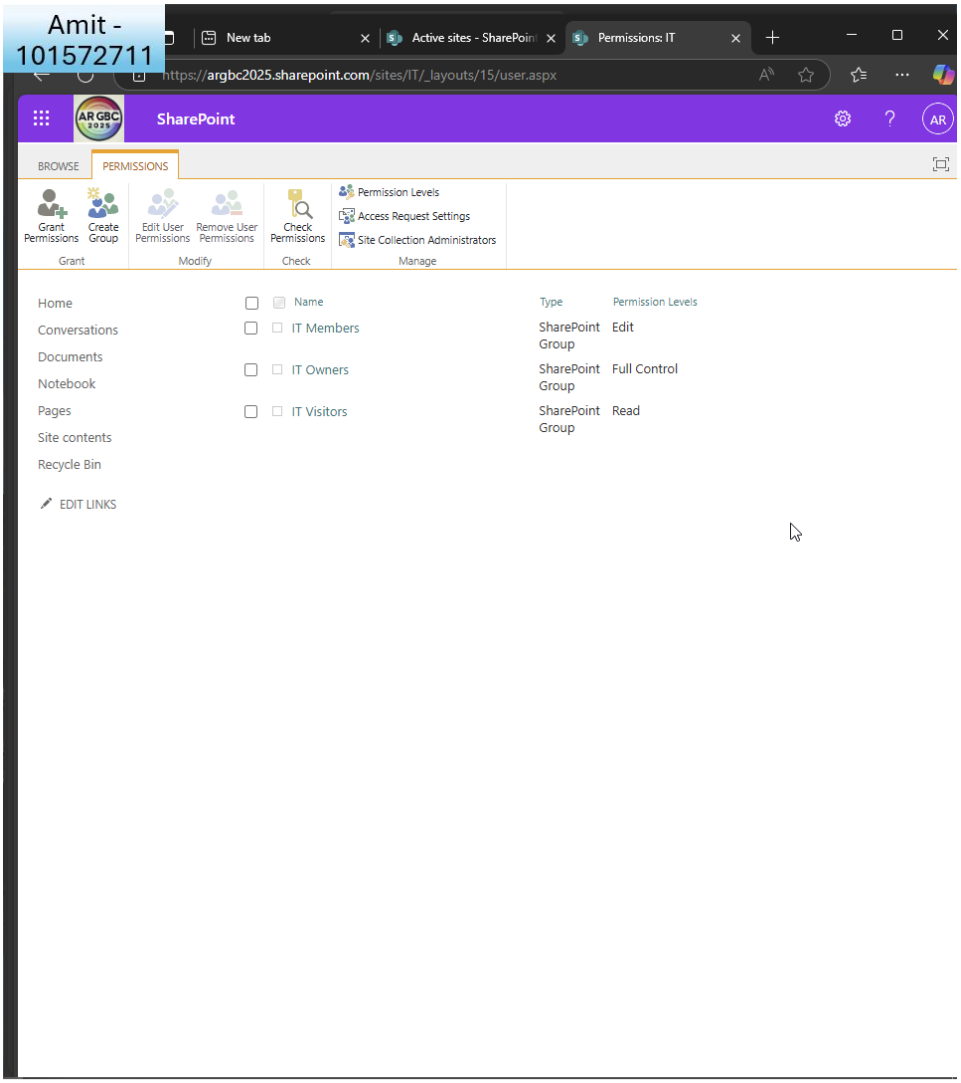
It gives me a warning via a popup

Student Name: ……. Term: ……..
Student ID: ……..



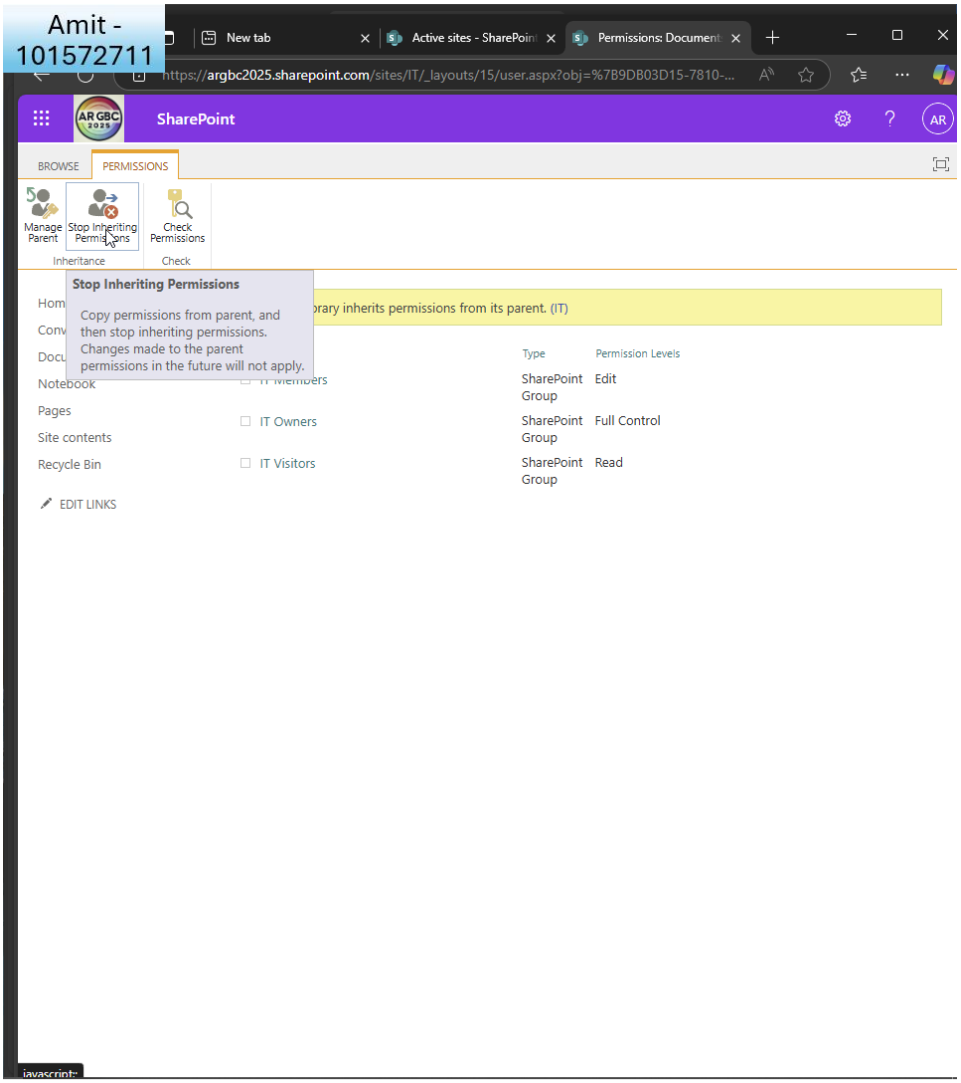
I do the same for IT department.

Student Name: ……. Term: ……..
Student ID: ……..



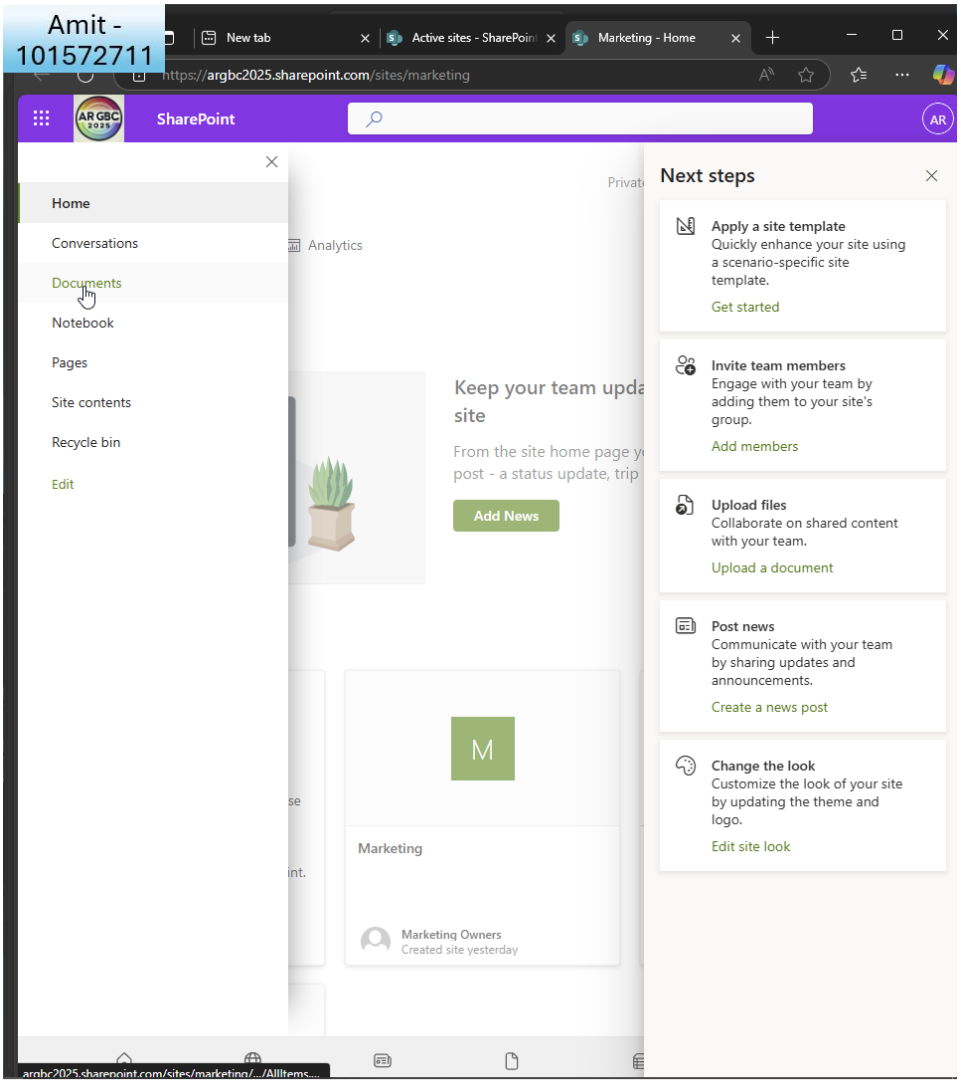
I see the permissions

Student Name: ……. Term: ……..
Student ID: ……..



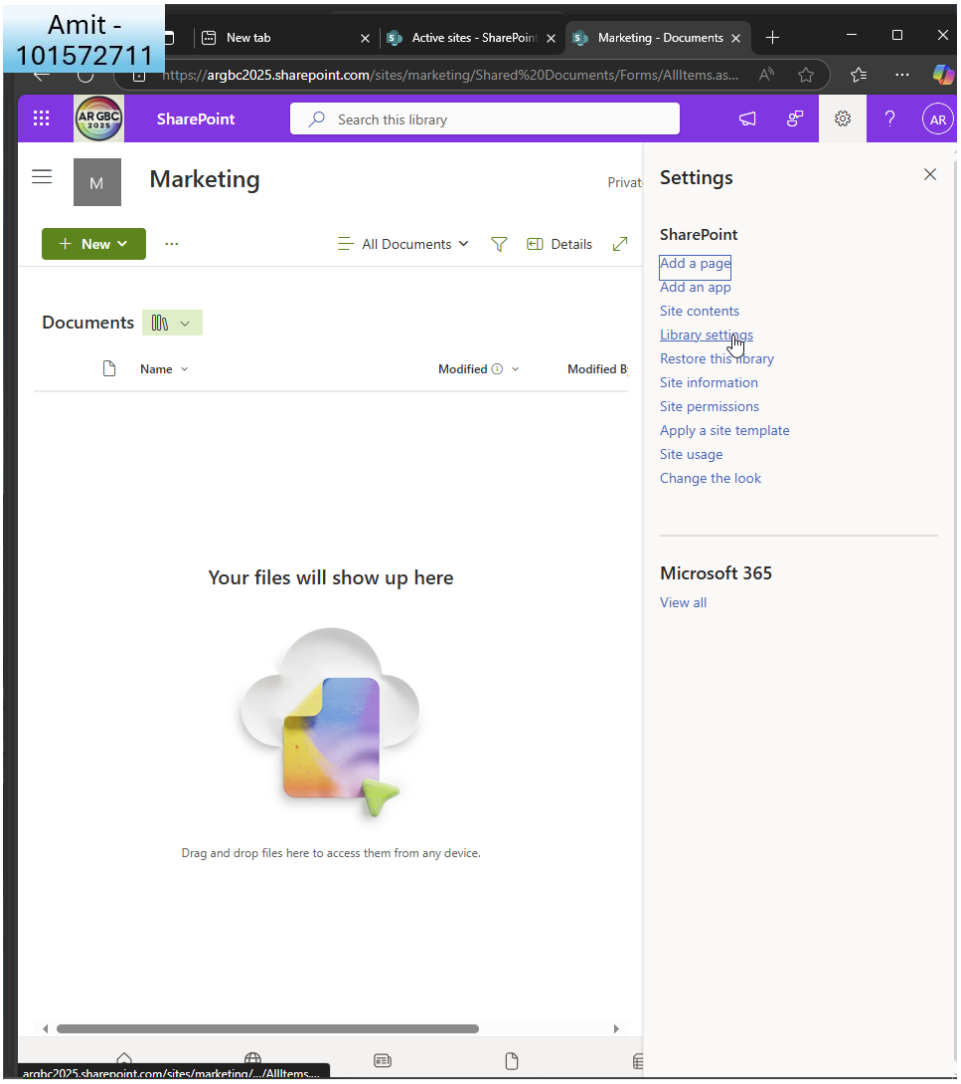
I click to stop inheriting permissions

Student Name: ……. Term: ……..
Student ID: ……..



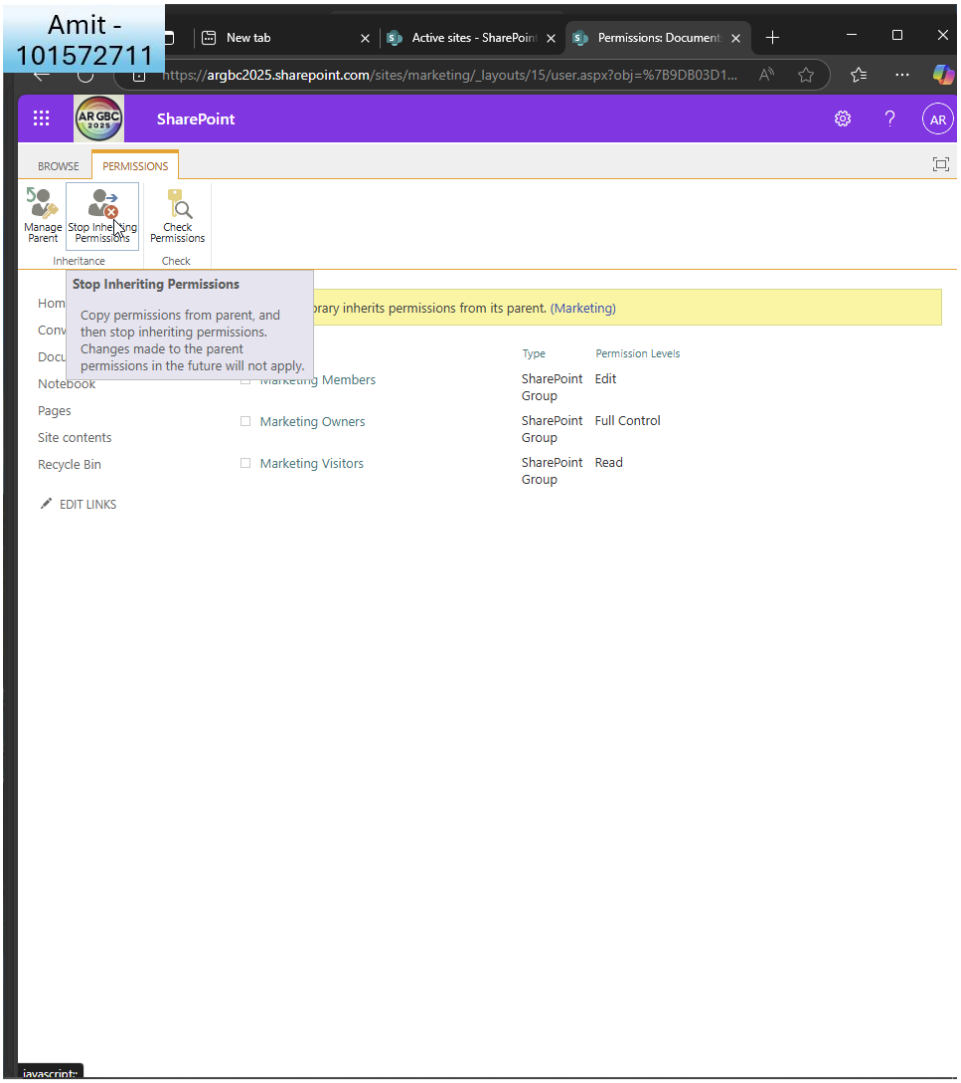
I do the same for the marketing site

Student Name: ……. Term: ……..
Student ID: ……..



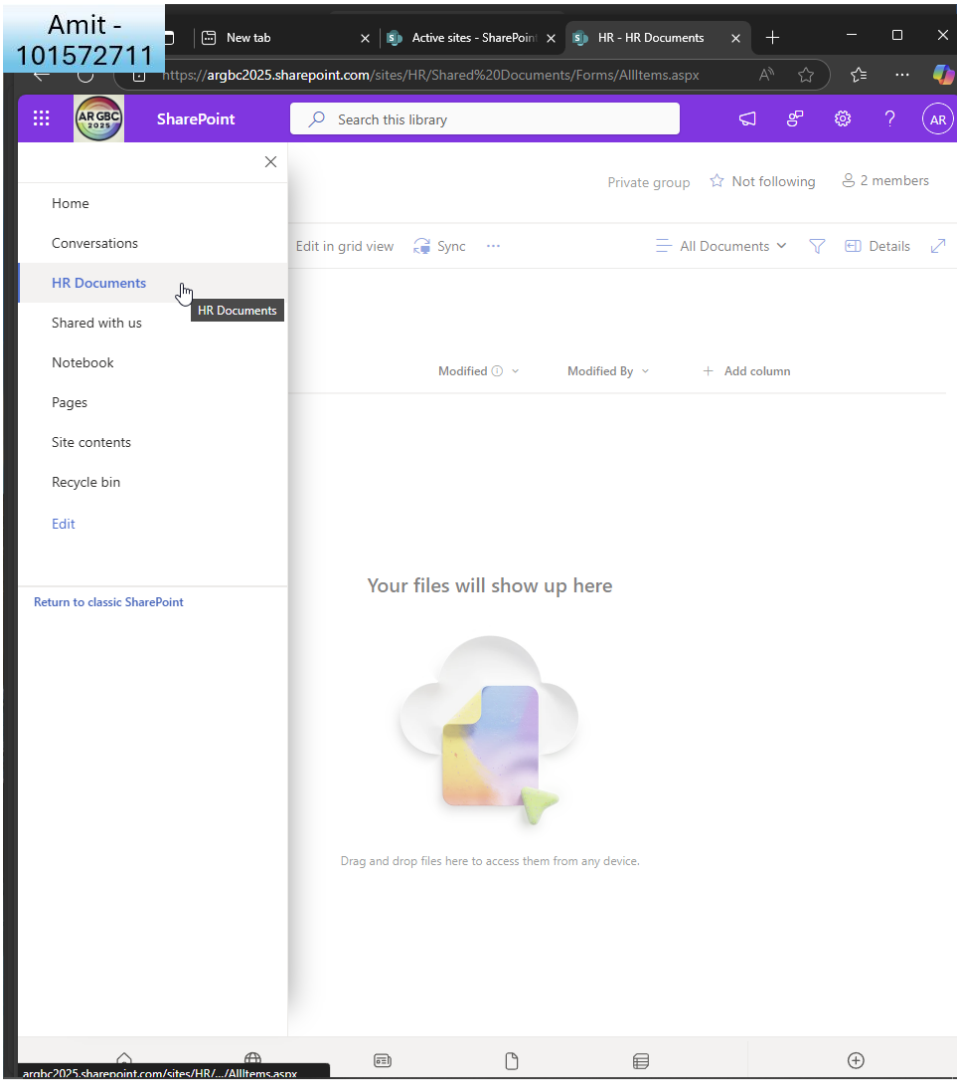
I click the library settings

Student Name: ……. Term: ……..
Student ID: ……..



I stop inheriting permissions once more

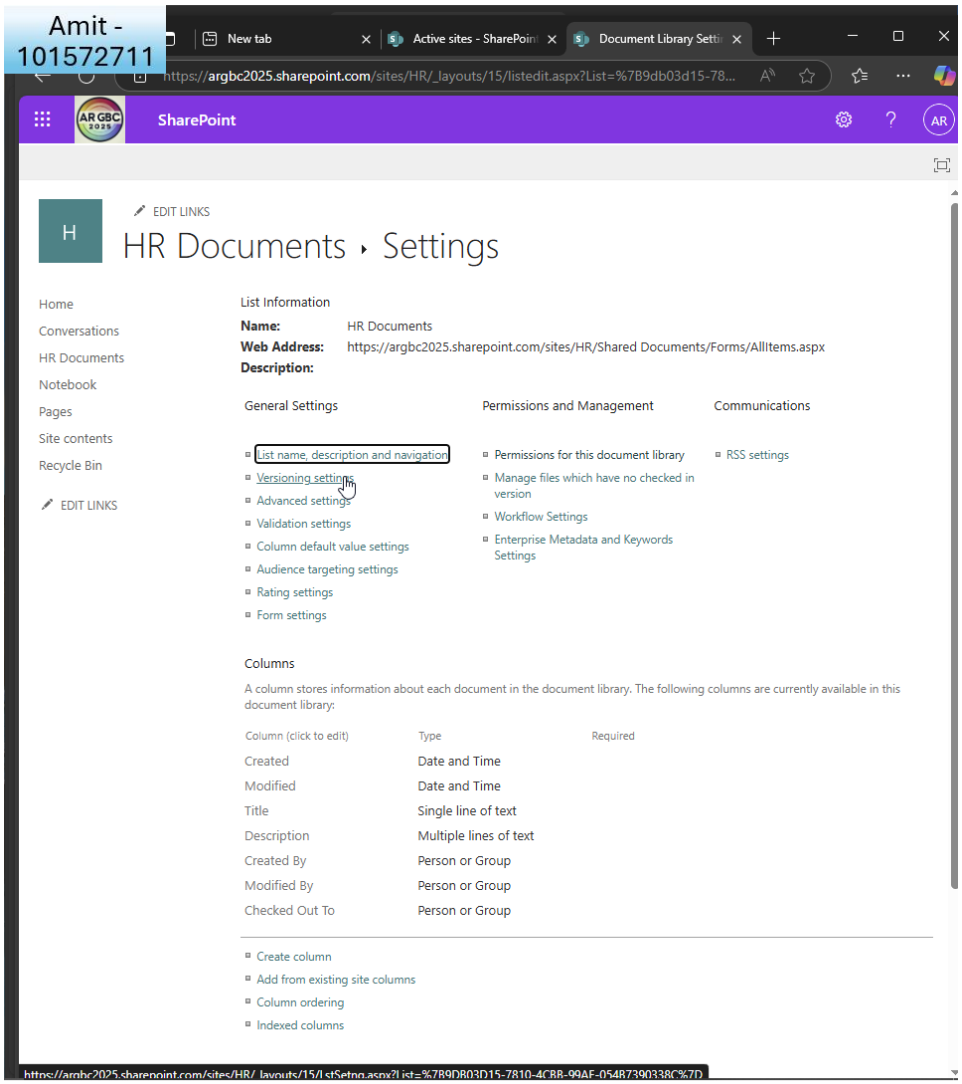
Student Name: ……. Term: ……..
Student ID: ……..



I also rename the documents to 'HR documents' for organisation

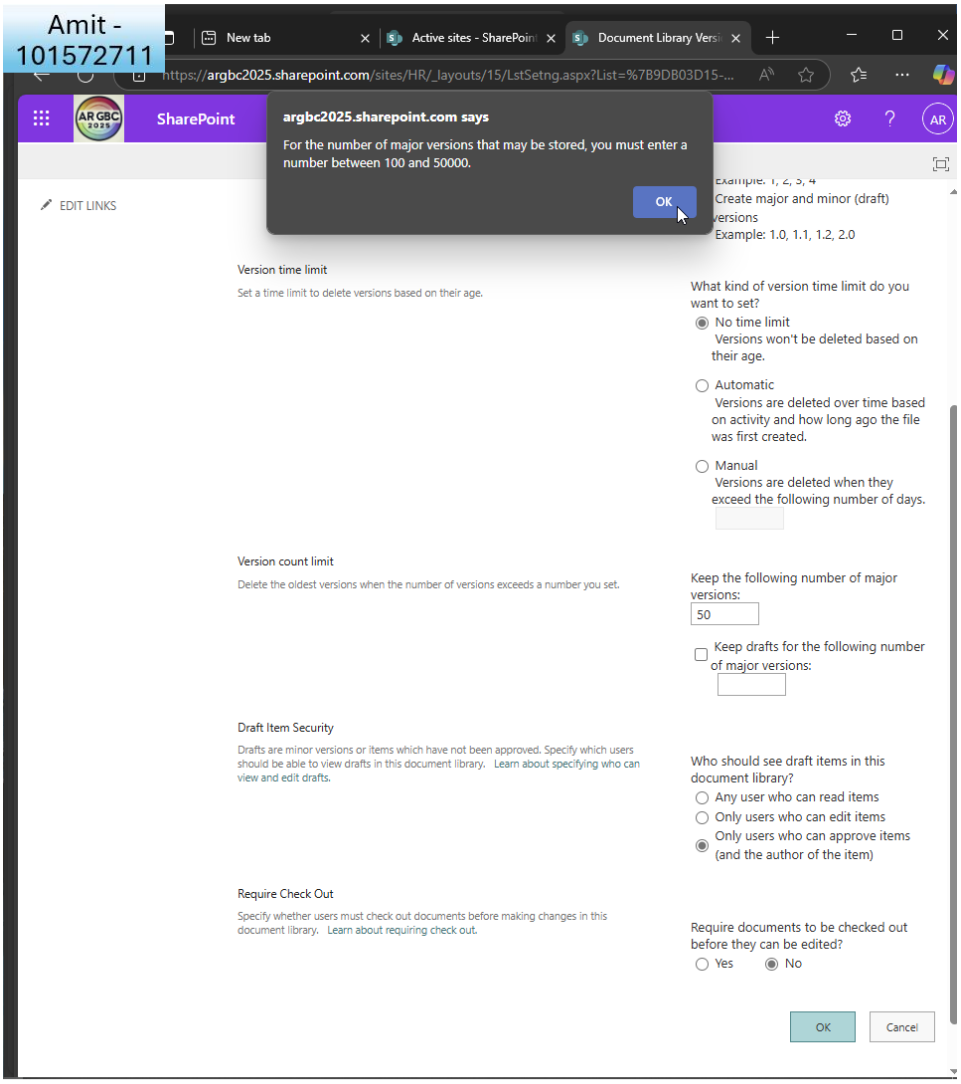
Student Name: ……. Term: ……..
Student ID: ……..

- Enable versioning and content approval for the HR document library.



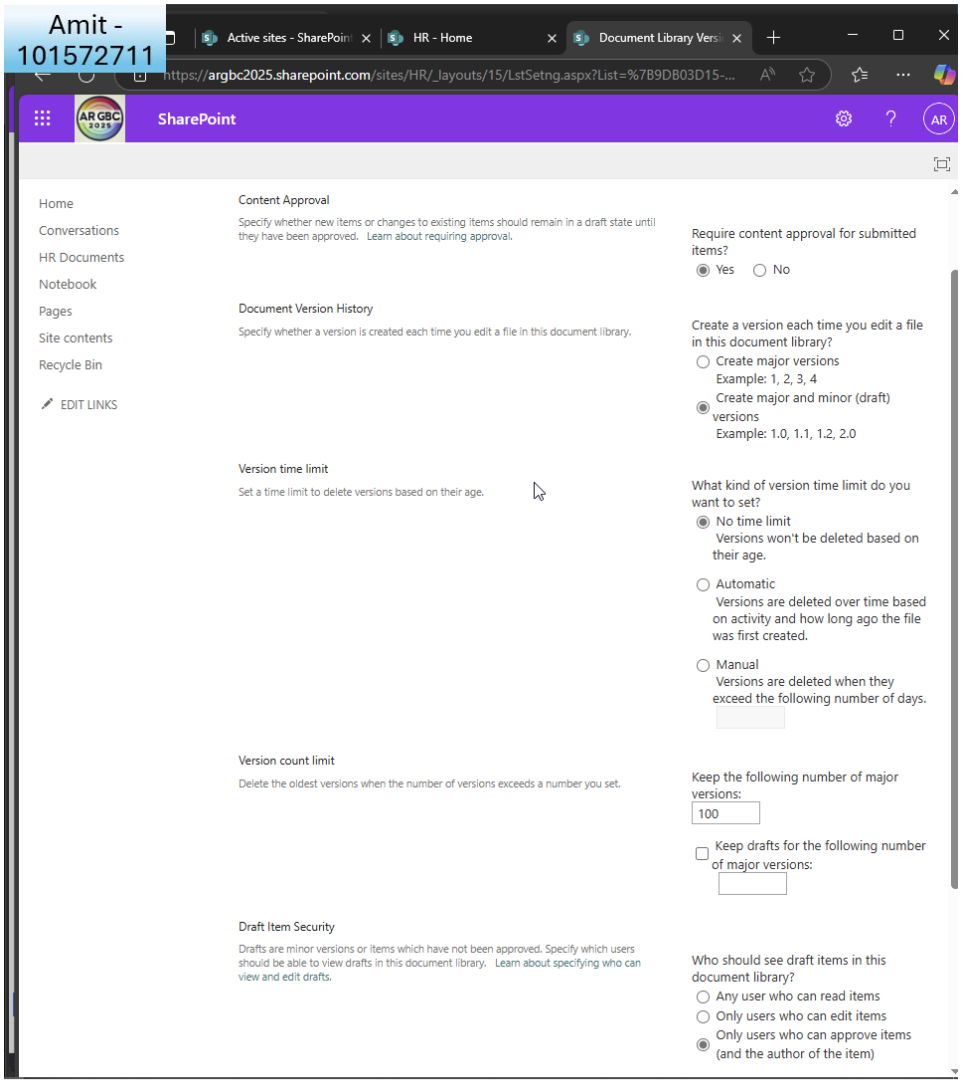
whilst in the document settings I click versioning settings

Student Name: ……. Term: ……..
Student ID: ……..



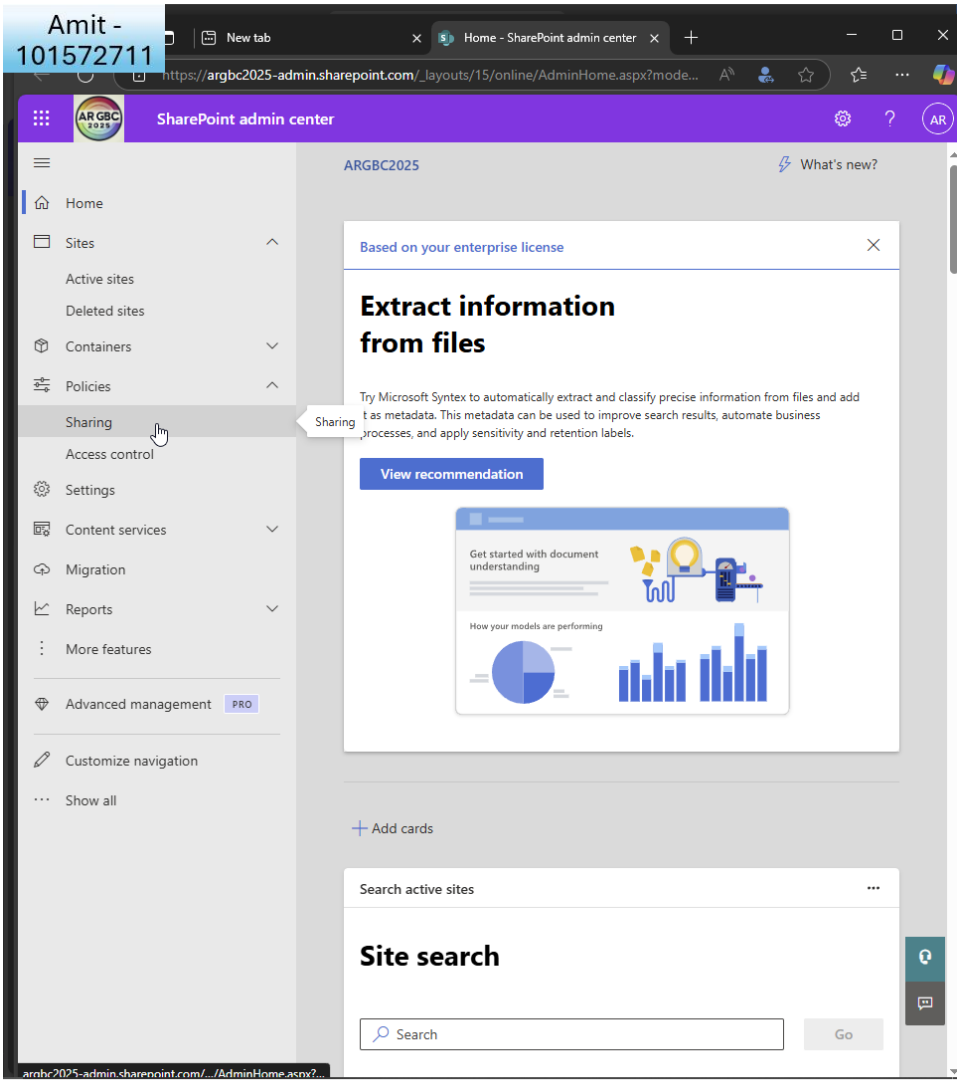
I change some options. For example, create major and minor drafts, number of major versions to 50 (later changed to 100 since MS only accept 100 as a minimum) and check only users who can approve items, and author can see draft items.

Student Name: ……. Term: ……..
Student ID: ……..



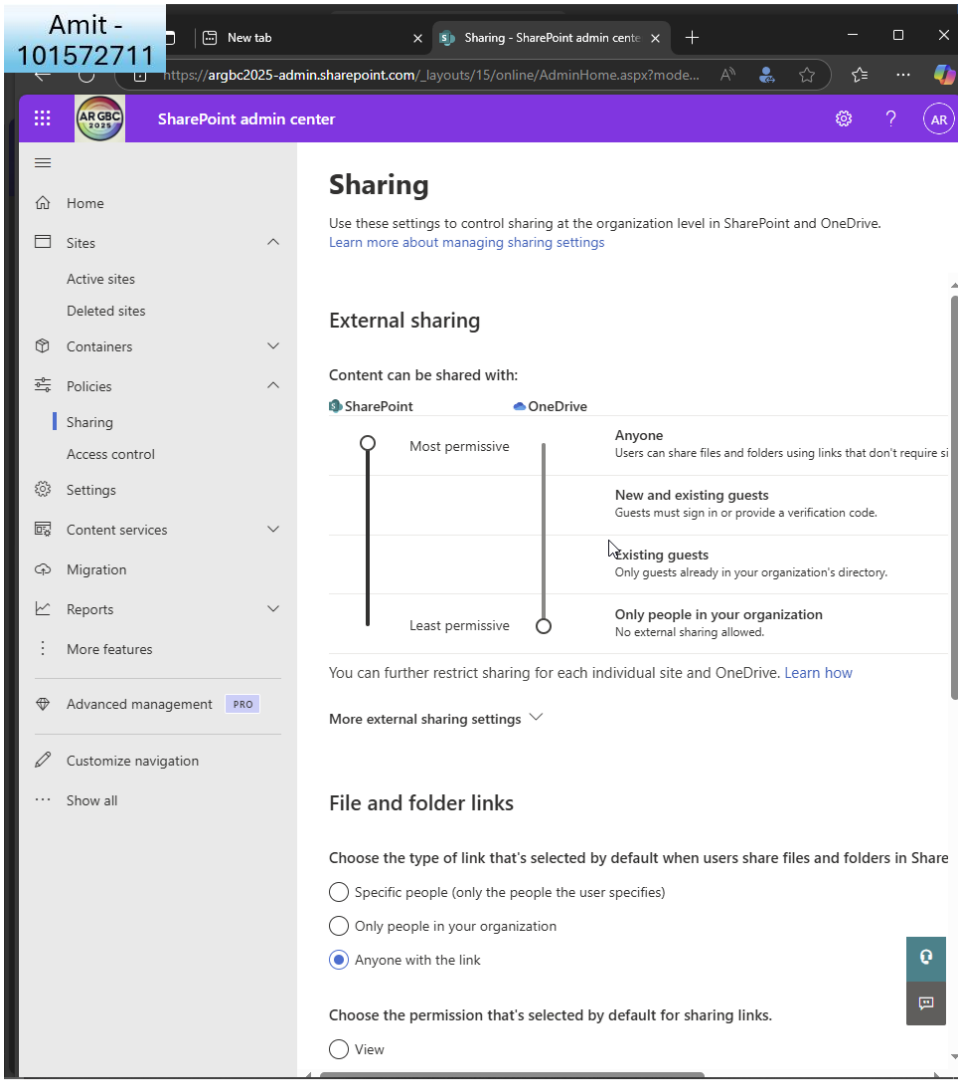
Student Name: ……. Term: ……..
Student ID: ……..

2. **Implement OneDrive for Business**:
    - Configure OneDrive settings to restrict external sharing.



I go to the sharepoint admin centre

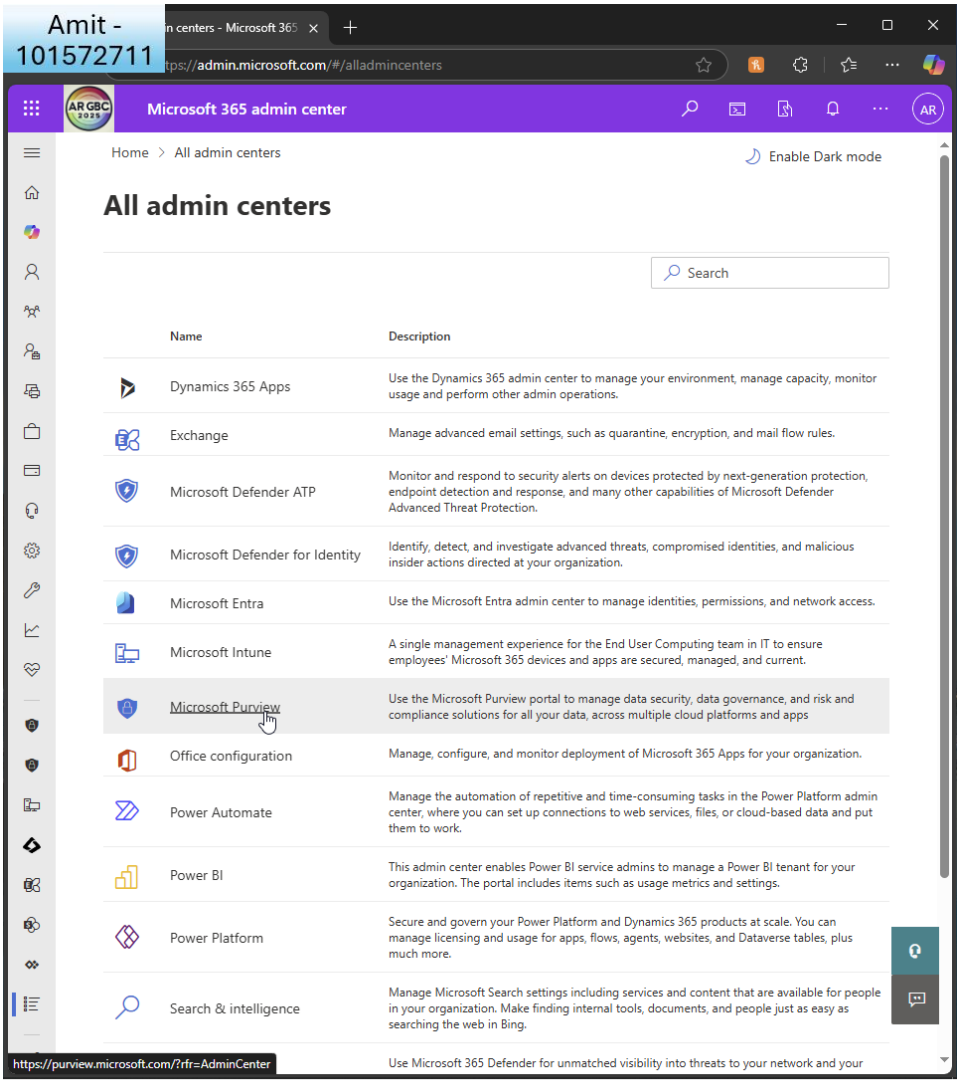
Student Name: ……. Term: ……..
Student ID: ……..



I click 'sharing' under 'policies' and slide the scale down for onedrive so only people within my organisation can share with each other

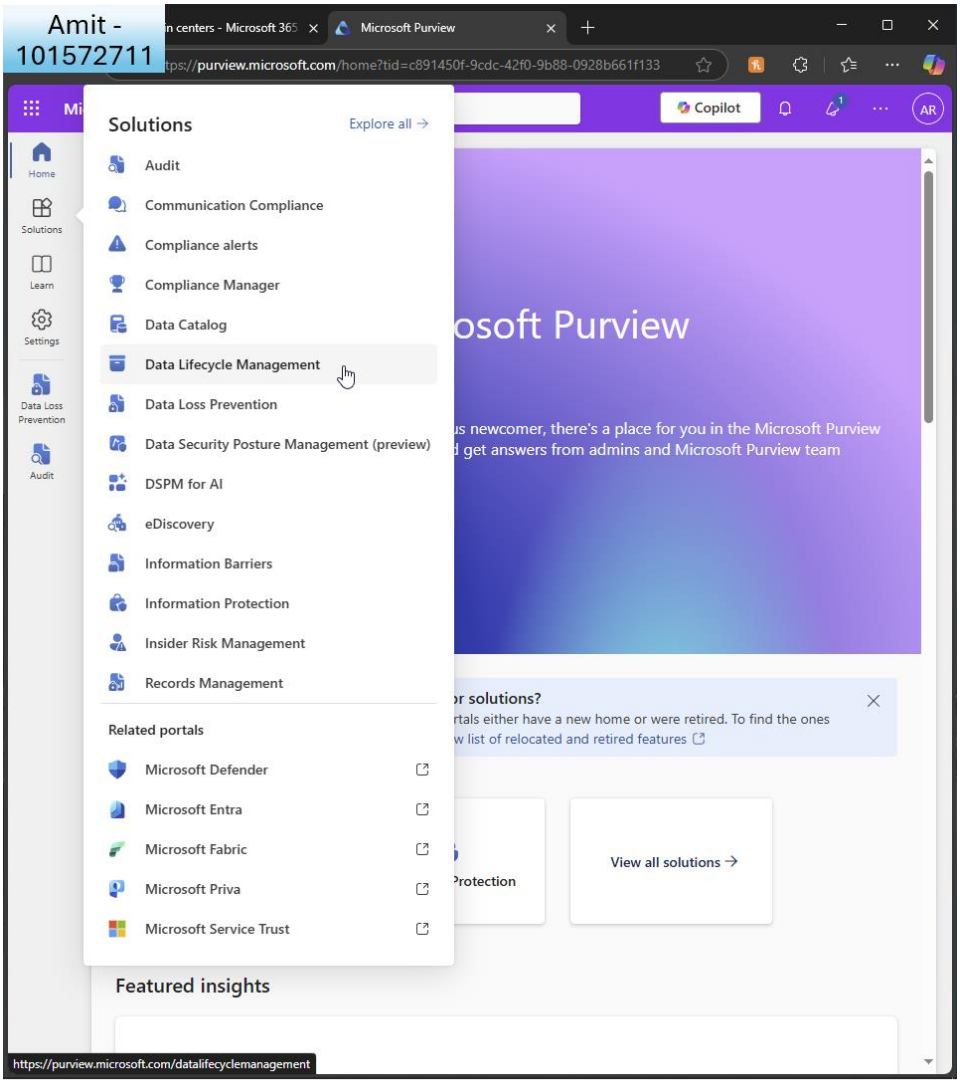
- Enable file retention policies to ensure data is retained for at least five years.

Student Name: ……. Term: …….
Student ID: …….



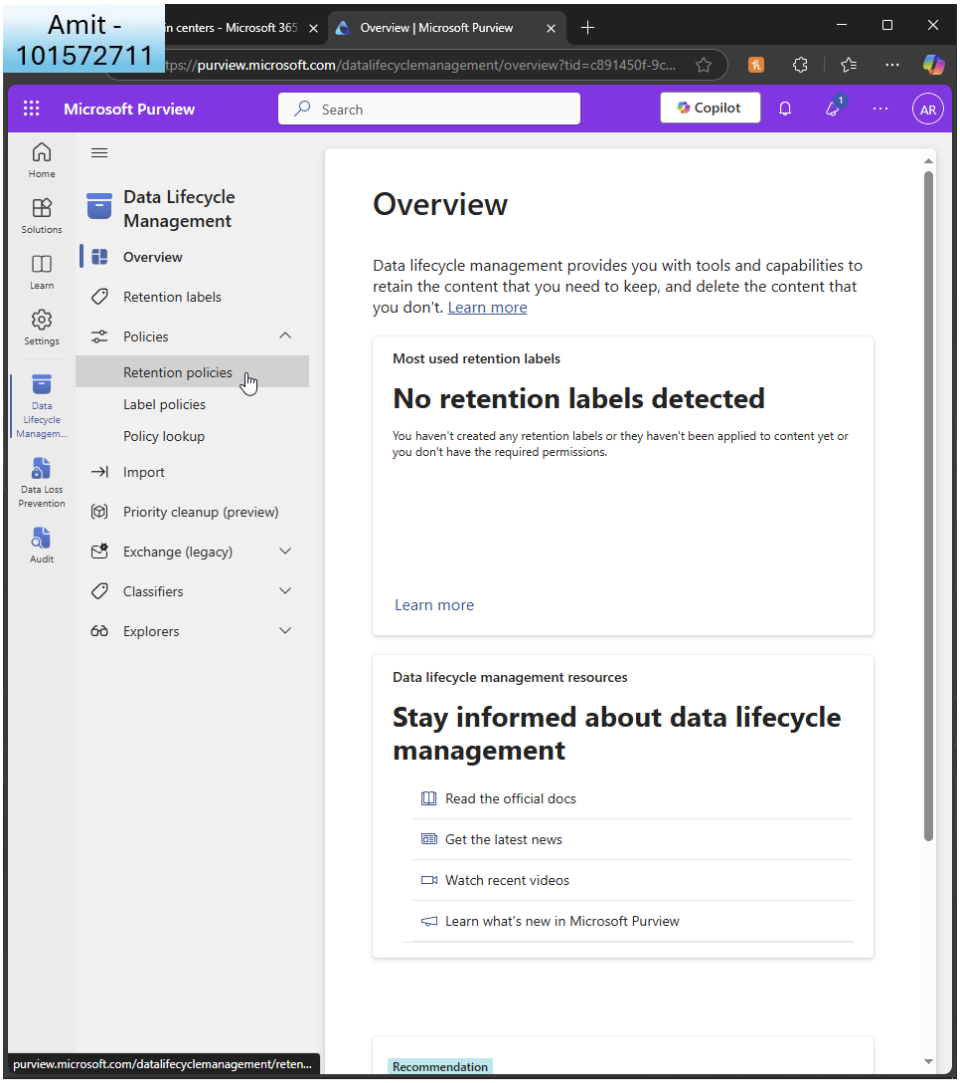
I go to MS purview

Student Name: ……. Term: ……..
Student ID: ……..



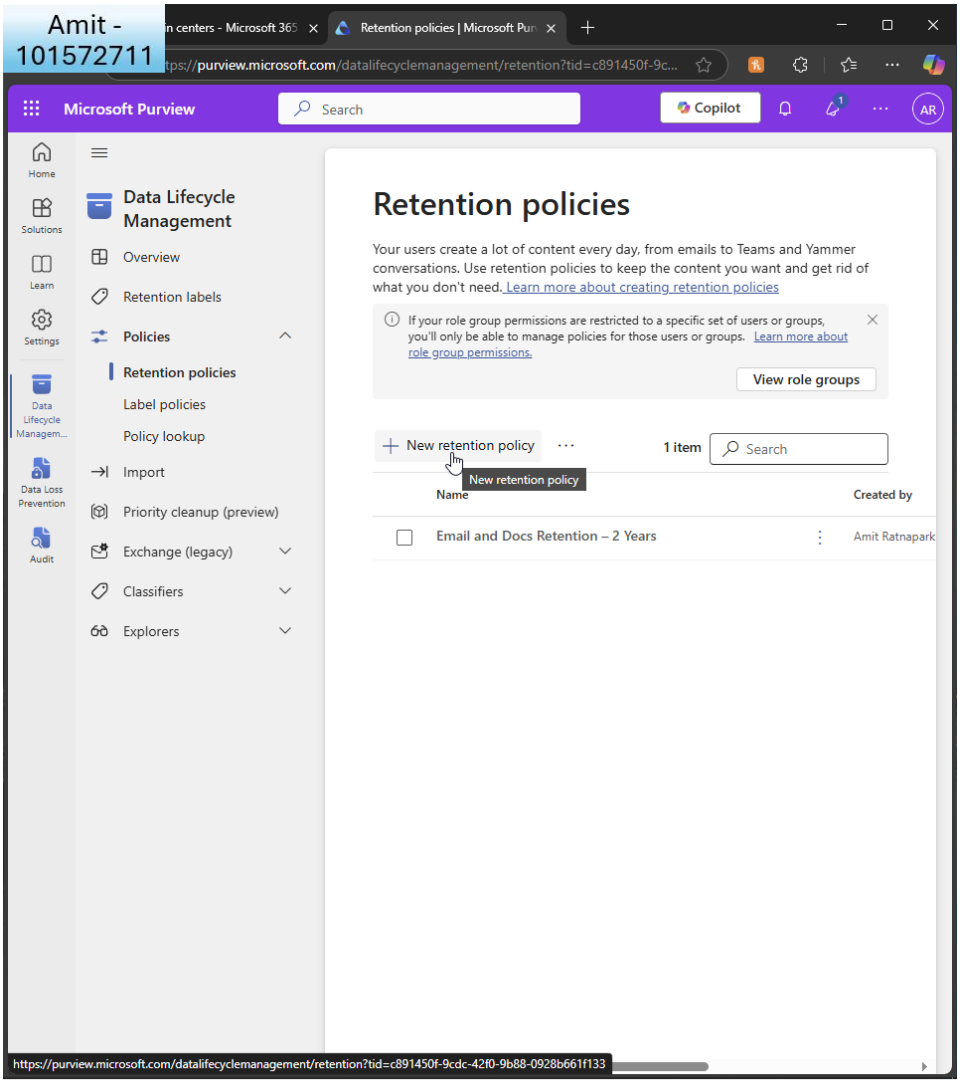
I click to create a DLP policy

Student Name: ……. Term: ……..
Student ID: ……..



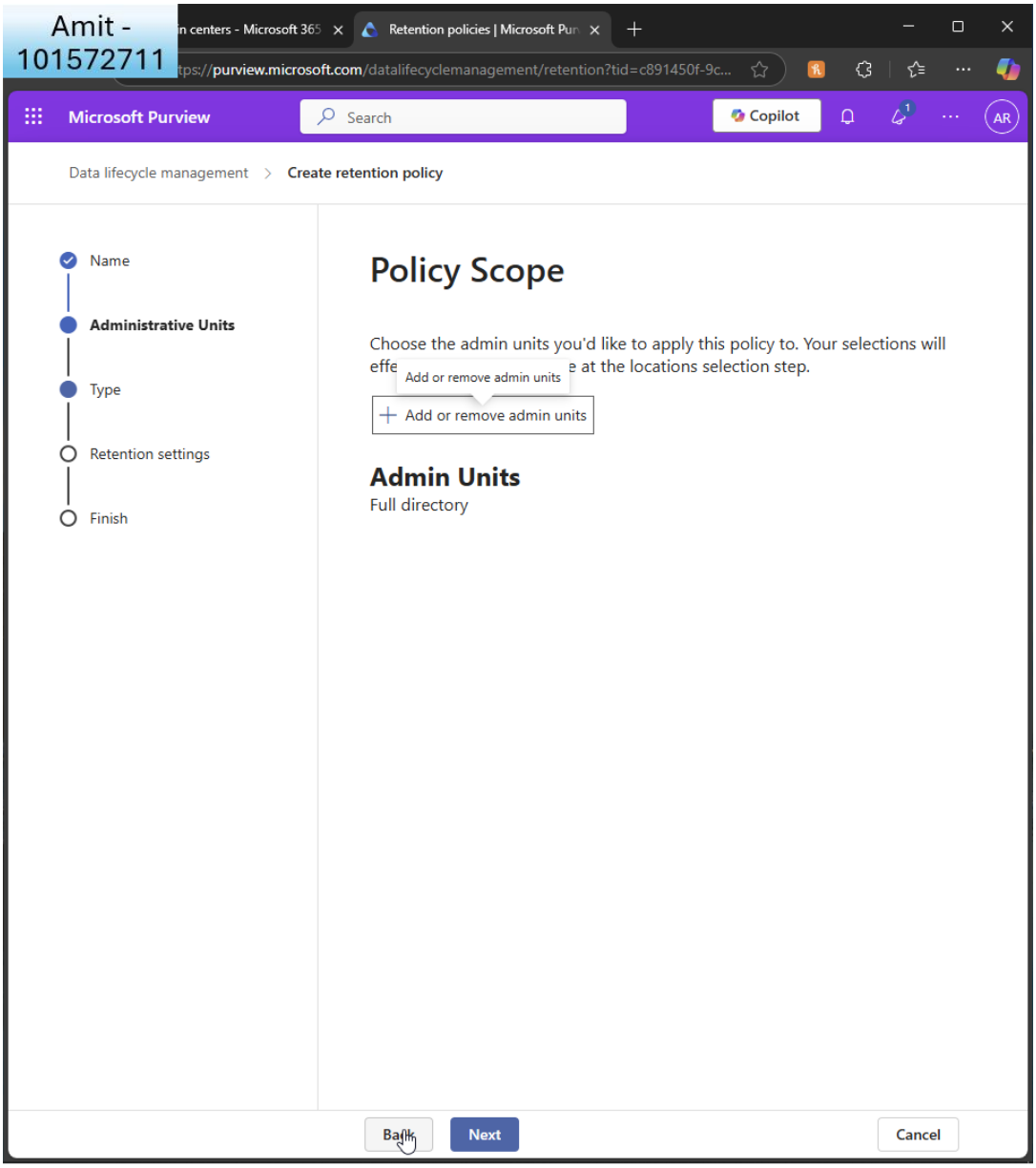
I click ’retention policies’

Student Name: ……. Term: ……..
Student ID: ……..



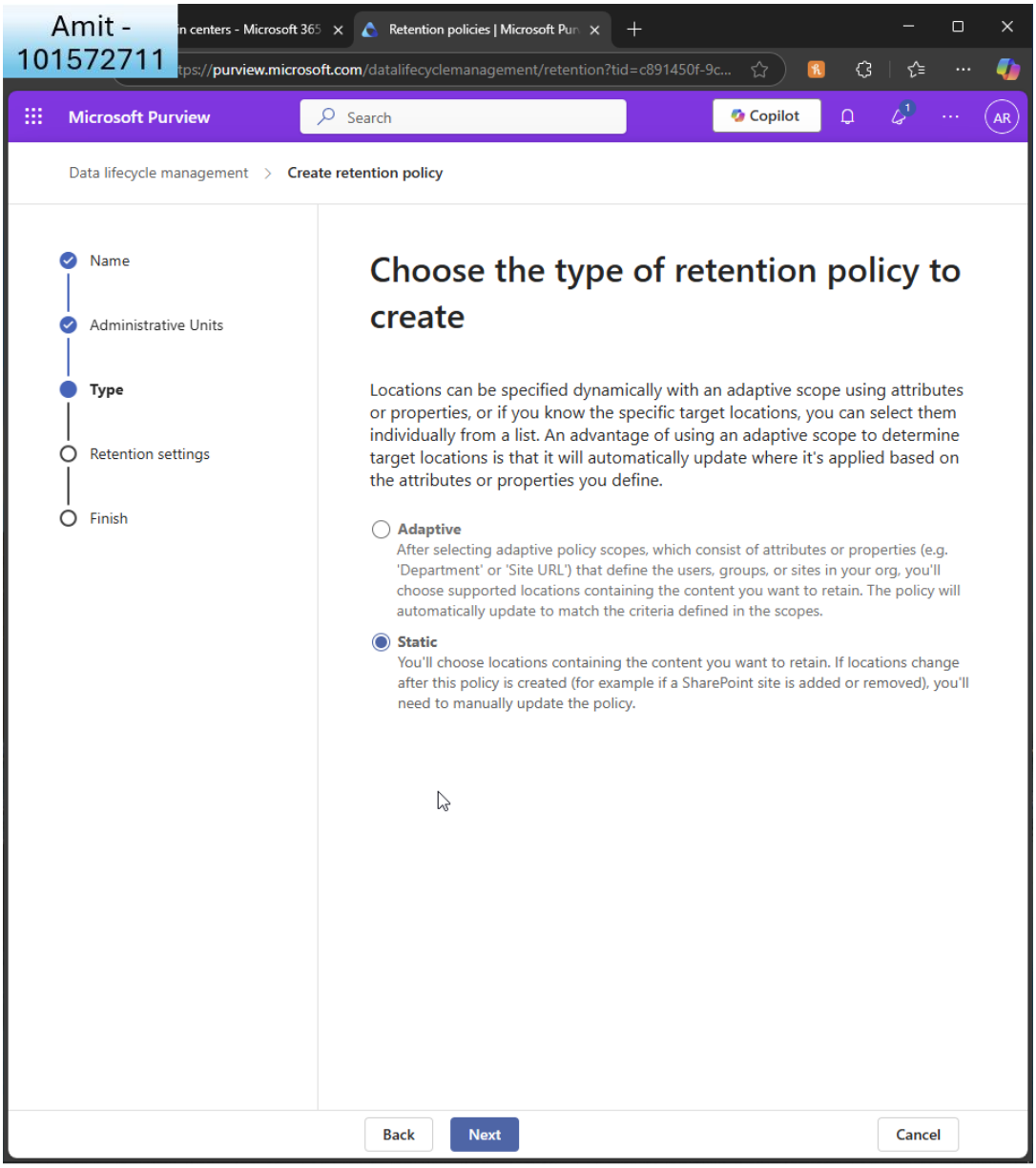
And create a new retention policy

Student Name: ……. Term: ……..
Student ID: ……..



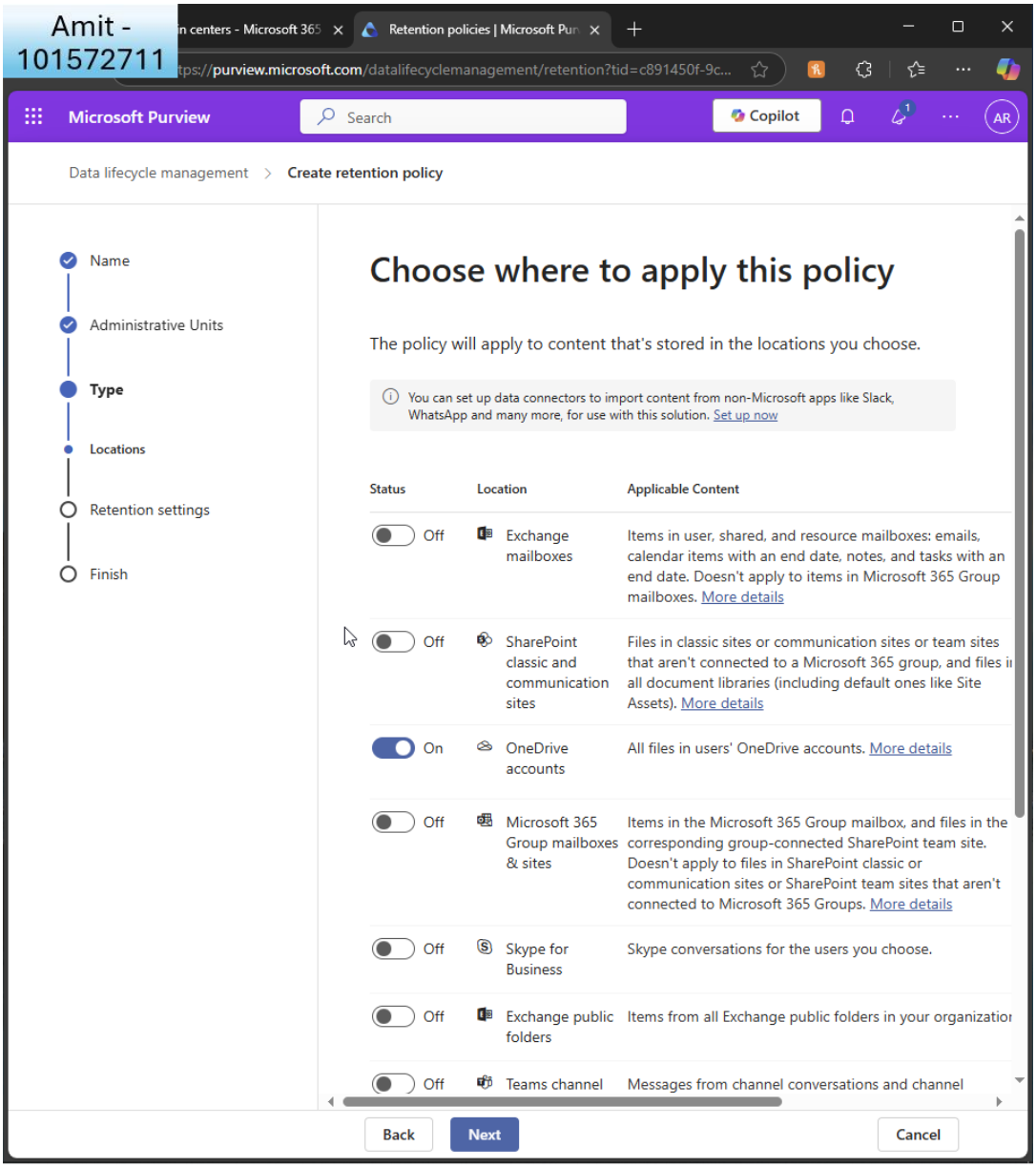
I leave it for all admin units

Student Name: ……. Term: ……..
Student ID: ……..



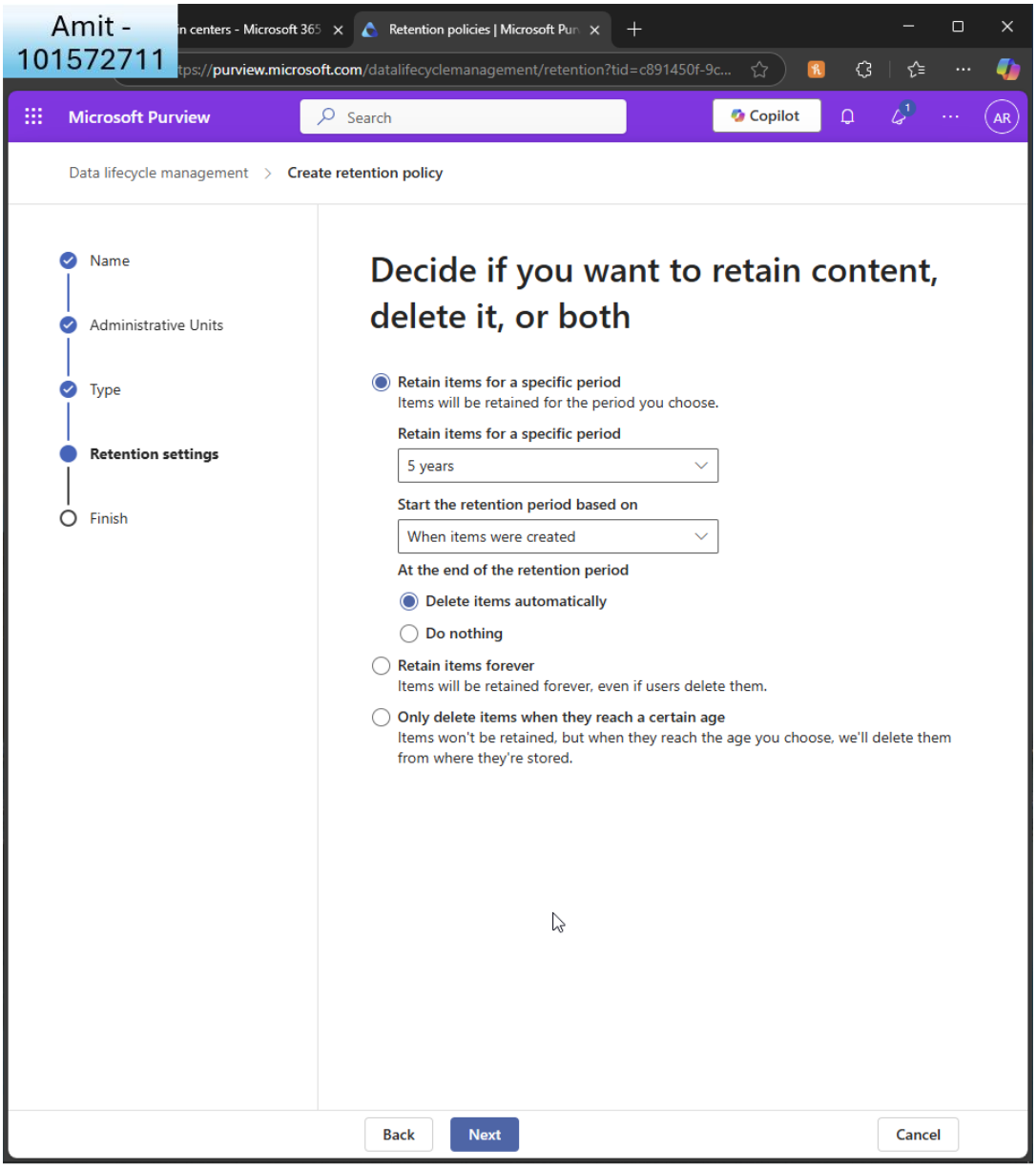
I choose 'static'

Student Name: ……. Term: ……..
Student ID: ……..



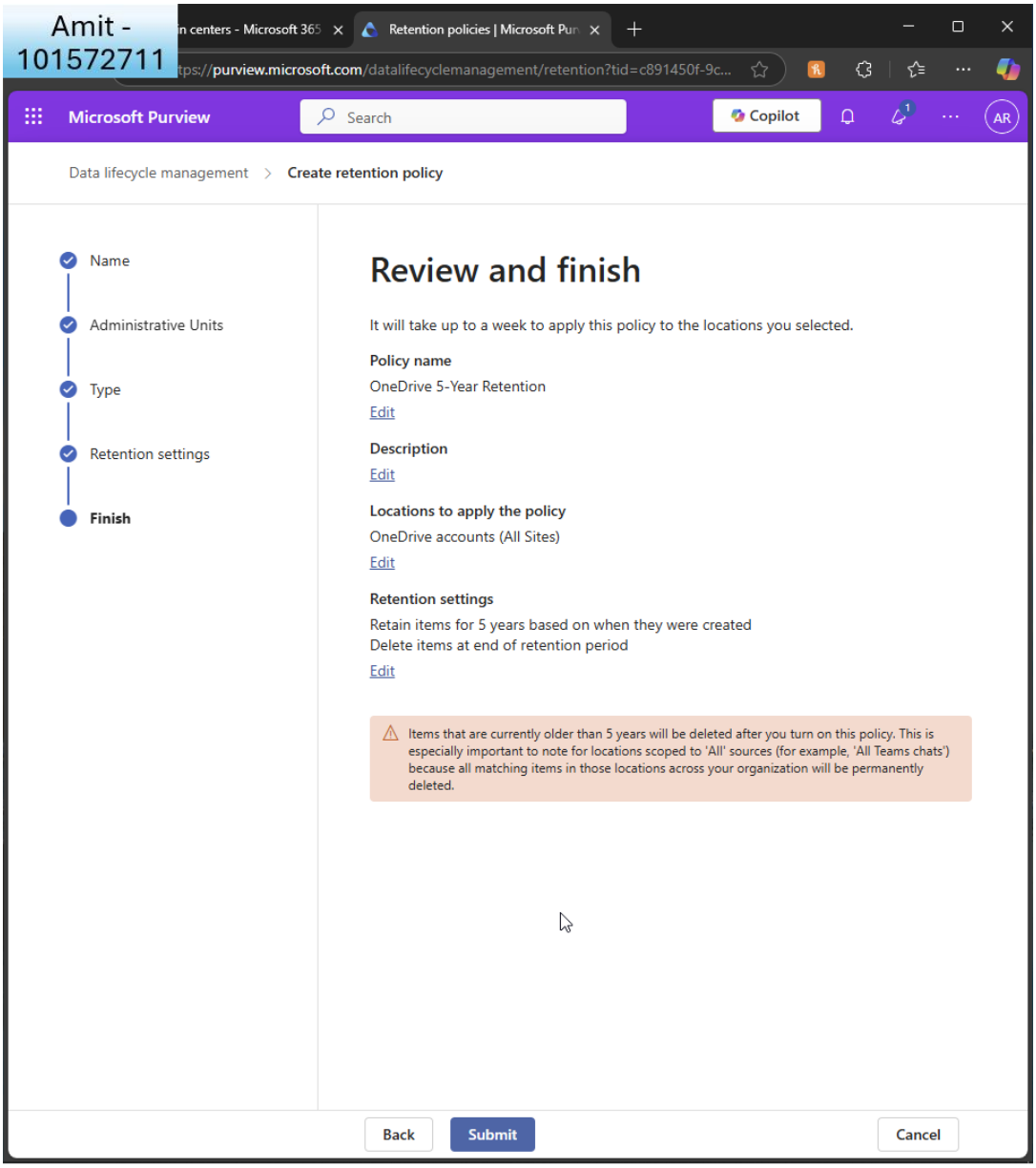
I apply it only to onedrive accounts

Student Name: ……. Term: ……..
Student ID: ……..



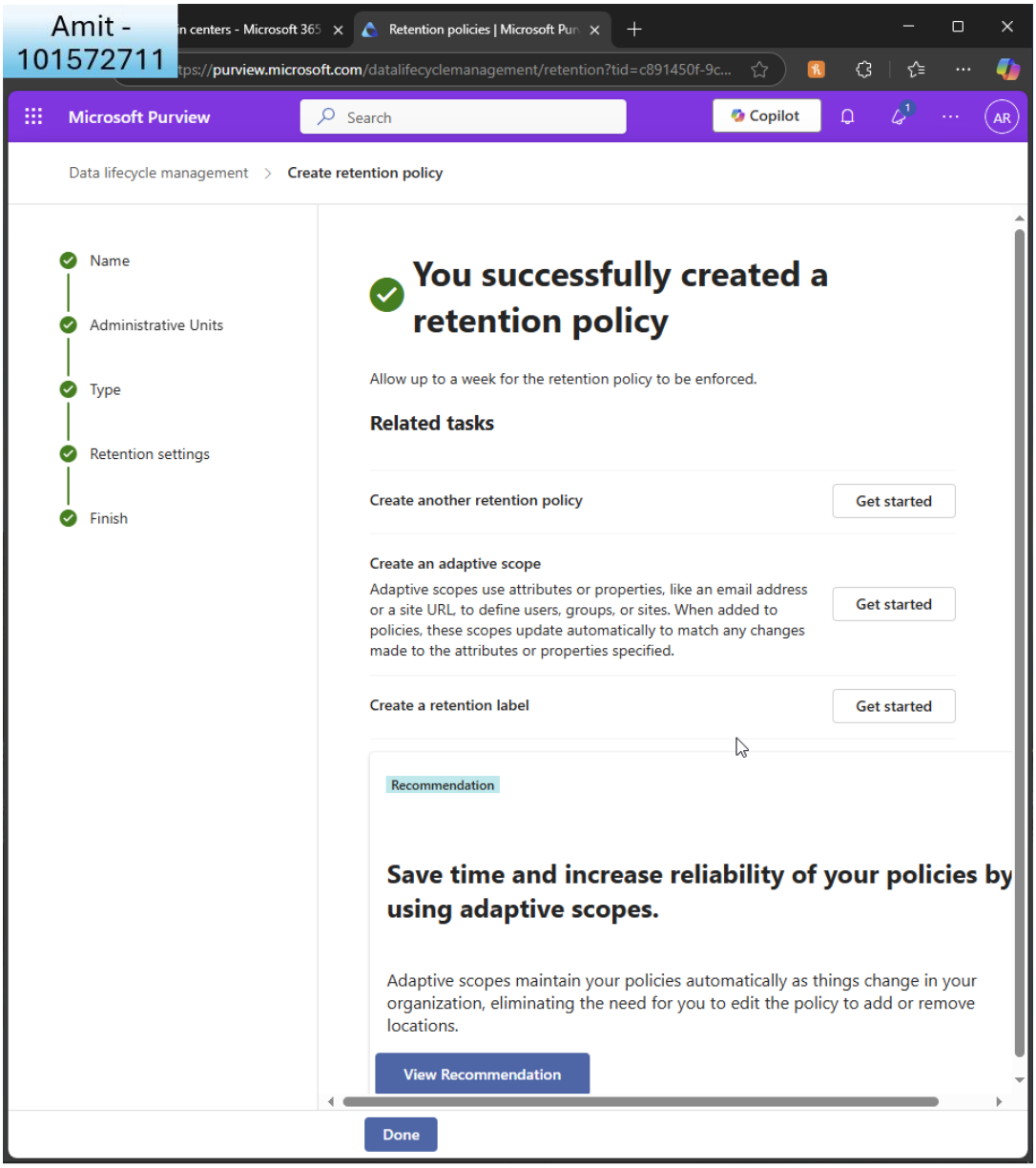
I choose to retain for 5 years and delete items automatically

Student Name: ……. Term: ……..
Student ID: ……..



I review and finish

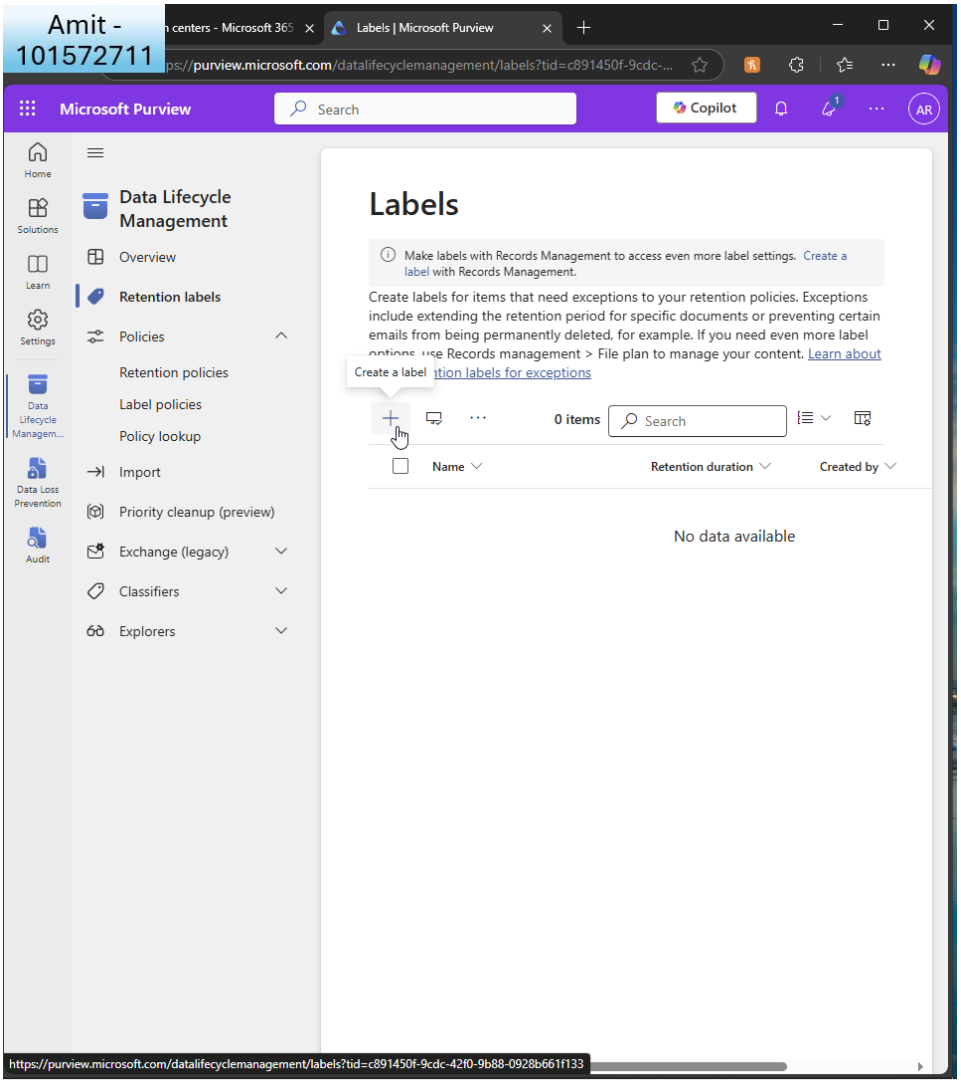
Student Name: ……. Term: ……..
Student ID: ……..



It confirms it has been created

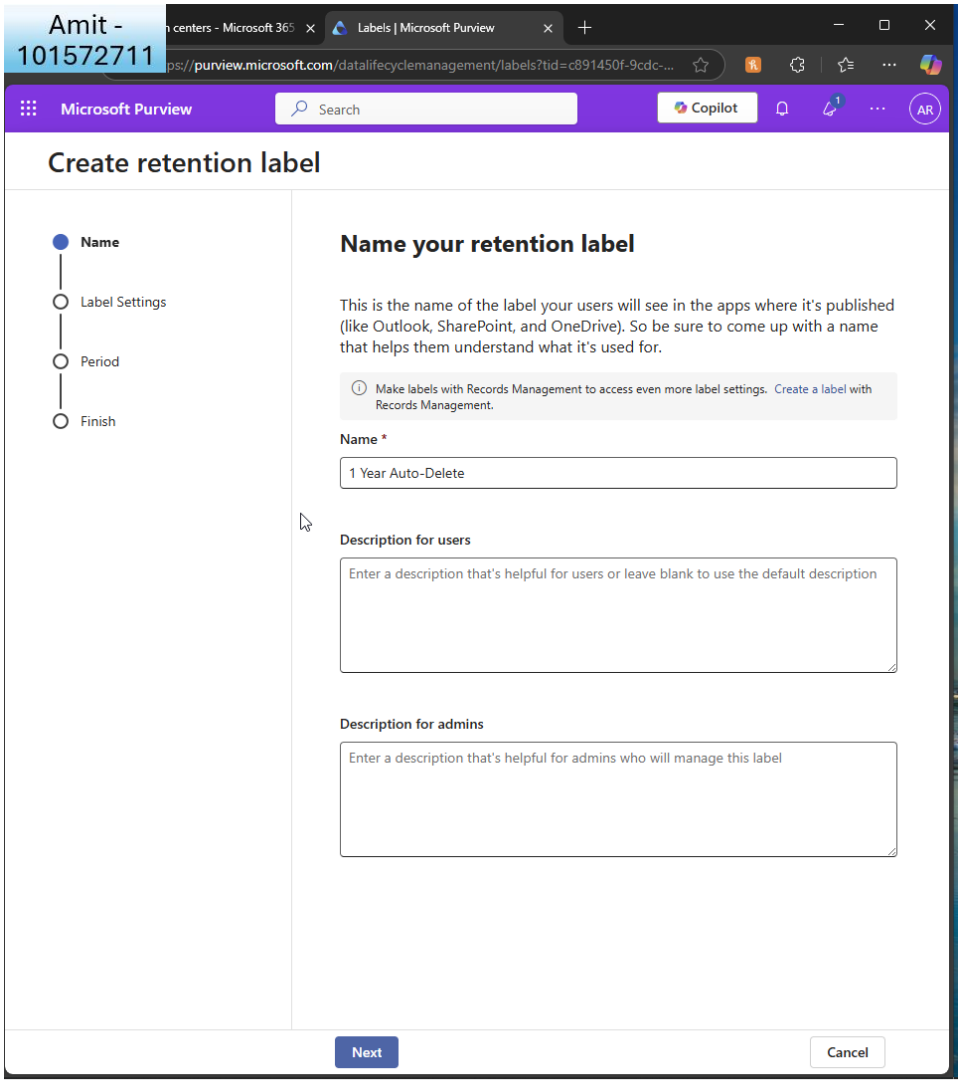
- Set up a policy to automatically move old files to the Recycle Bin after a year.

Student Name: ……. Term: ……..
Student ID: ……..



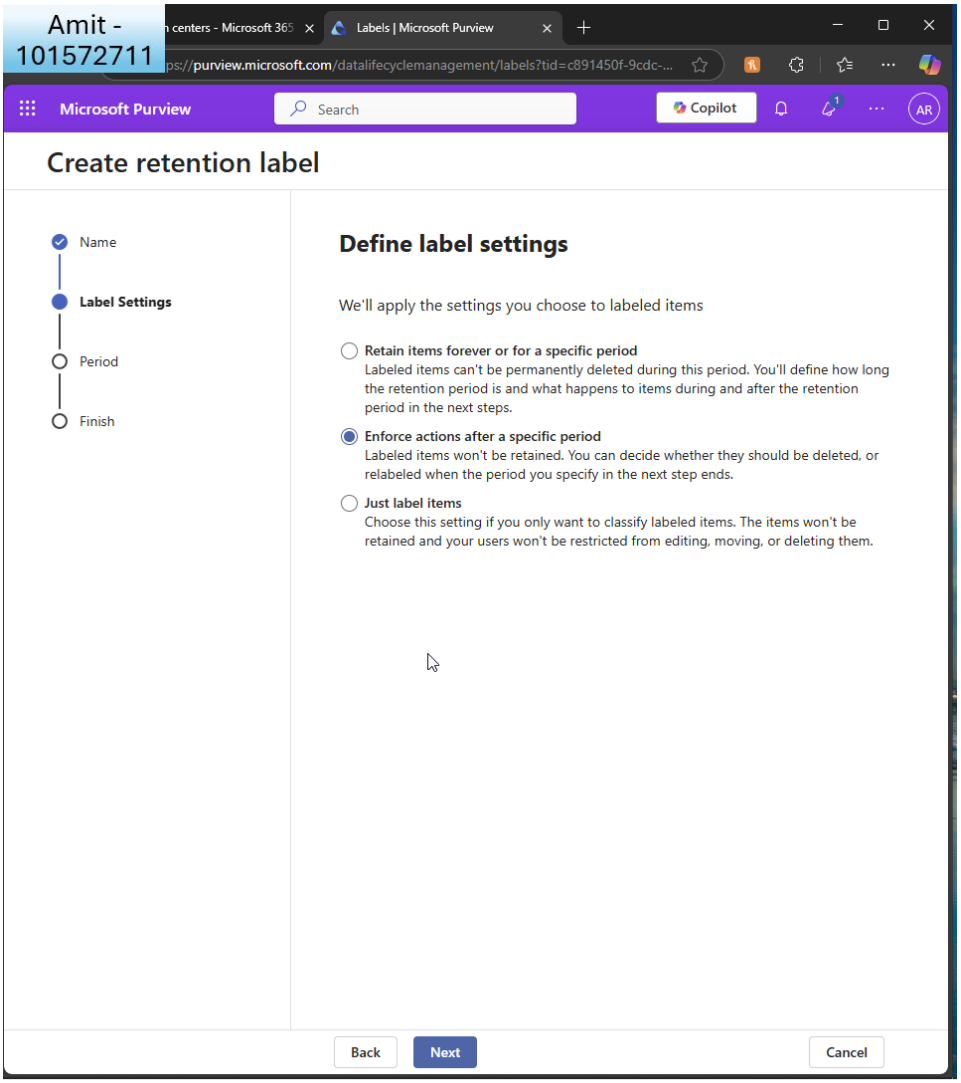
Still within DLP, I choose ’retention labels’

Student Name: ……. Term: ……..
Student ID: ……..



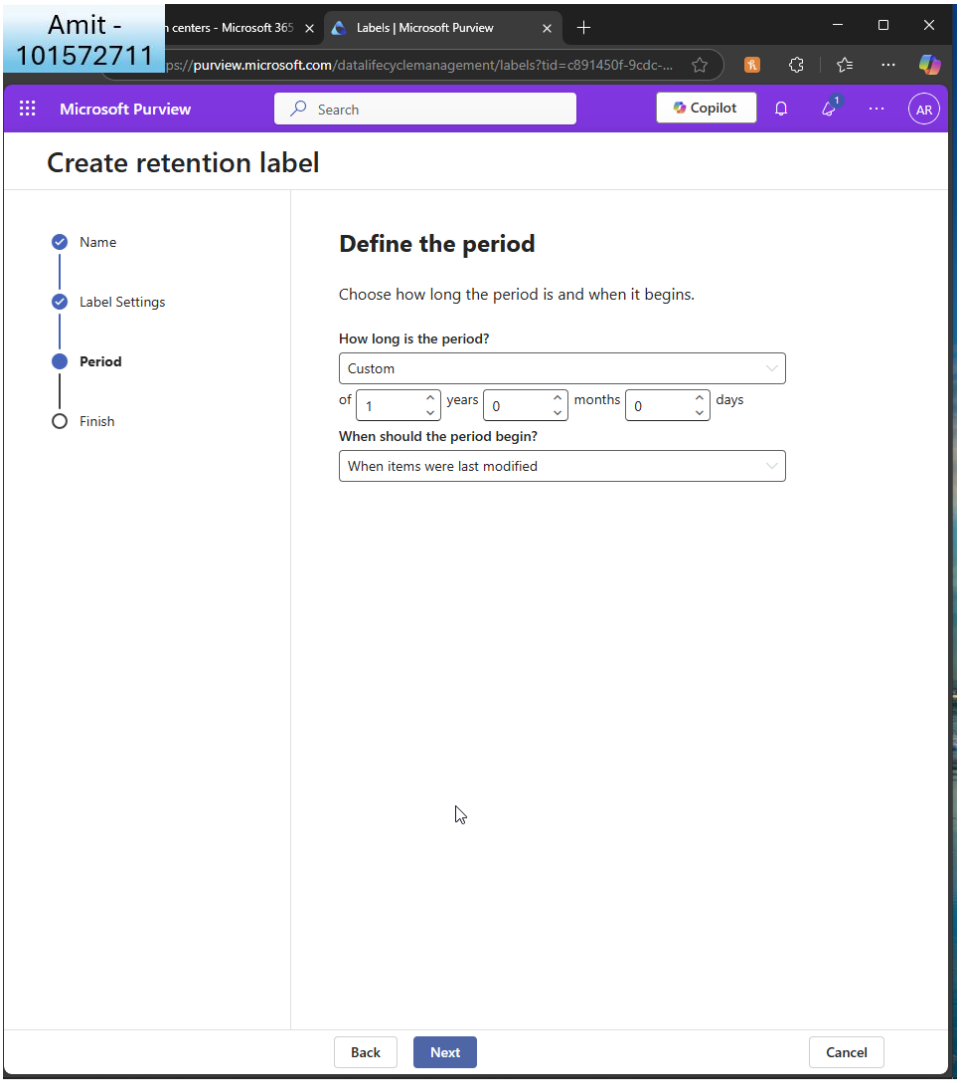
I name the retention label

Student Name: ……. Term: ……..
Student ID: ……..



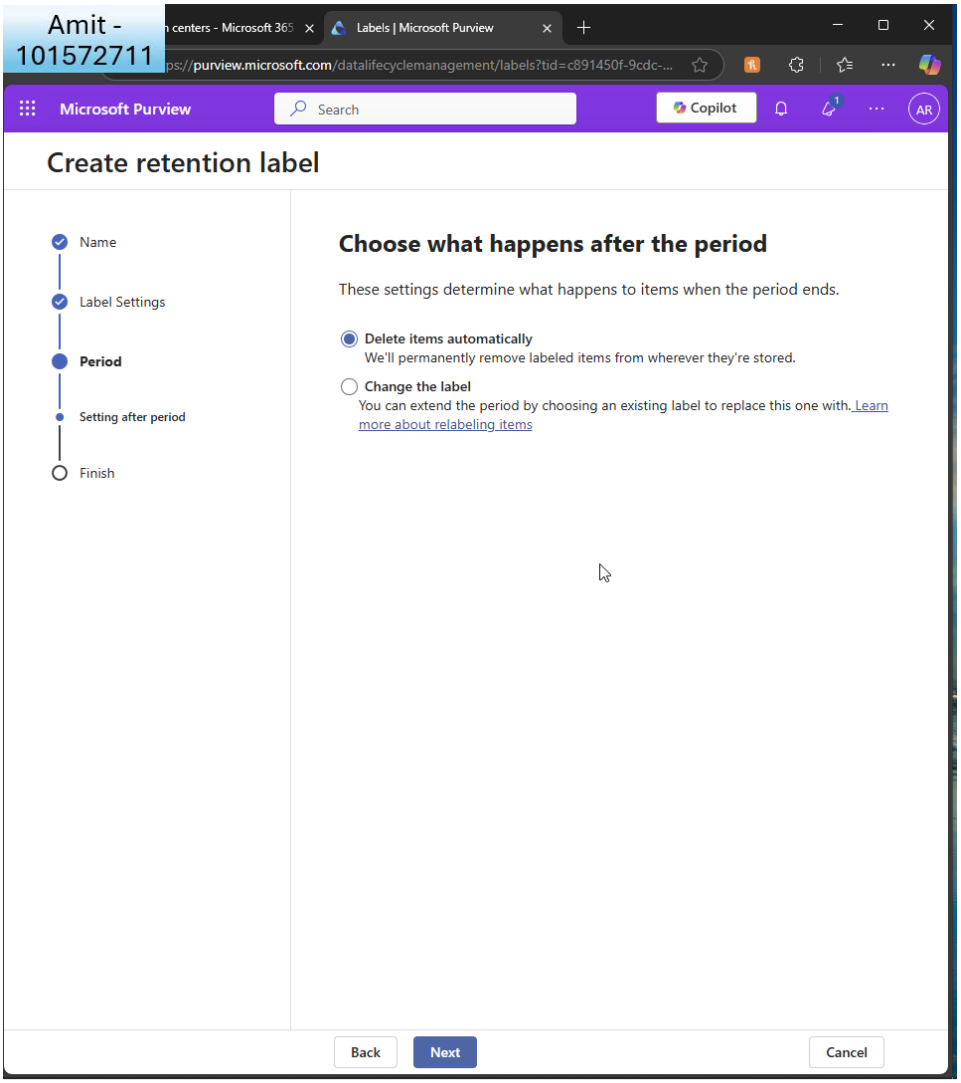
I enforce action after specific period i.e. 1 year

Student Name: ……. Term: ……..
Student ID: ……..



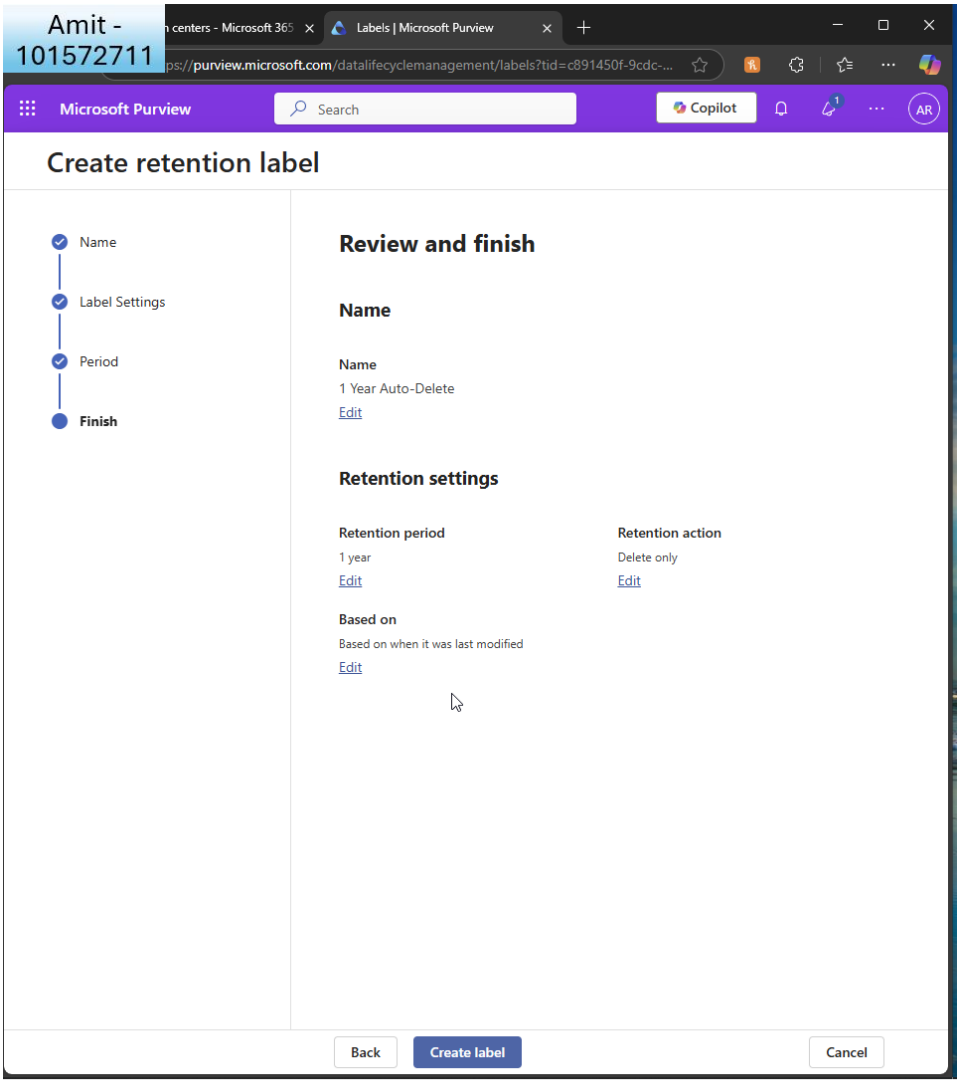
Here I specify 1 year retention from when the item was last modified.

Student Name: ……. Term: ……..
Student ID: ……..



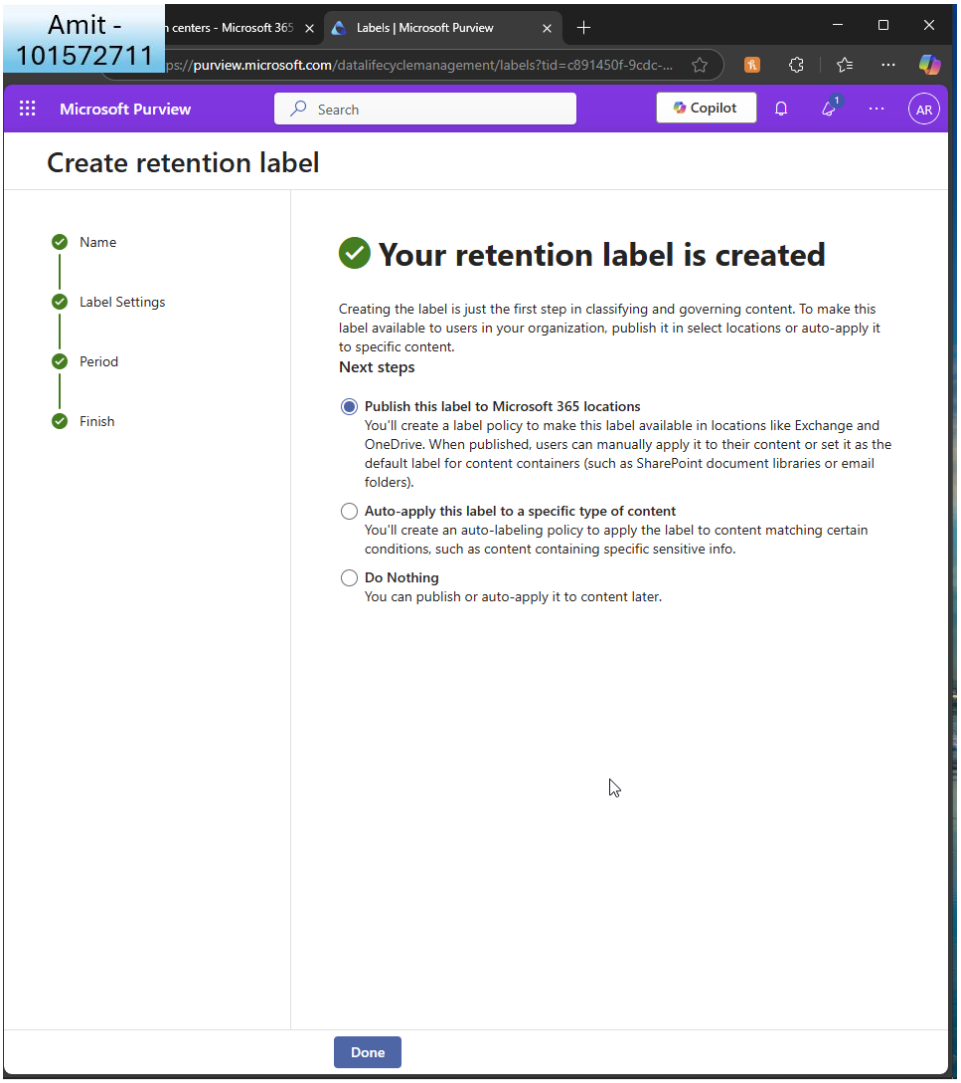
Here I choose the action to delete the items automatically

Student Name: ……. Term: ……..
Student ID: ……..



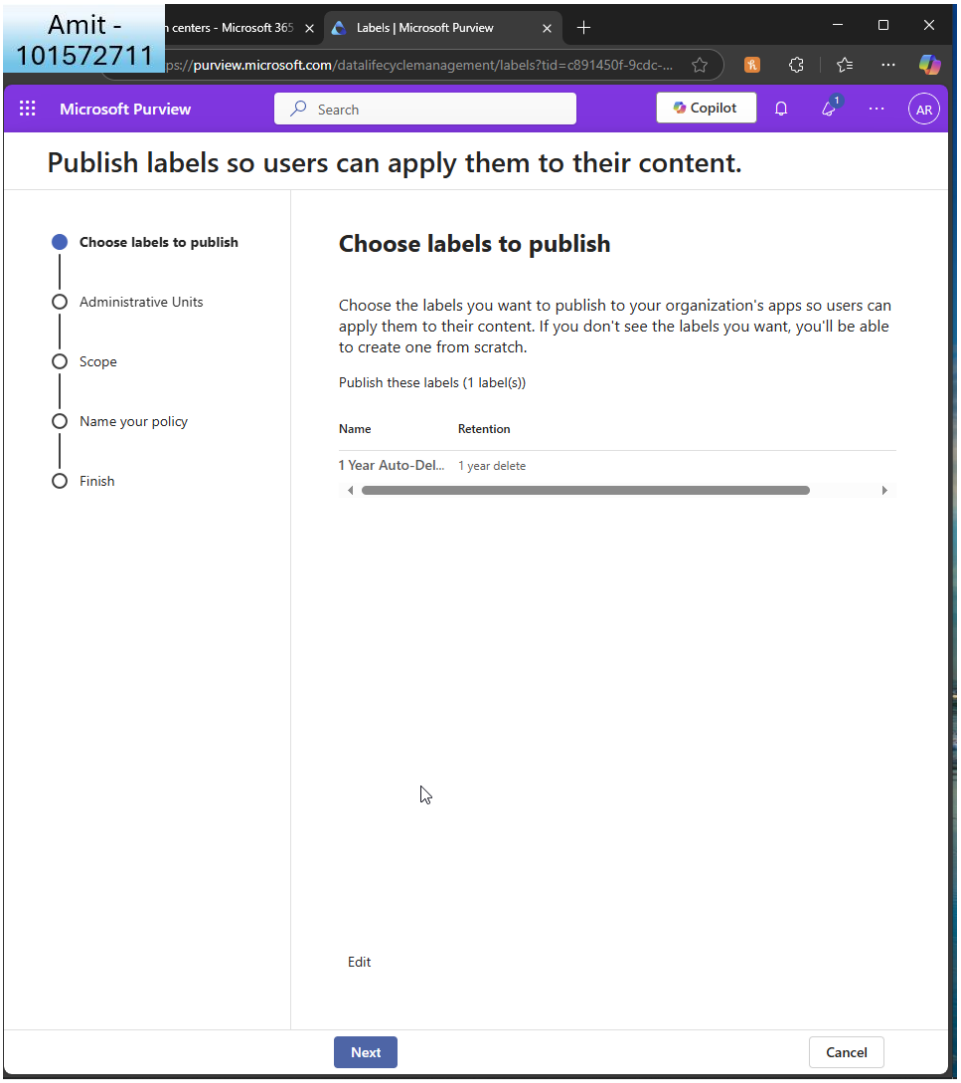
I review and finish

Student Name: ……. Term: ……..
Student ID: ……..



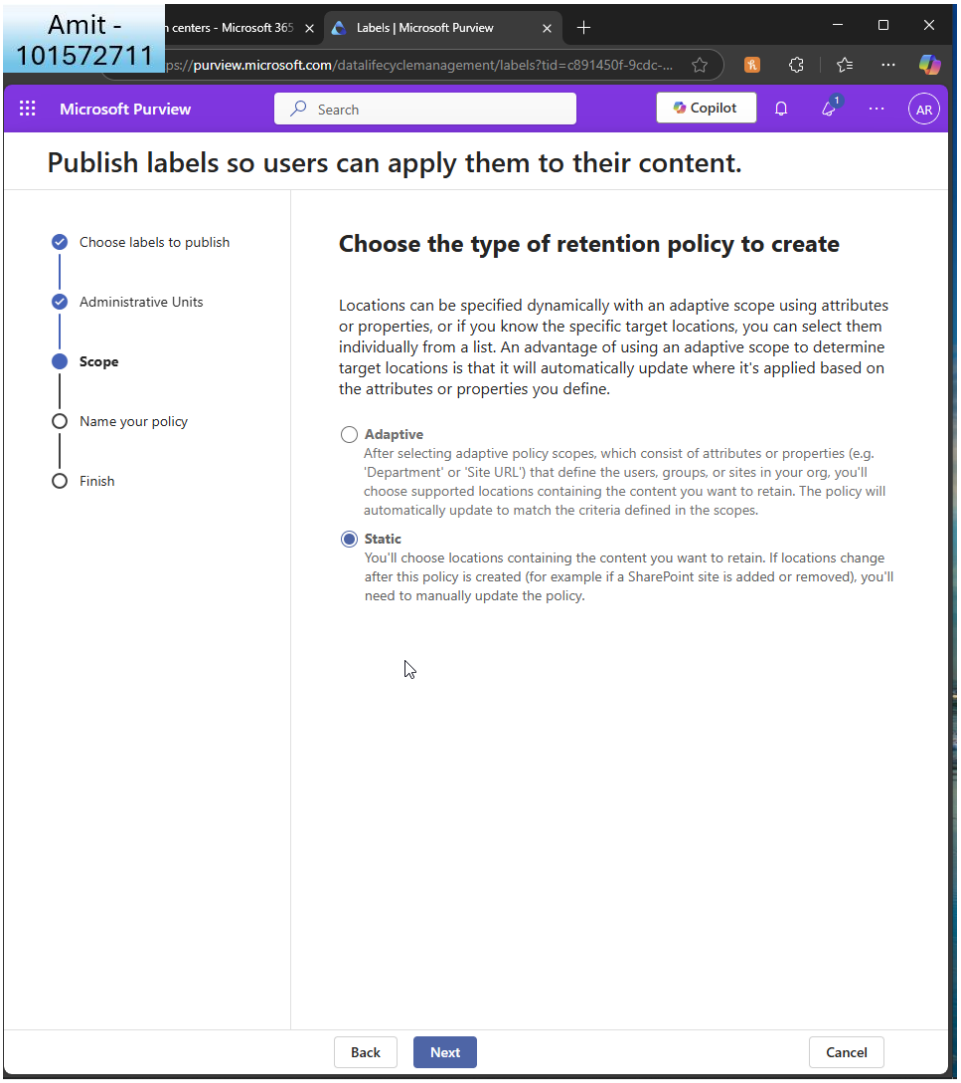
I see the confirmation

Student Name: ……. Term: ……..
Student ID: ……..



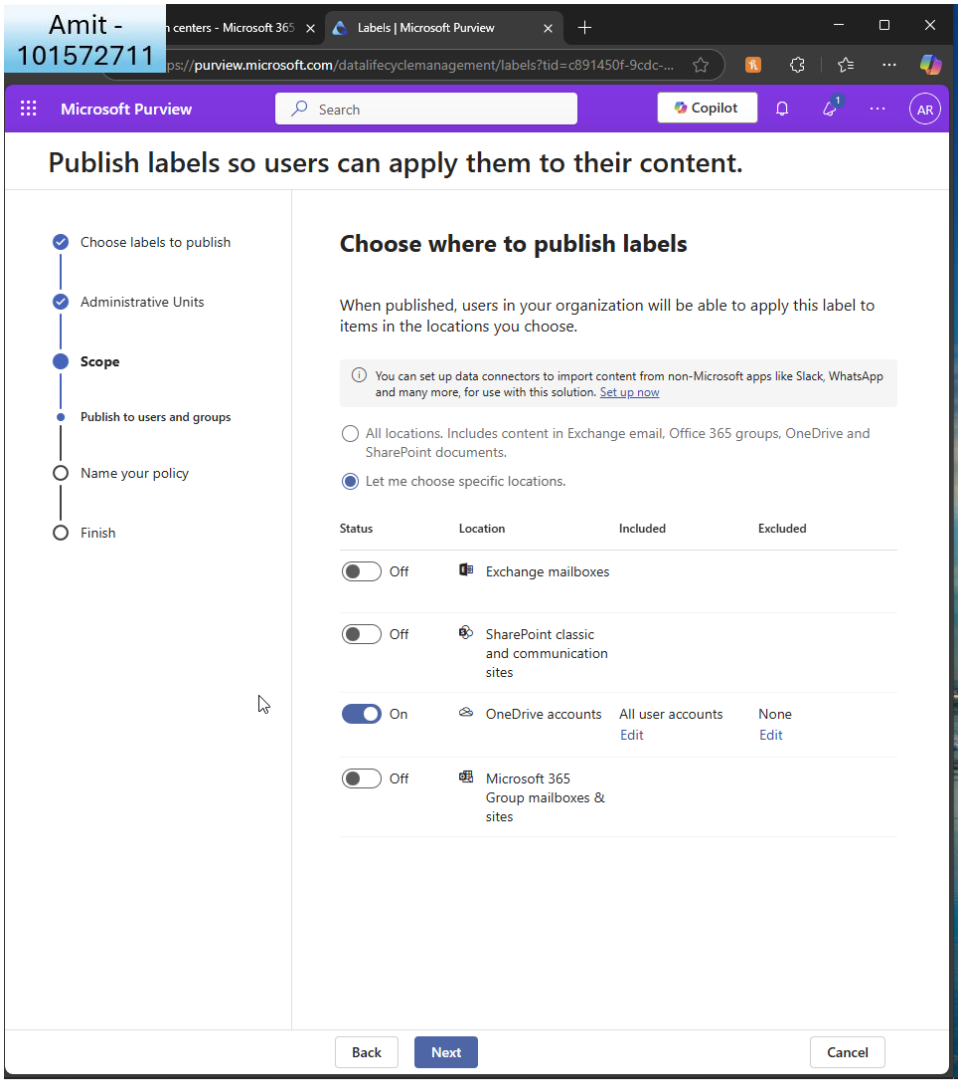
I now publish the label

Student Name: ……. Term: ……..
Student ID: ……..



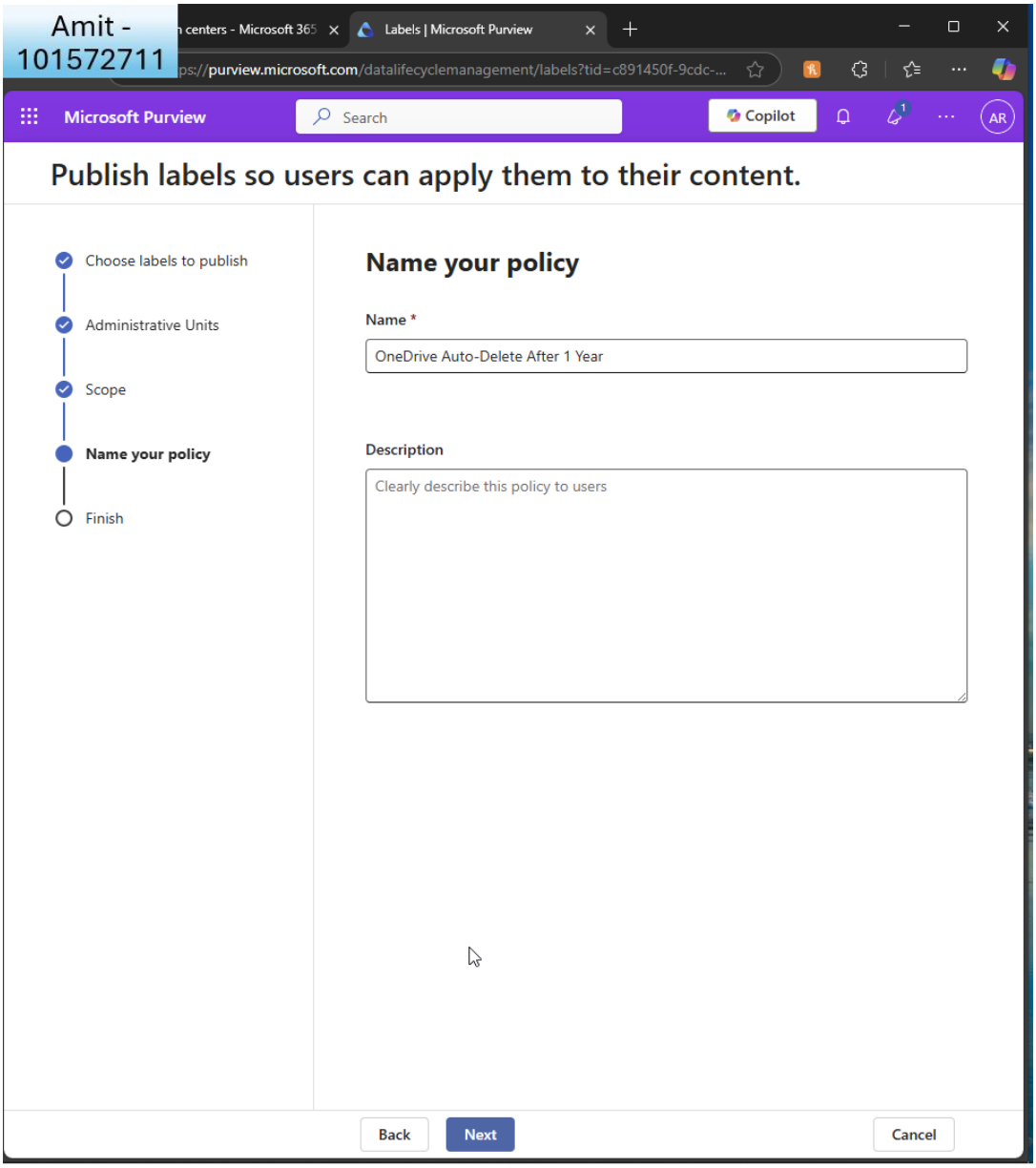
I choose 'static'

Student Name: ……. Term: ……..
Student ID: ……..



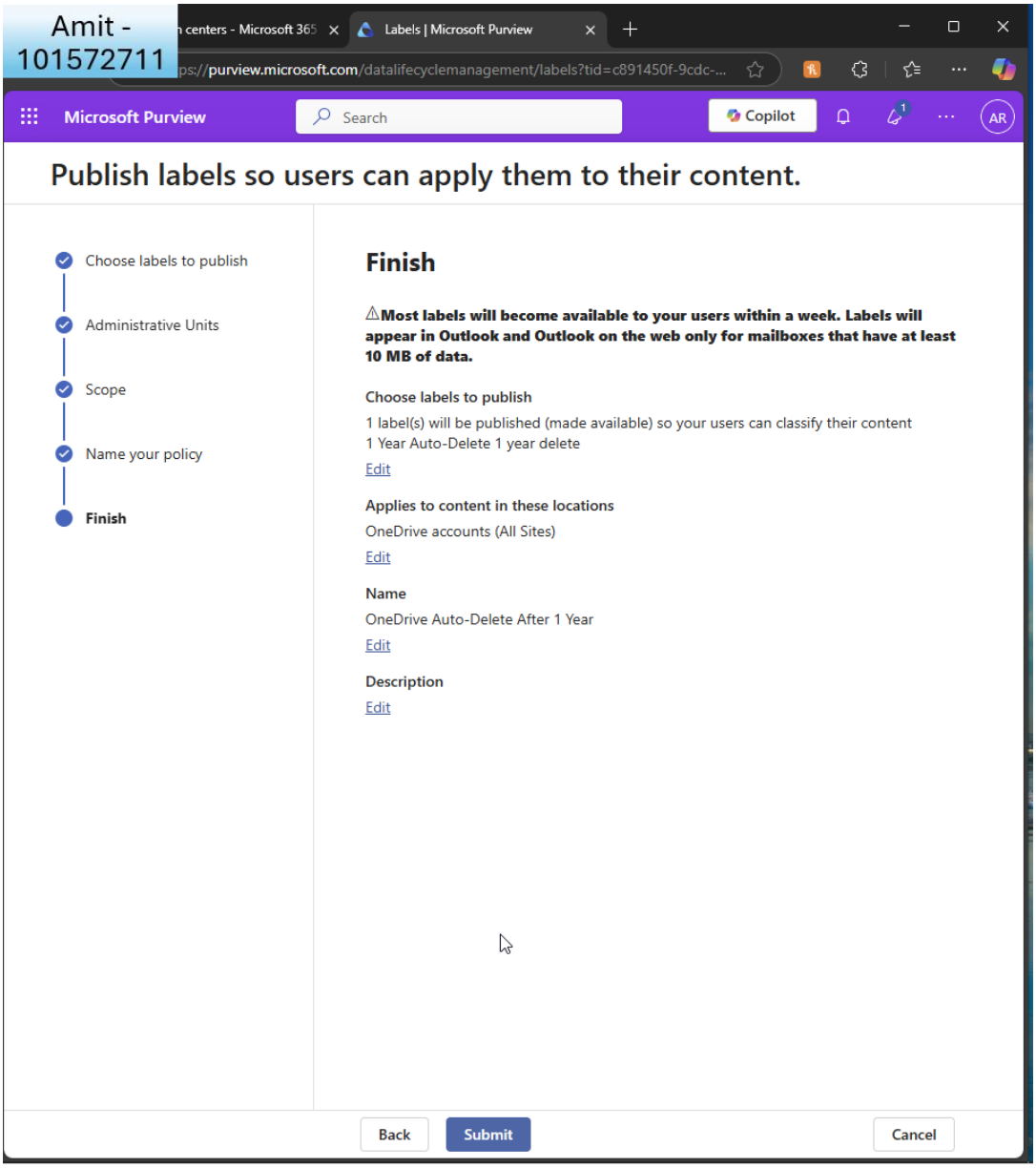
And specify only onedrive accounts

Student Name: ……. Term: ……..
Student ID: ……..



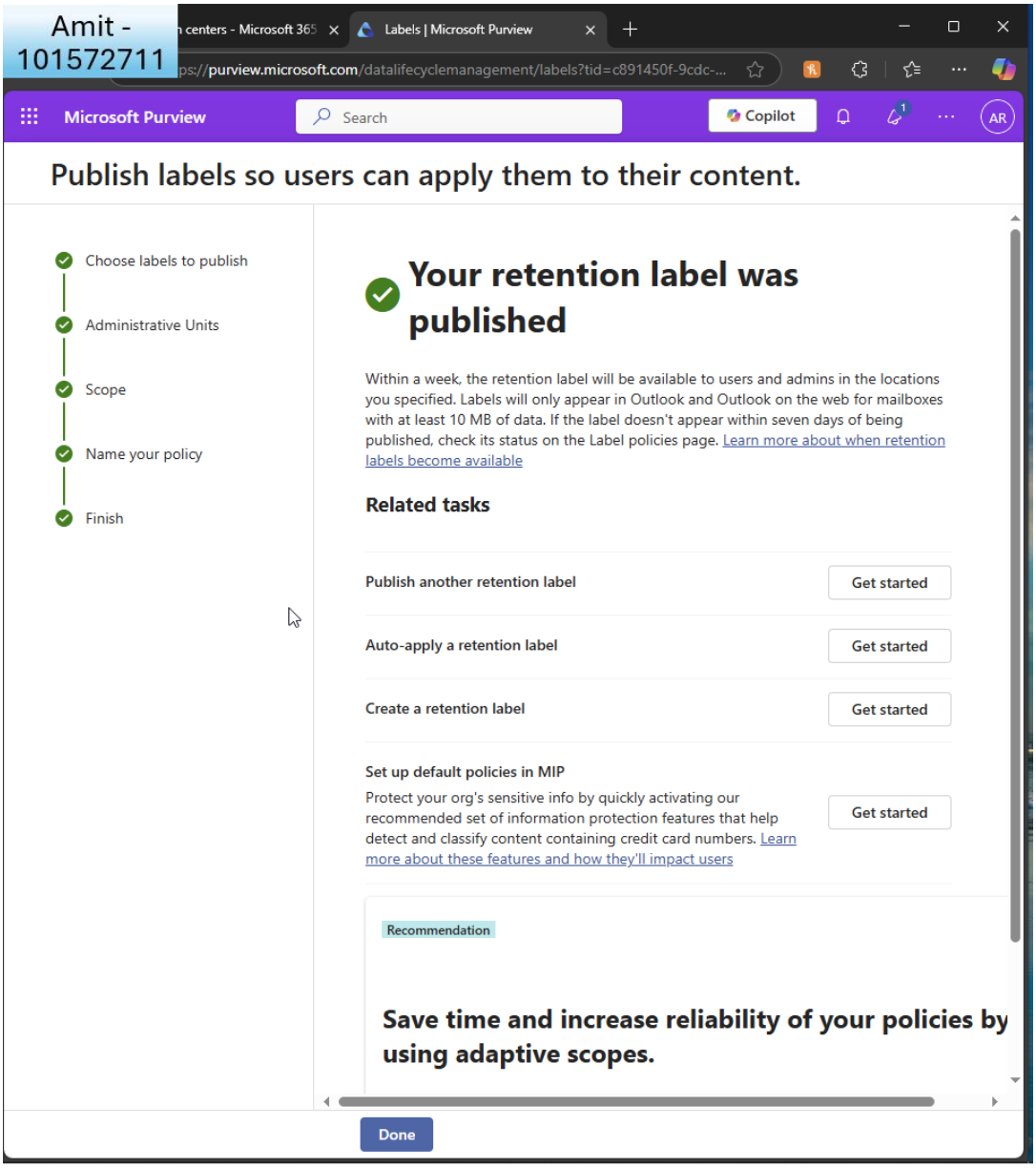
I name the policy

Student Name: ……. Term: ……..
Student ID: ……..



I finish creating the policy

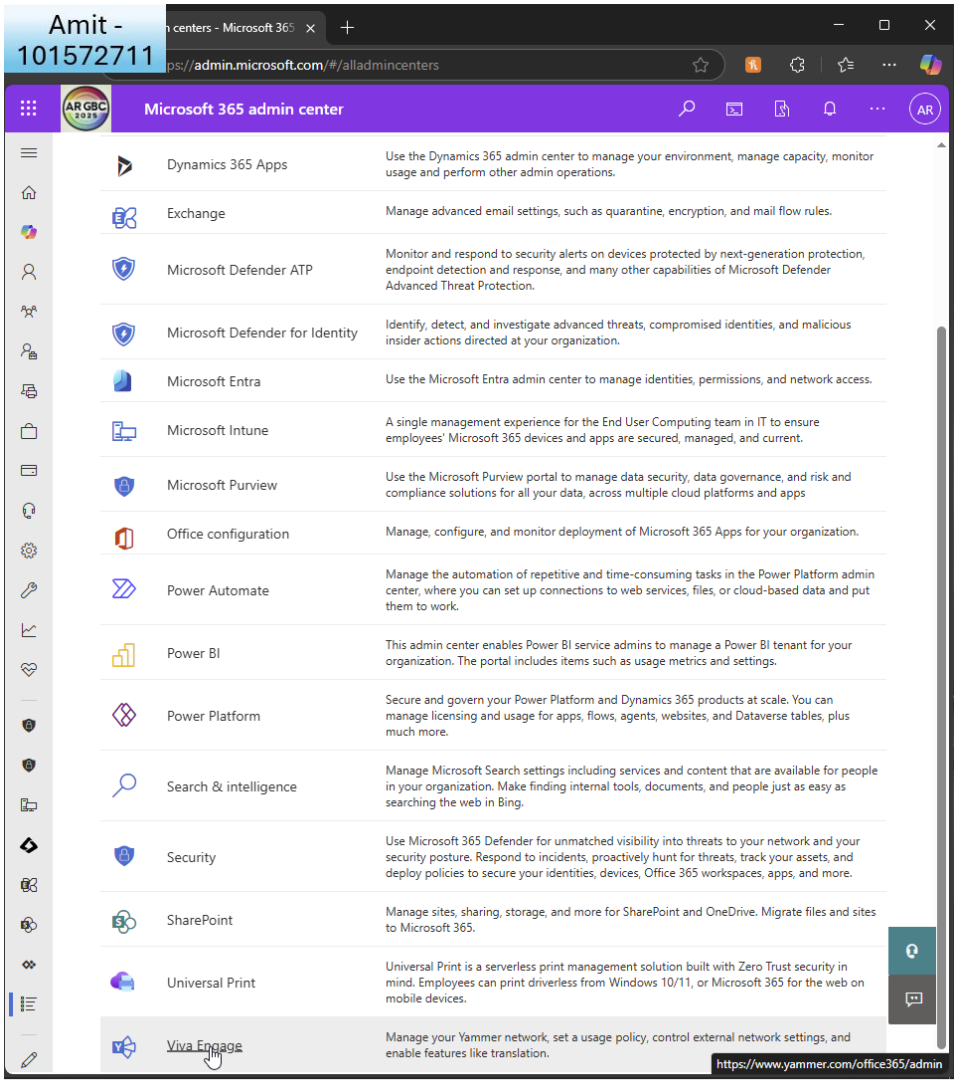
Student Name: ……. Term: ……..
Student ID: ……..



I see the confirmation

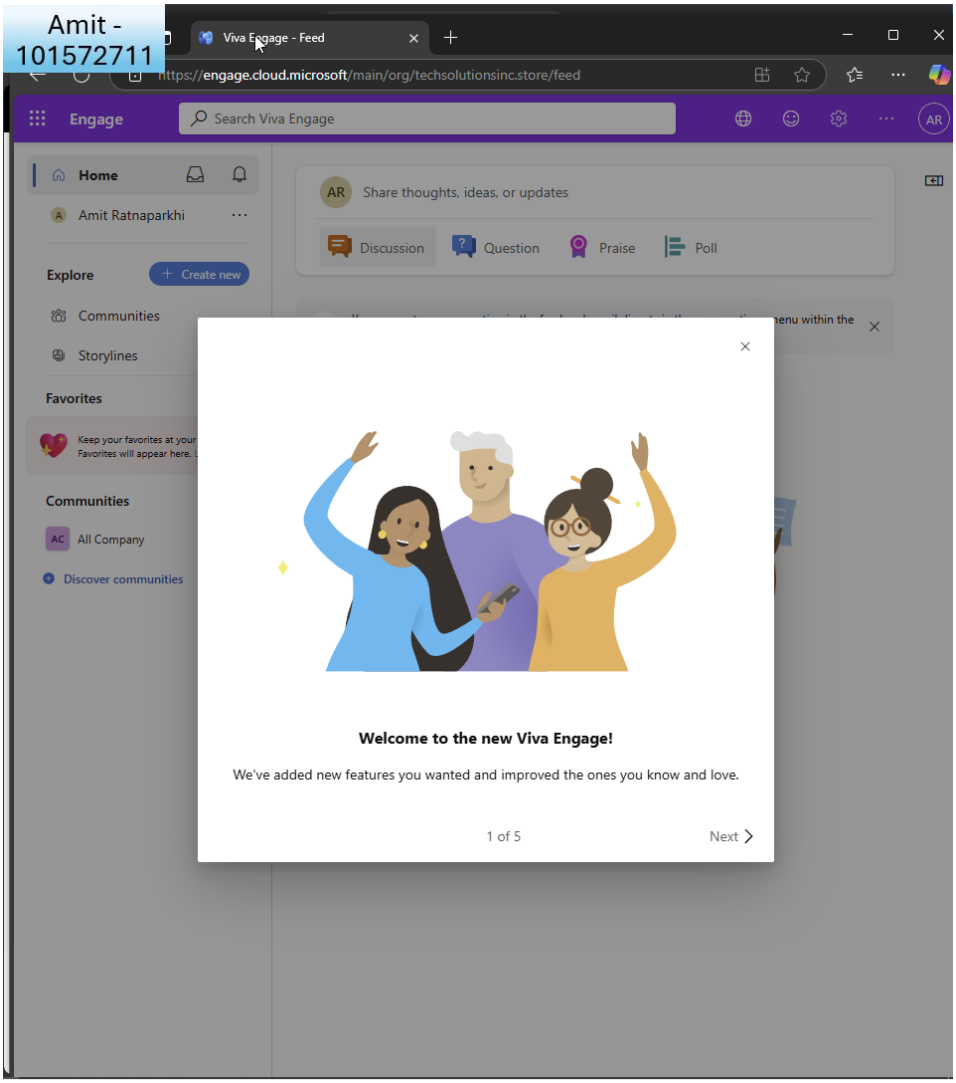
Student Name: ……. Term: ……..
Student ID: ……..

3. **Set Up Viva Engage for Enterprise Social Networking**:
    - Configure Viva to allow only internal communications.



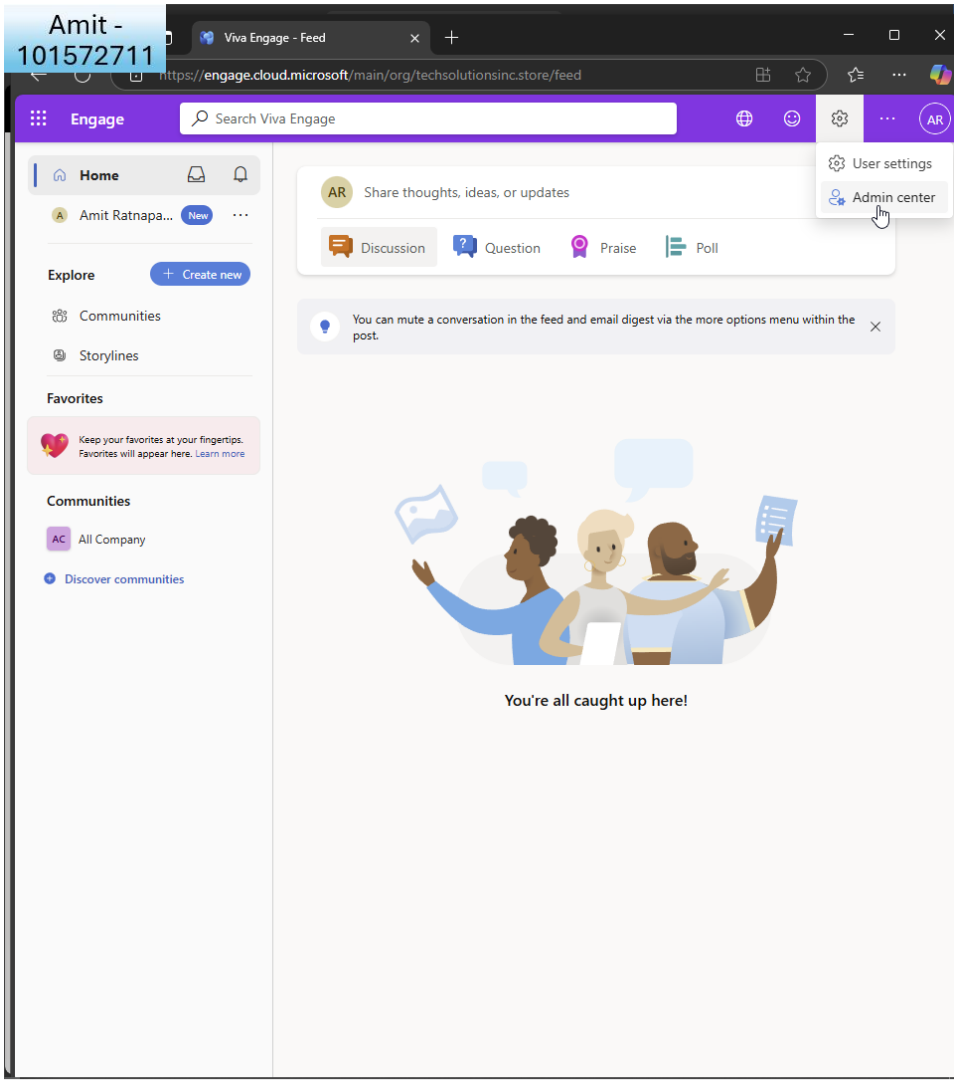
I choose 'Viva Engage' from all admin centres

Student Name: ……. Term: ……..
Student ID: ……..



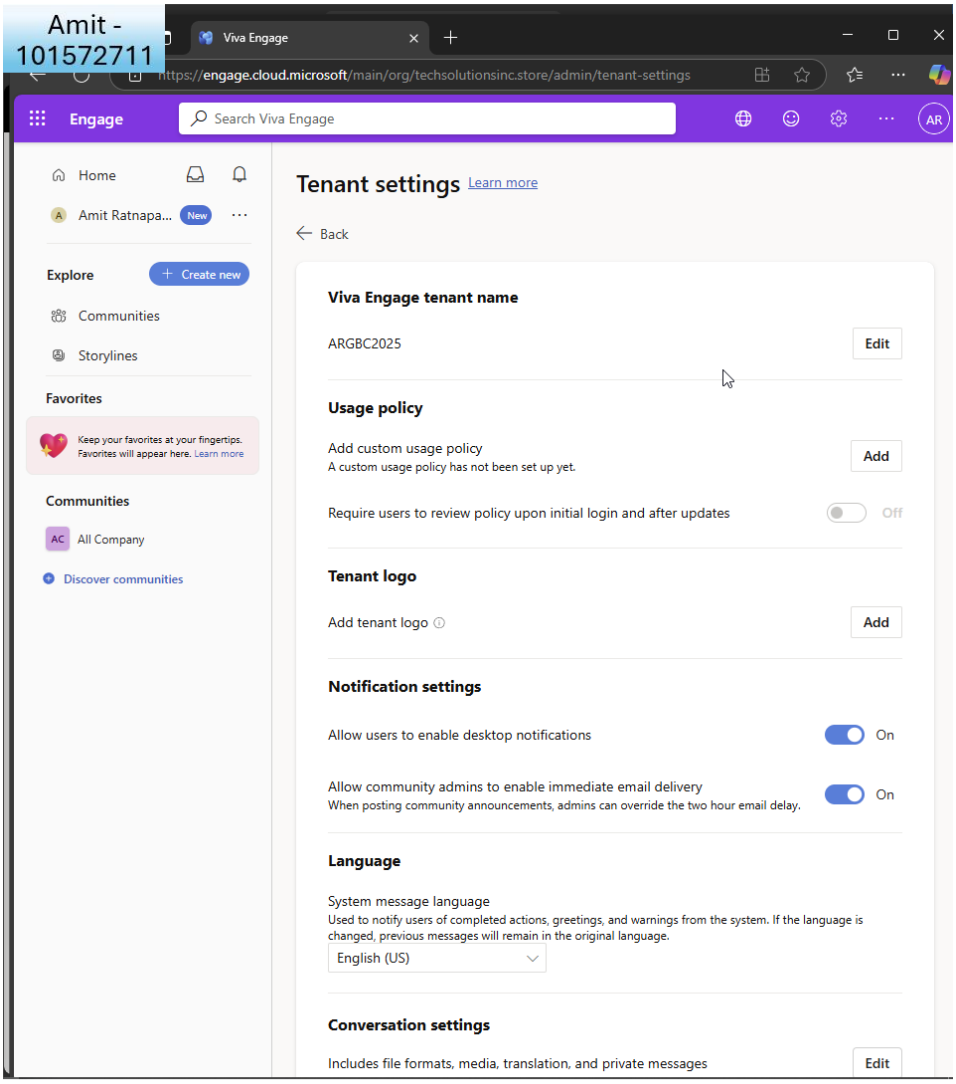
I see the welcome screen for the new viva engage

Student Name: ……. Term: ……..
Student ID: ……..



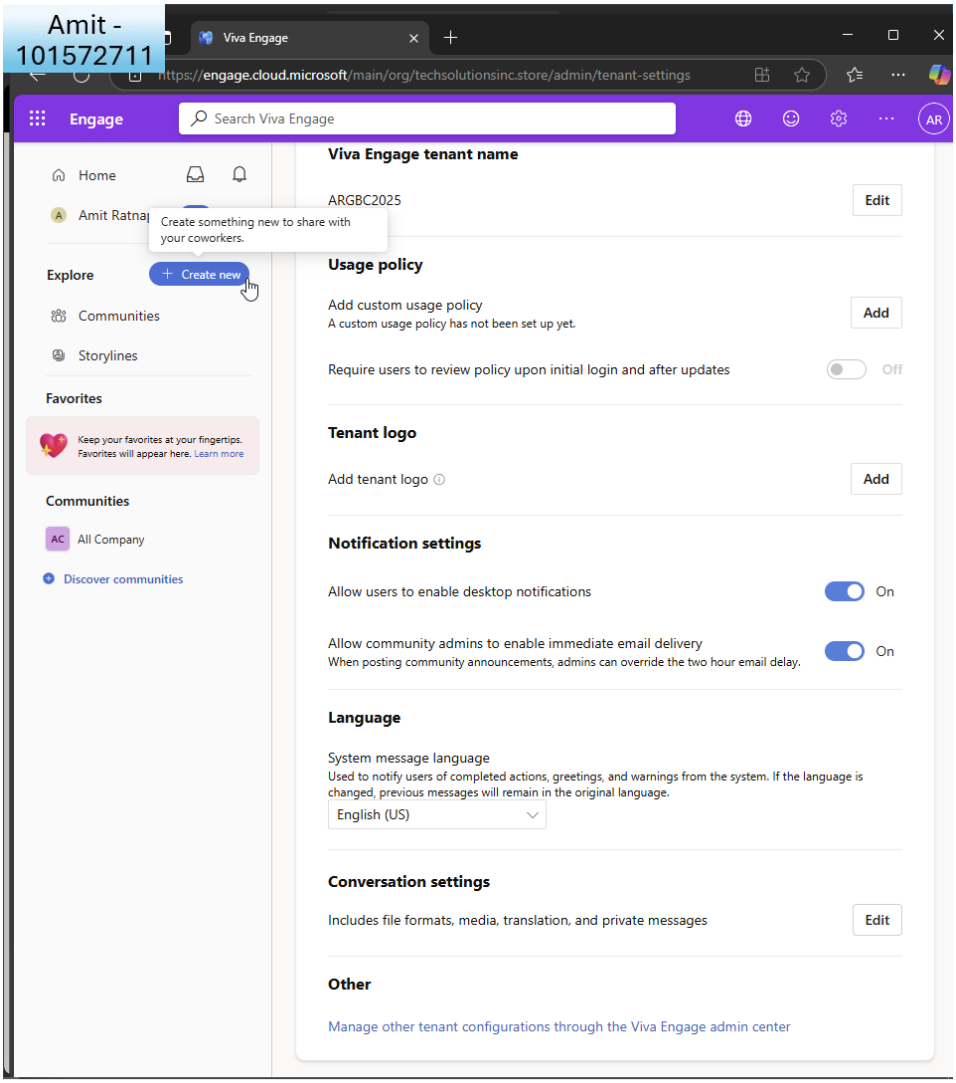
I click ’admin cerntre’

Student Name: ……. Term: ……..
Student ID: ……..



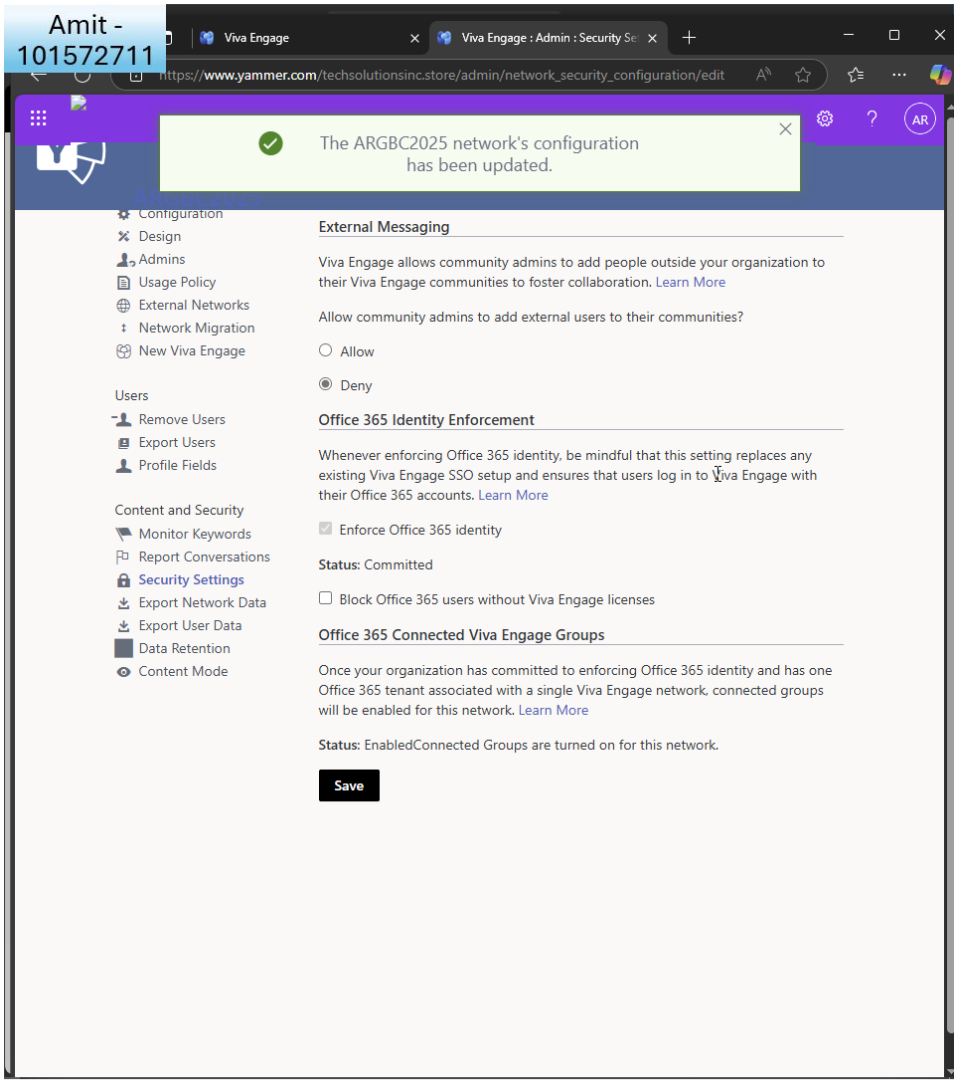
I see the tenant settings

Student Name: ……. Term: ……..
Student ID: ……..



I click ’other tenant configurations’ at the bottom

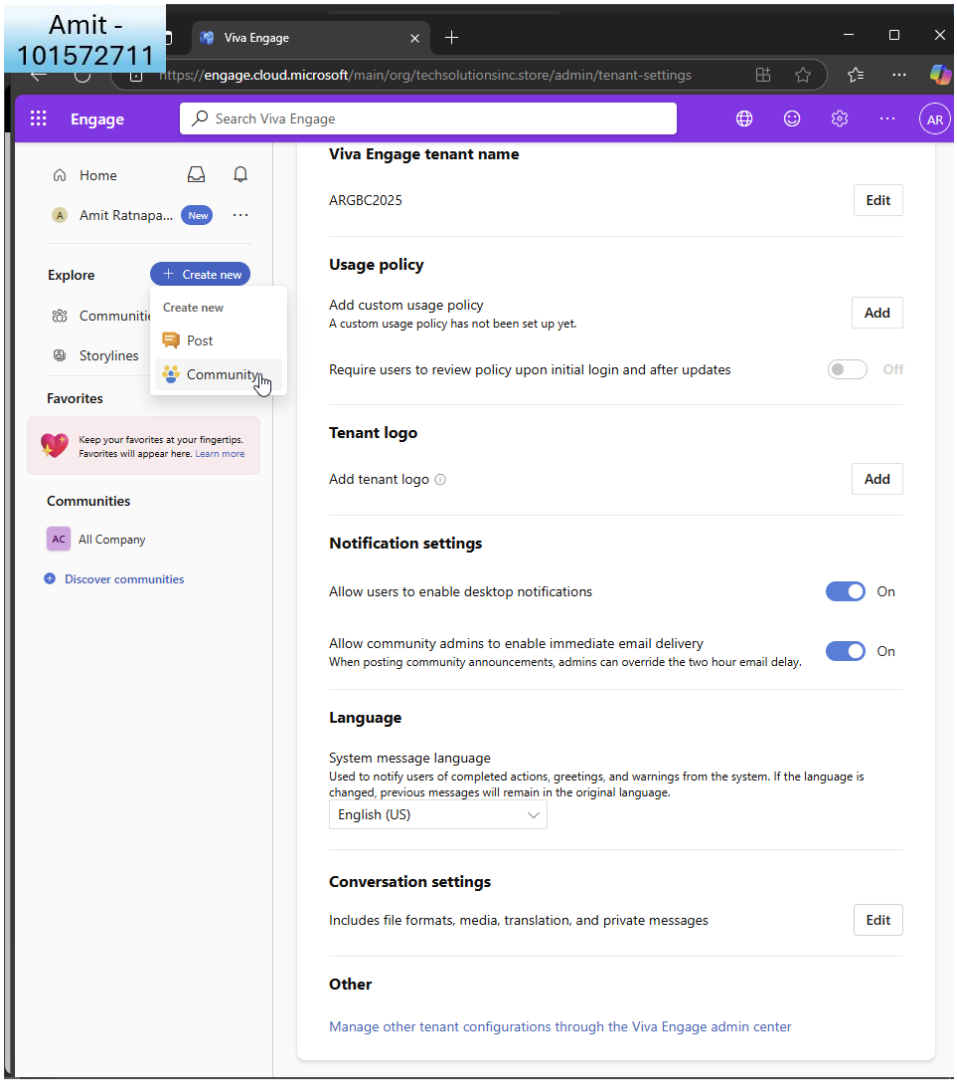
Student Name: ……. Term: ……..
Student ID: ……..



I choose to ‘deny’ the ability for community admins to add external users

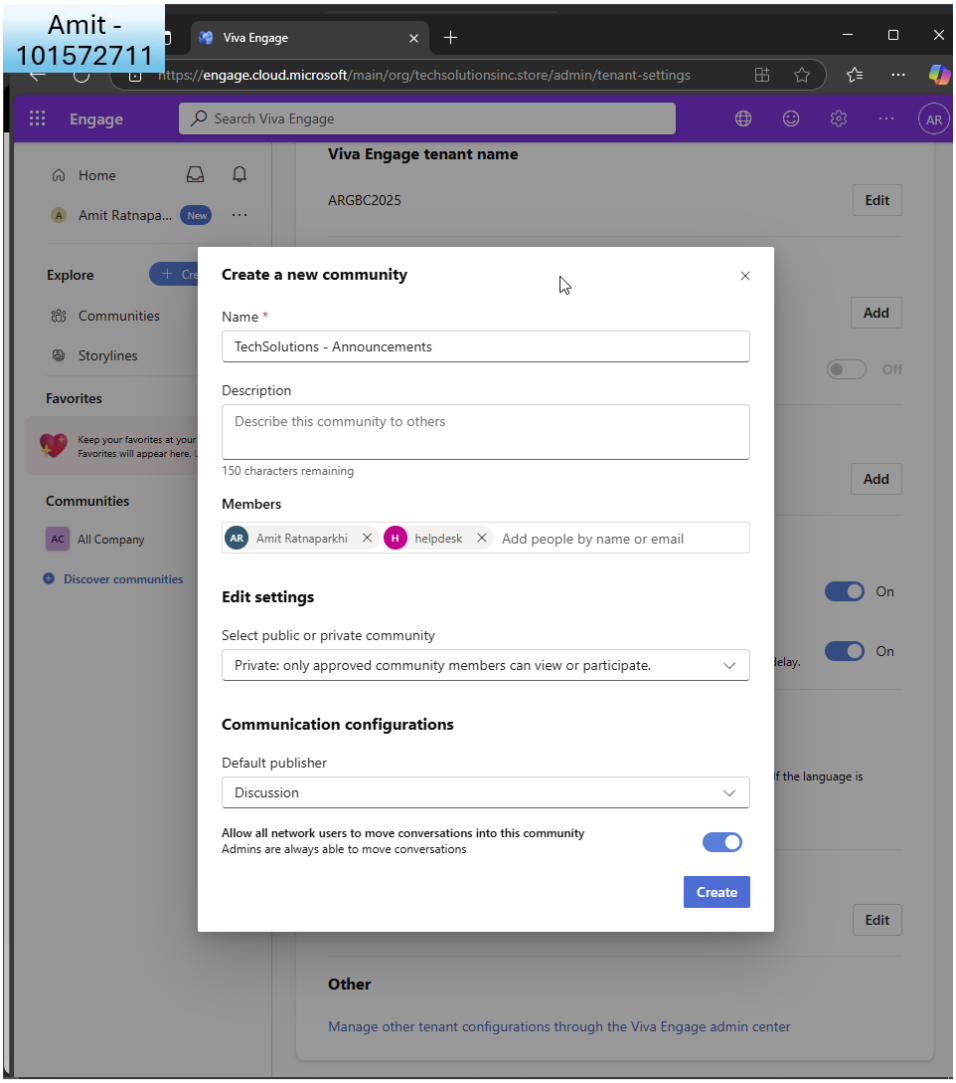
Student Name: ……. Term: ……..
Student ID: ……..

- Set up groups for company-wide announcements and department-specific discussions.



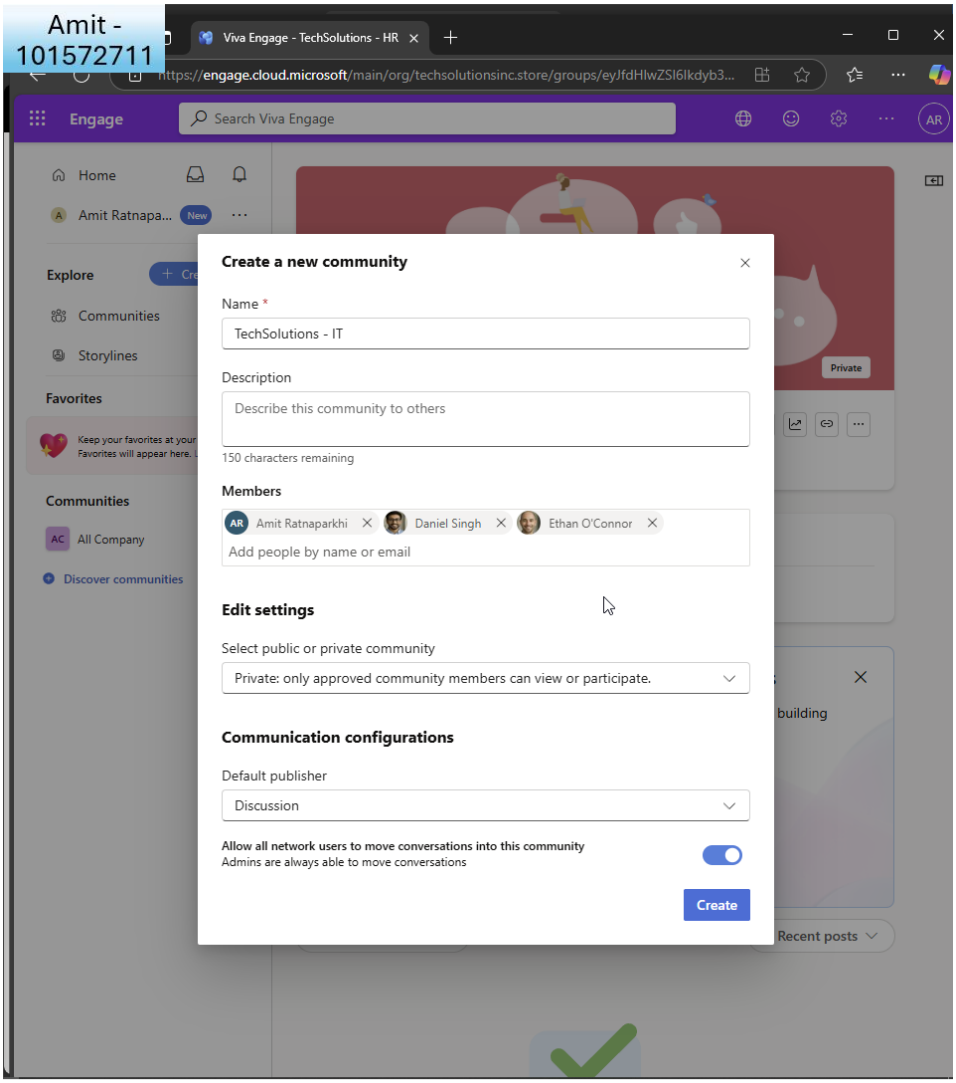
I go back to the main menu and 'create new community'

Student Name: ……. Term: ……..
Student ID: ……..



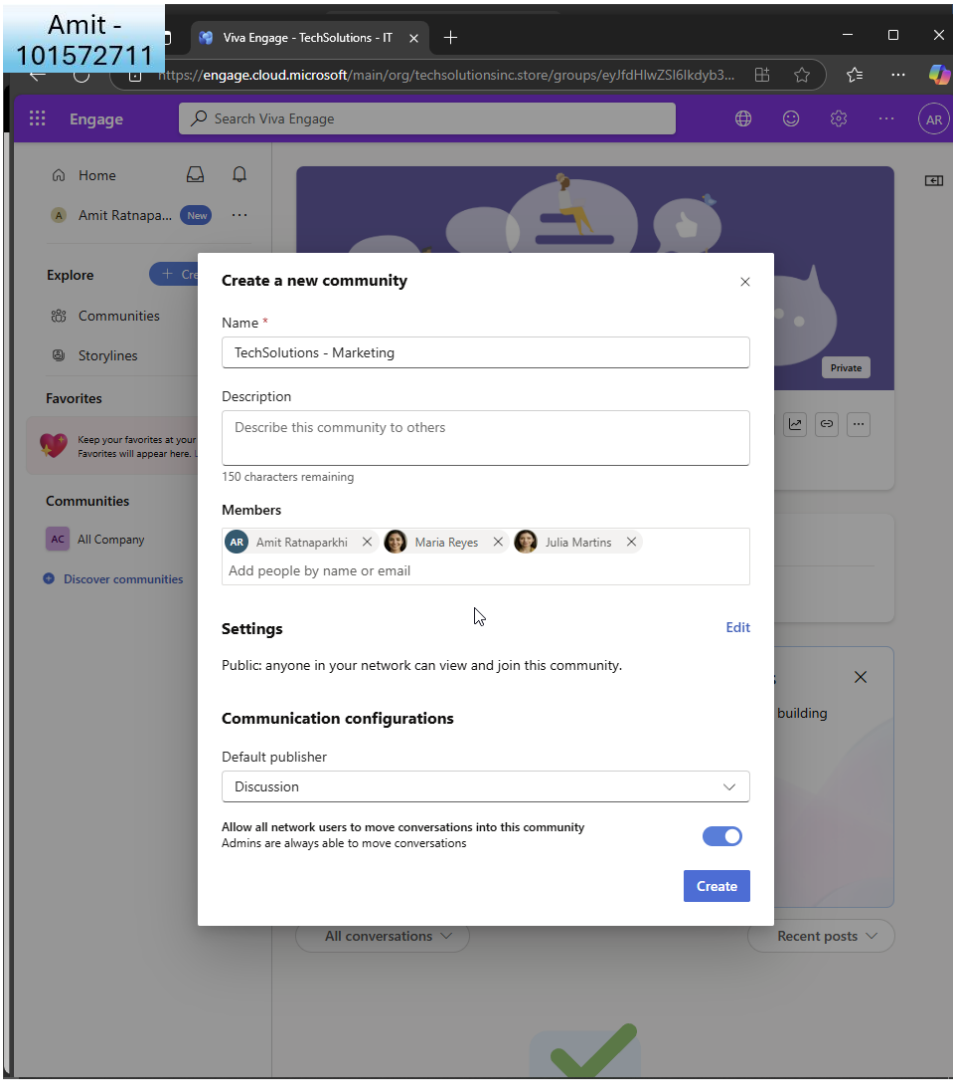
I create a new community for announcements, make it private and add GA and helpdesk

Student Name: ……. Term: ……..
Student ID: ……..



I do the same for IT department and add GA, and IT leads

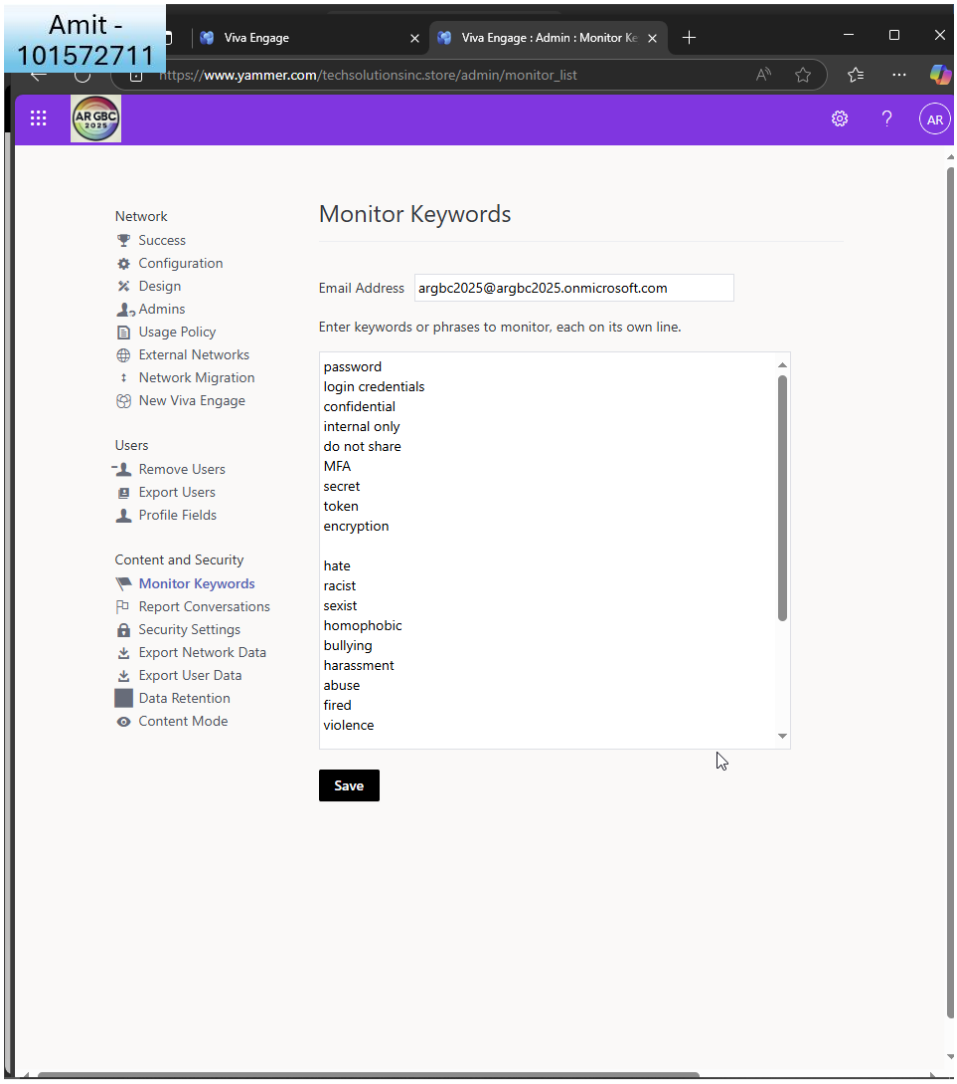
Student Name: ……. Term: ……..
Student ID: ……..



Once more I do the same for Marketing, add GA and marketing leads. I make this one public.

- Ensure compliance with the company's social media policy.

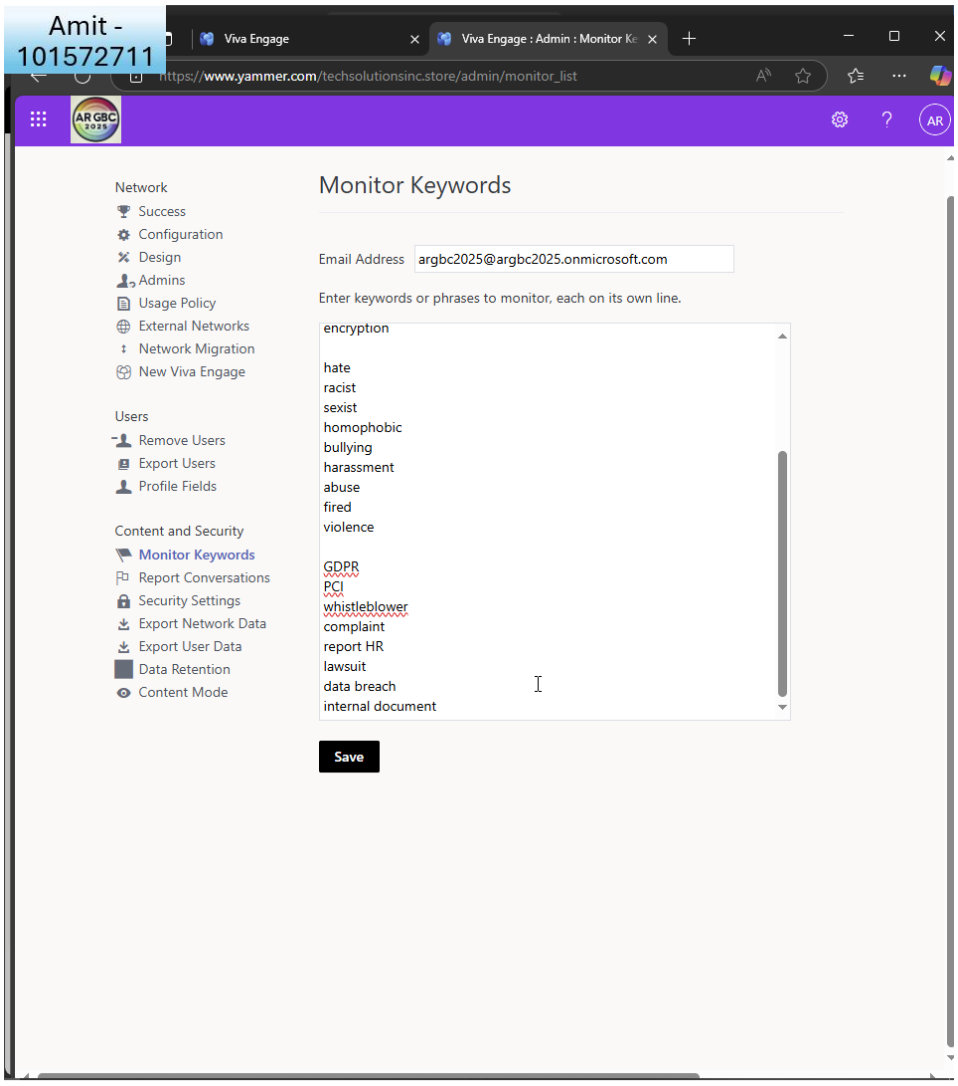
Student Name: ……. Term: ……..
Student ID: ……..



I go back to security settings for the tenant and click ’monitor keywords’ and add some

Student Name: ……. Term: ……..
Student ID: ……..

keywords to monitor.



Here are some more.

~~~~~~

Student Name: …………………………. Term: …………………………..
Student ID: ………………………………..

~~~~~~

Part B:

Wow this task was so very eye-opening! it was like experiencing creating a real workplace start to finish. I started in SharePoint and created the IT, HR, and Marketing departmental sites in seperate of one another. Organising different document libraries and doing permissions gave a feel for the work that even the simplest aspect, like who sees what, entails. I like how MS365 organises this. Within the HR site, I enabled versioning and content approval, and it was really simple once I had located the settings, and it really made sense of how sensitive documents are managed in real organisations. I like how MS365 showcases this.

OneDrive work opened my eyes to compliance and retention at a different level altogether but I got so confused that onedrive is managed by sharepoint now! I disabled external sharing, then set policies to keep files for five years and auto-delete outdated files in a year's time. Learning how to create retention labels and deploy them through Microsoft Purview was so confusing at first (so many menus and policies!) but once I had it, it was powerful. I realised how important these features are when you're trying to manage data responsibly at scale.

The best part was Viva Engage, honestly. So, I set up internal sites for announcements and team chats, and it actually did feel like building the social centre of a real company. I can see this how can be someone’s full time job! I blocked external communication and even set up content filtering by keyword to highlight the important/dangerous stuff. One shock was the retirement of Yammer and moving everything to Viva. In the beginning, I was looking for the old admin centre, but it's set up differently in a way. It was a bit confusing, but it did give me some indication of how the platform is building out. It would be super useful if MS365 had access to legacy systems too.

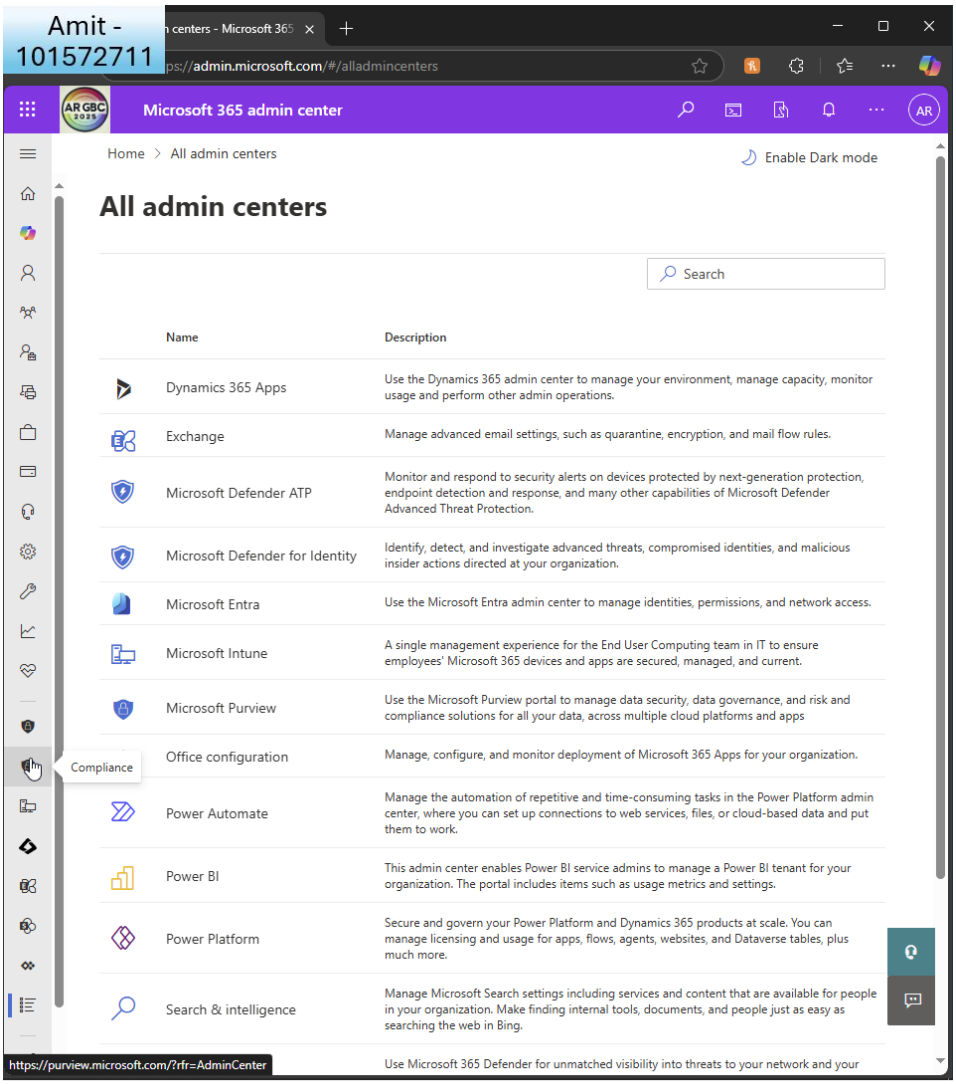
There were a couple of frustrating moments along the way. Some of the config areas were tucked away where I wasn't expecting to find them, and plenty of back-and-forthing amongst the admin centres SharePoint, Viva, Purview, the primary M365 admins, Teams. It's a lot to keep track of. Opening, closing Windows, tabs and some admin centres opened in an entirely new window and required log in details again!

Language wasn't being applied consistently either. "policy", "label", and "retention" had different meanings in different areas. And while I liked the new Viva UI, it took way too long to discover the correct settings (specifically, to block external messaging). But it did teach me a lot. Task 3 boosted my confidence in using Microsoft 365 to create safe, organised areas in which one can really work and collaborate. Much to keep track of, but also fascinating to see it all come together but I still have a lot to learn.

Student Name: …….. Term: ……..
Student ID: ……..

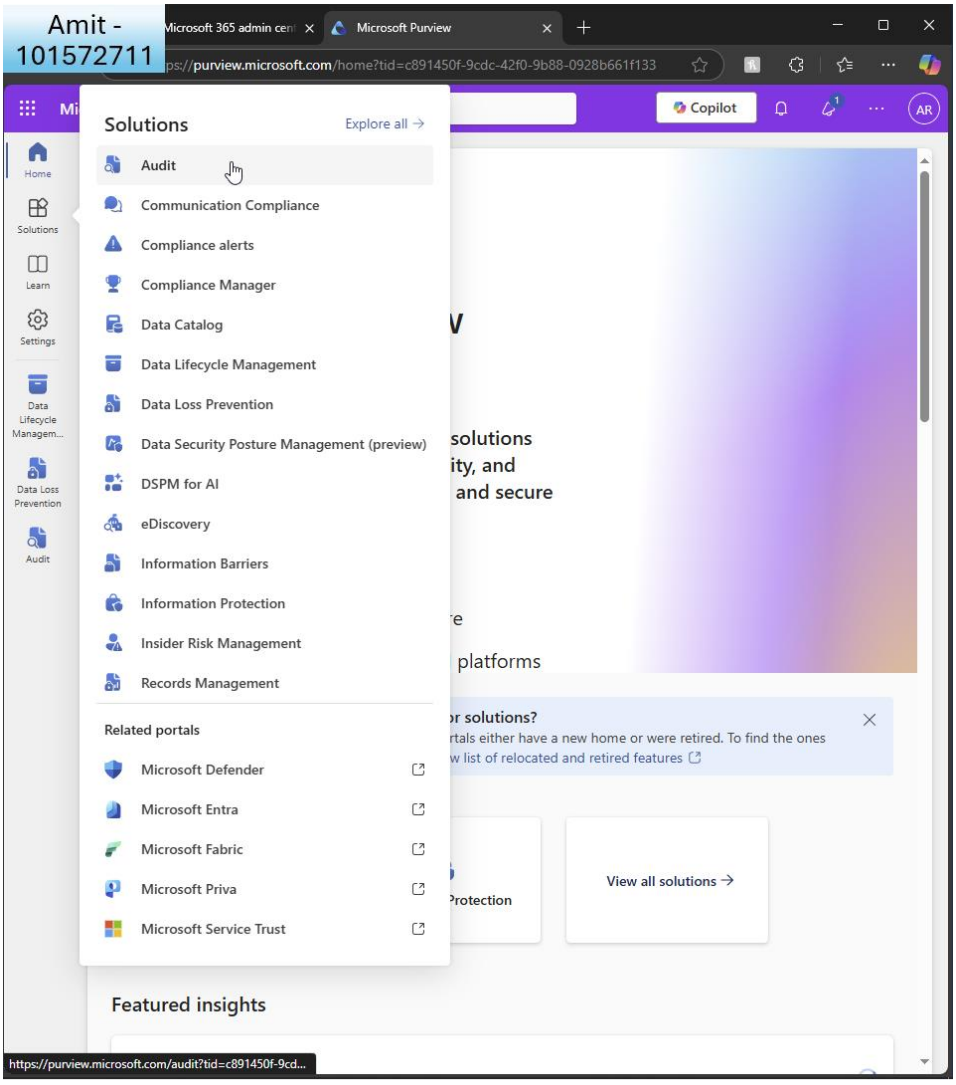
Task 4: Monitoring and Reporting

1. **Configure Audit Logs**:
    - Enable and configure audit logging in the Microsoft 365 compliance center.



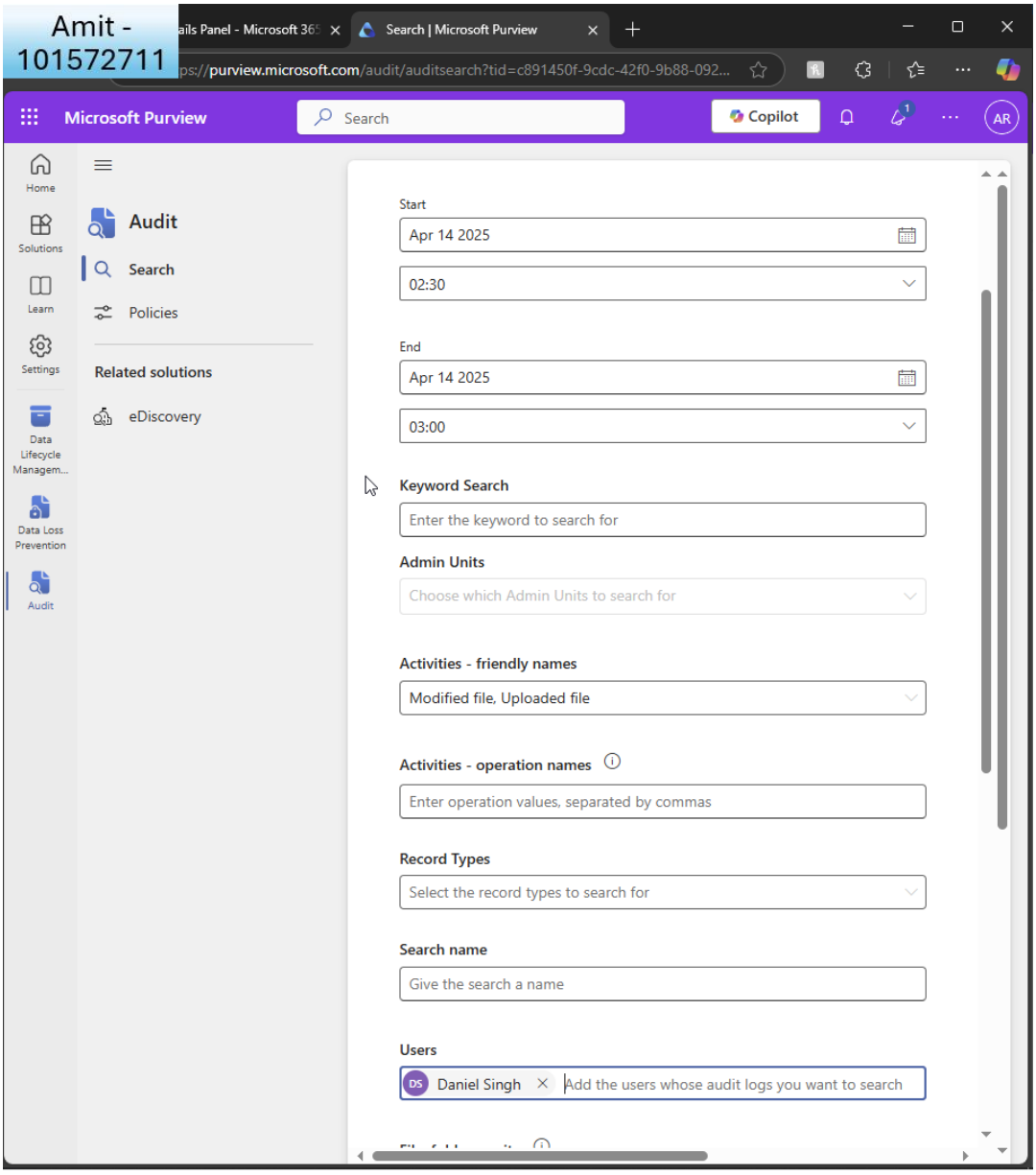
I go to the compliance centre

Student Name: ……. Term: ……..
Student ID: ……..



Under ‘solutions’ I choose ‘audit’

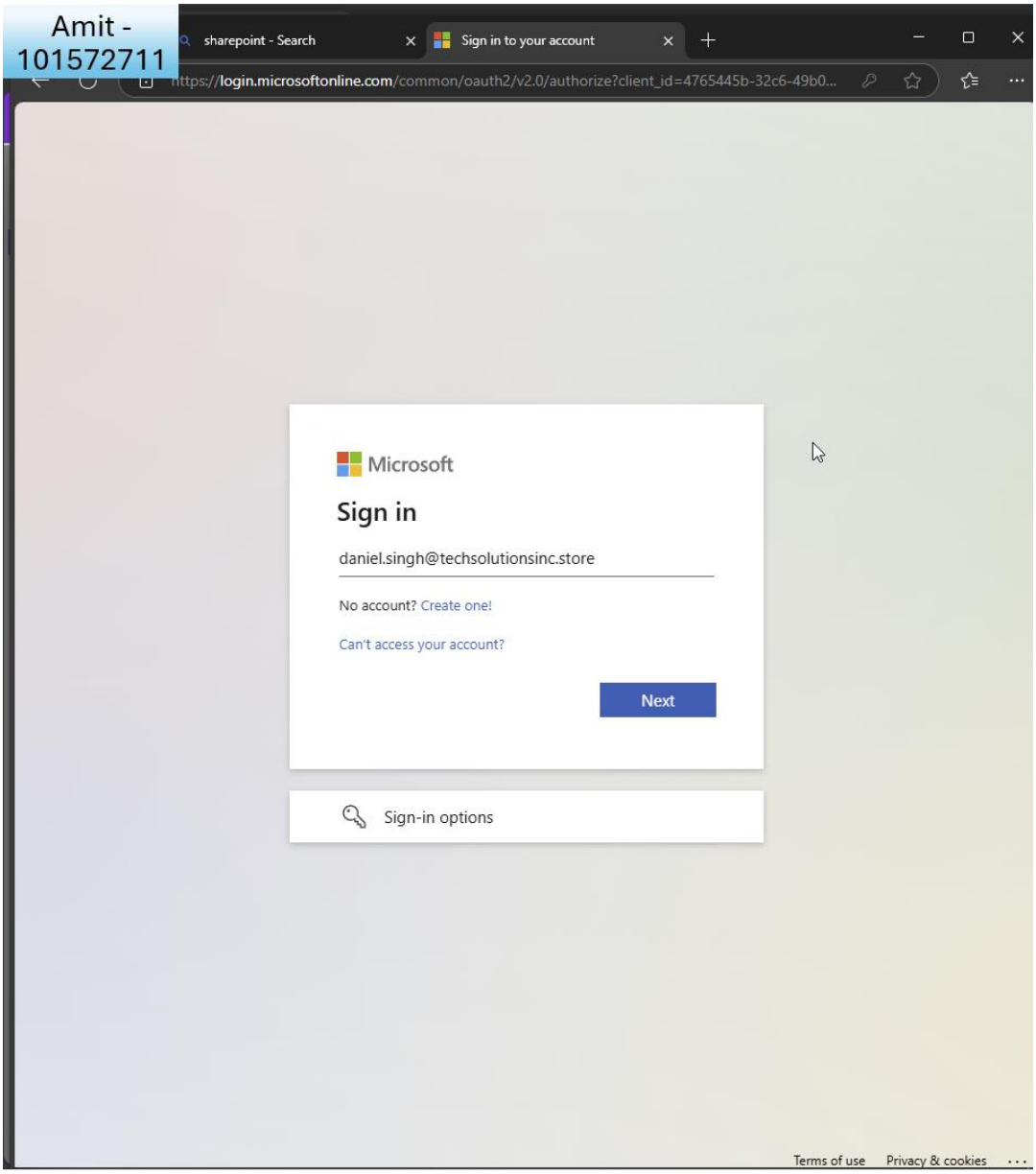
Student Name: ……. Term: ……..
Student ID: ……..



I can see auditing is already enabled (from a previous task).

Student Name: ……. Term: ……..
Student ID: ……..

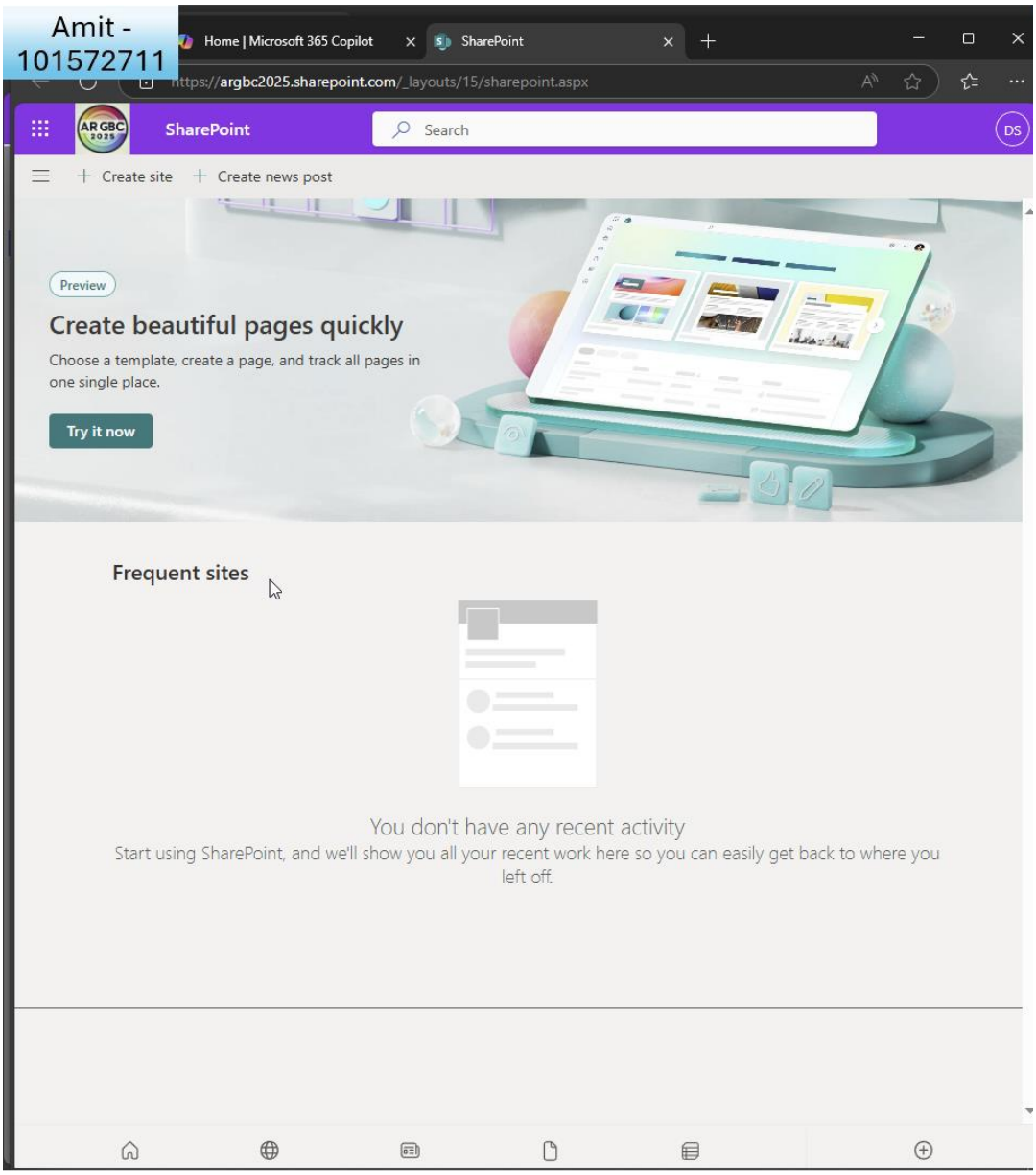
- Create a custom audit log search to track user activities related to at least one activity in SharePoint such as updating the site content



I wish to run a search for user 'Daniel' to see if he uploaded and modified a file to IT

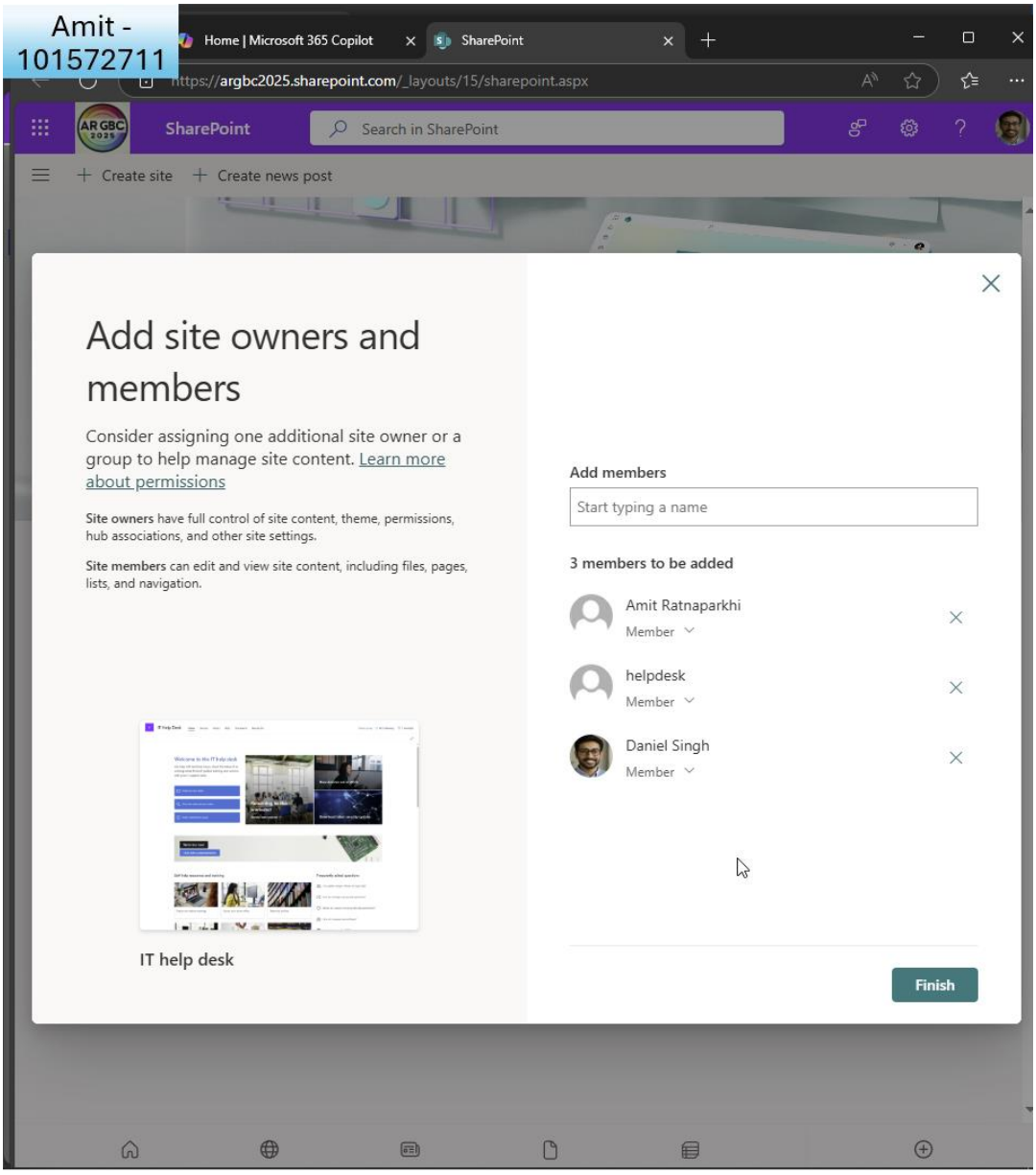
Student Name: ……. Term: ……..
Student ID: ……..

sharepoint site. I log in as him to replicate the actions.



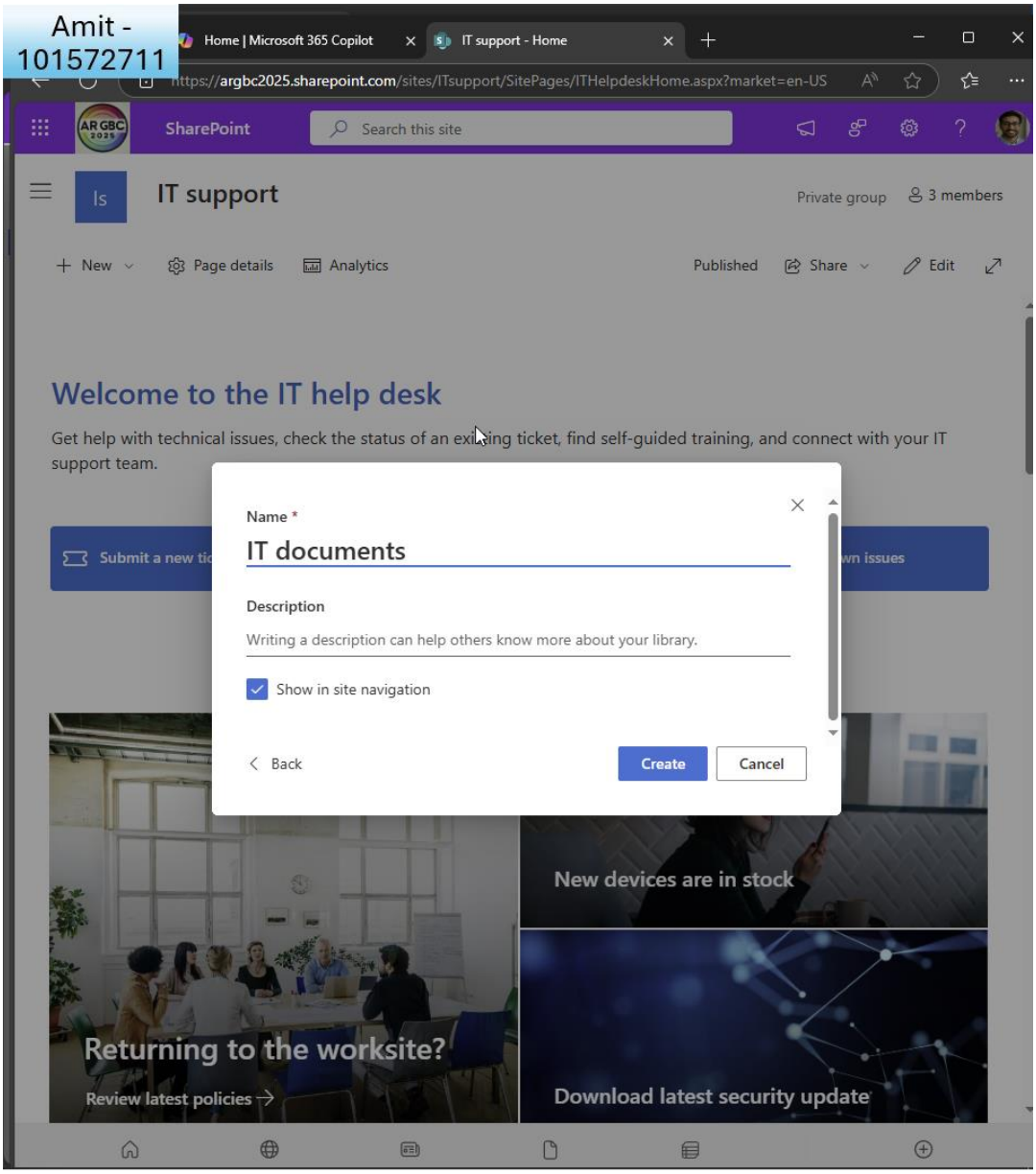
First I must create a site within IT sharepoint

Student Name: ……. Term: ……..
Student ID: ……..



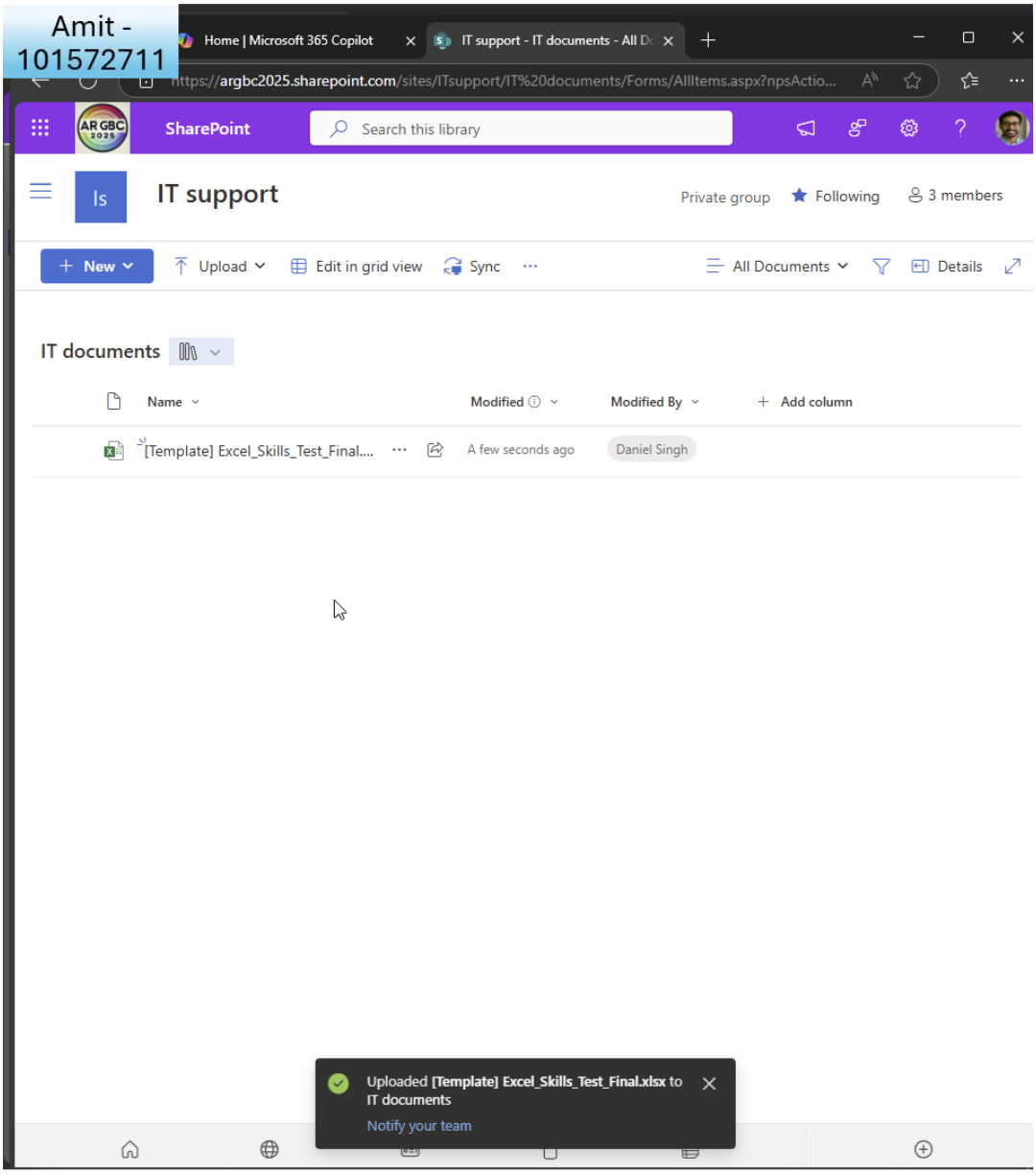
I add ’Daniel’ with GA and helpdesk as members

Student Name: ……. Term: ……..
Student ID: ……..



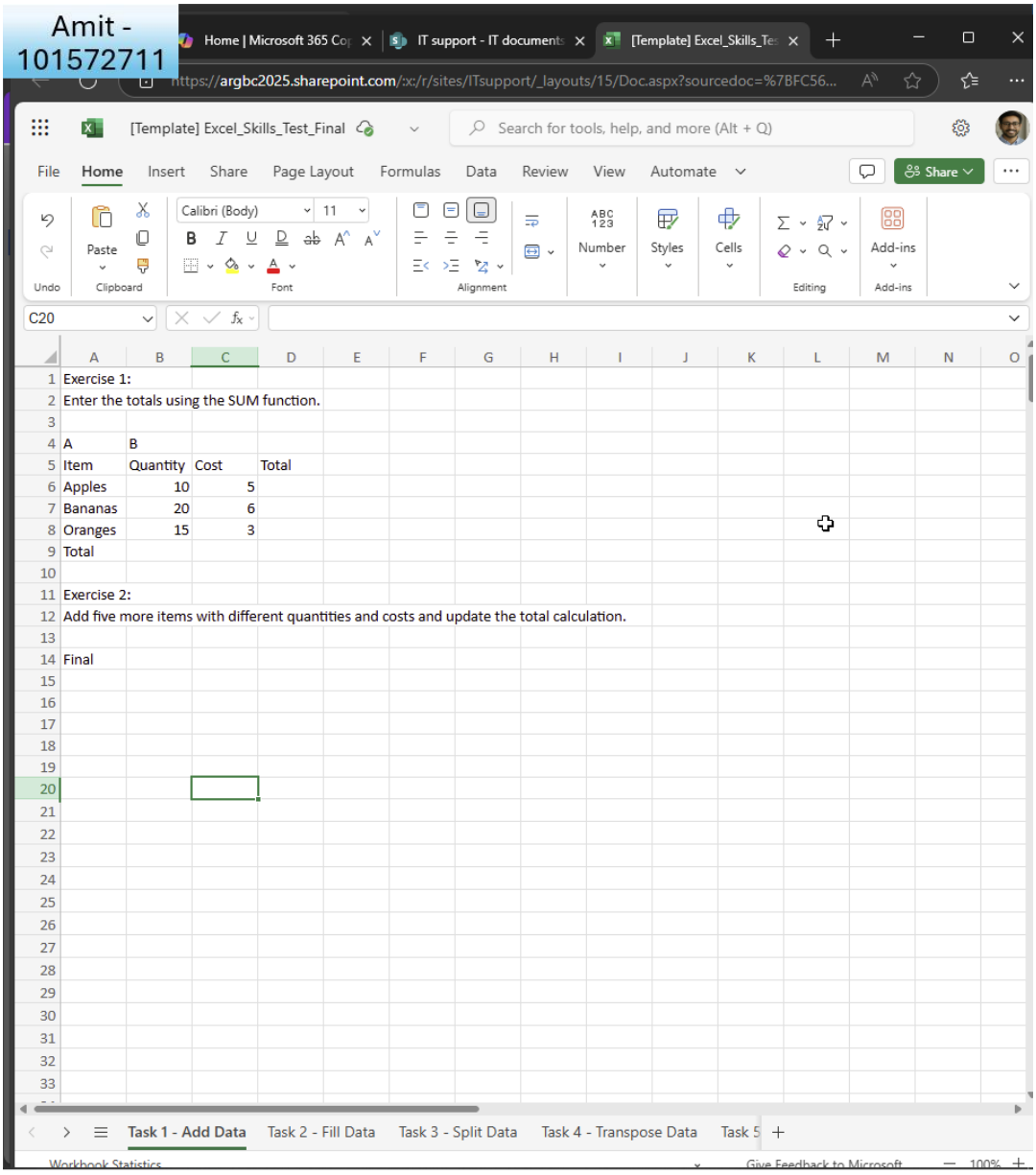
I create an 'IT documents' page

Student Name: ……. Term: ……..
Student ID: ……..



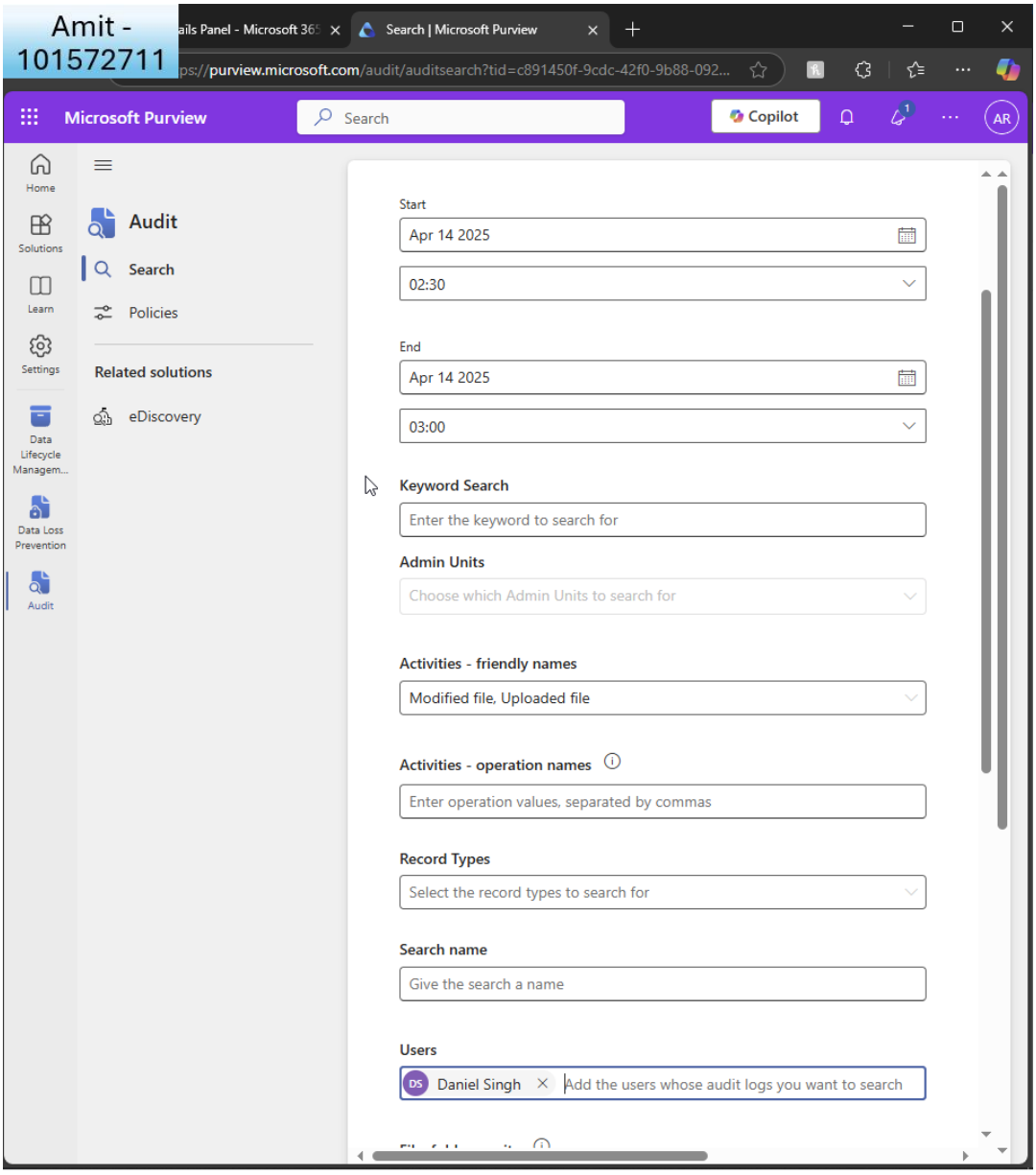
I log in as Daniel once more and upload an excel file

Student Name: ……. Term: …….
Student ID: ……..



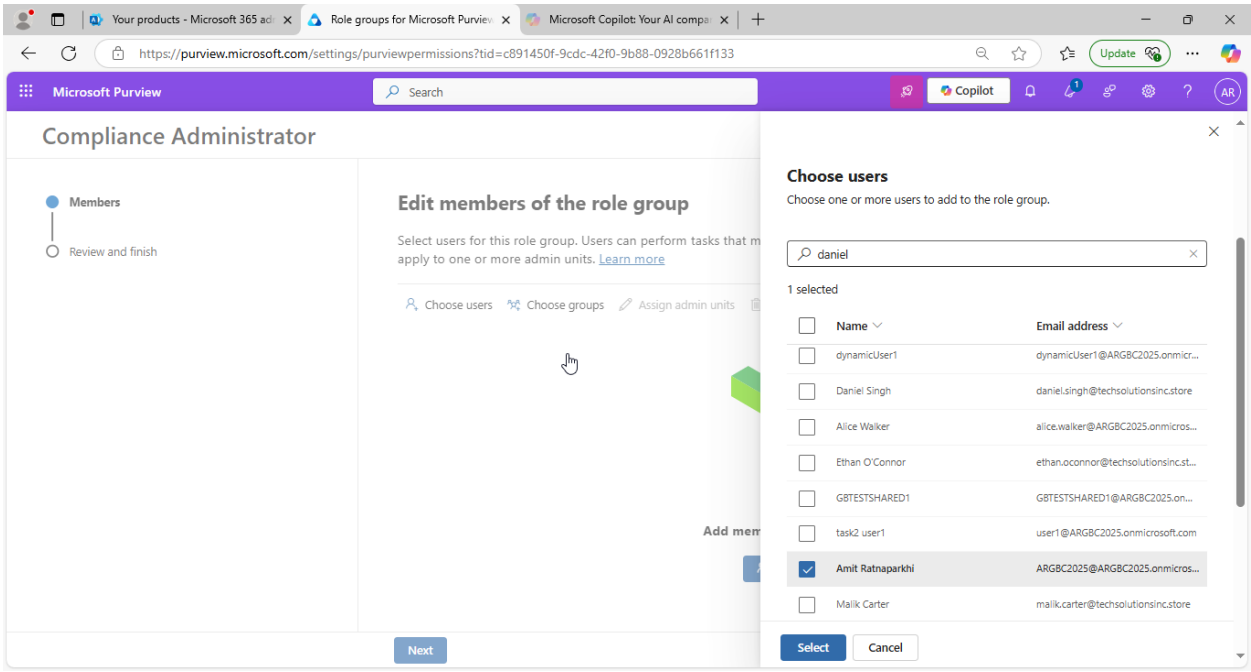
I modify the file

Student Name: ……. Term: ……..
Student ID: ……..

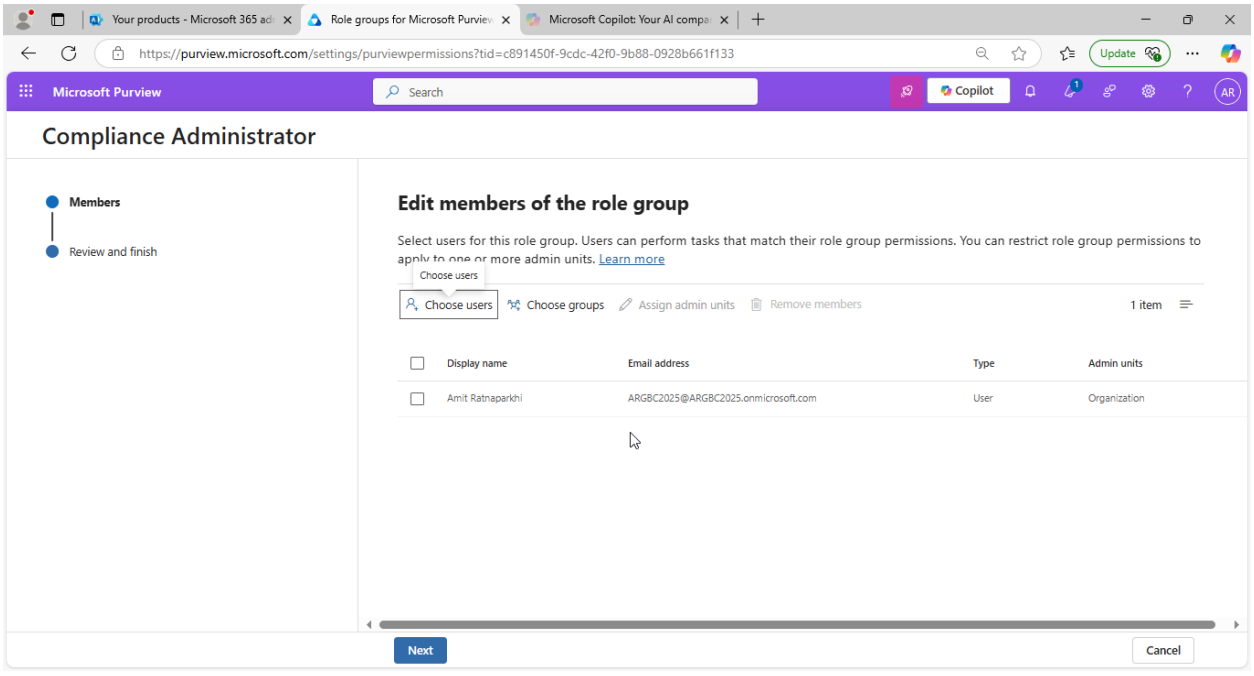


I now wait 30 minutes and run a search to see any modified/uploaded files by Daniel today

Student Name: ……. Term: ……..
Student ID: ……..

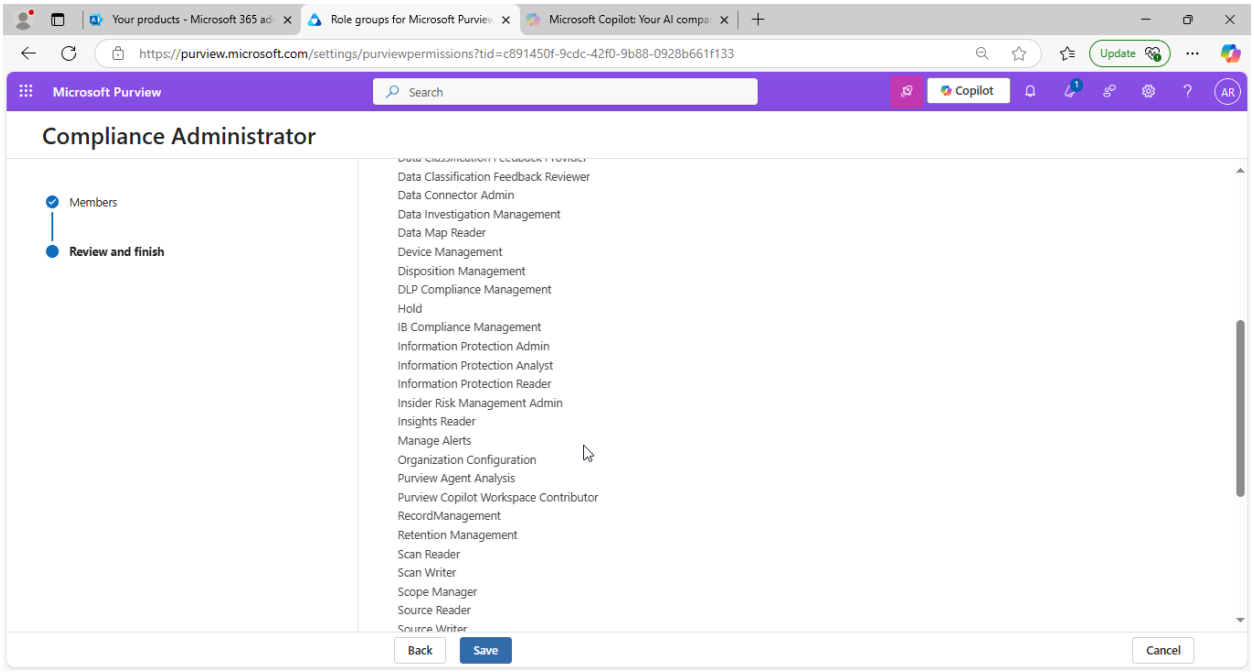


I realise I need to assign the role of 'compliance administrator' to the GA before I can run audits

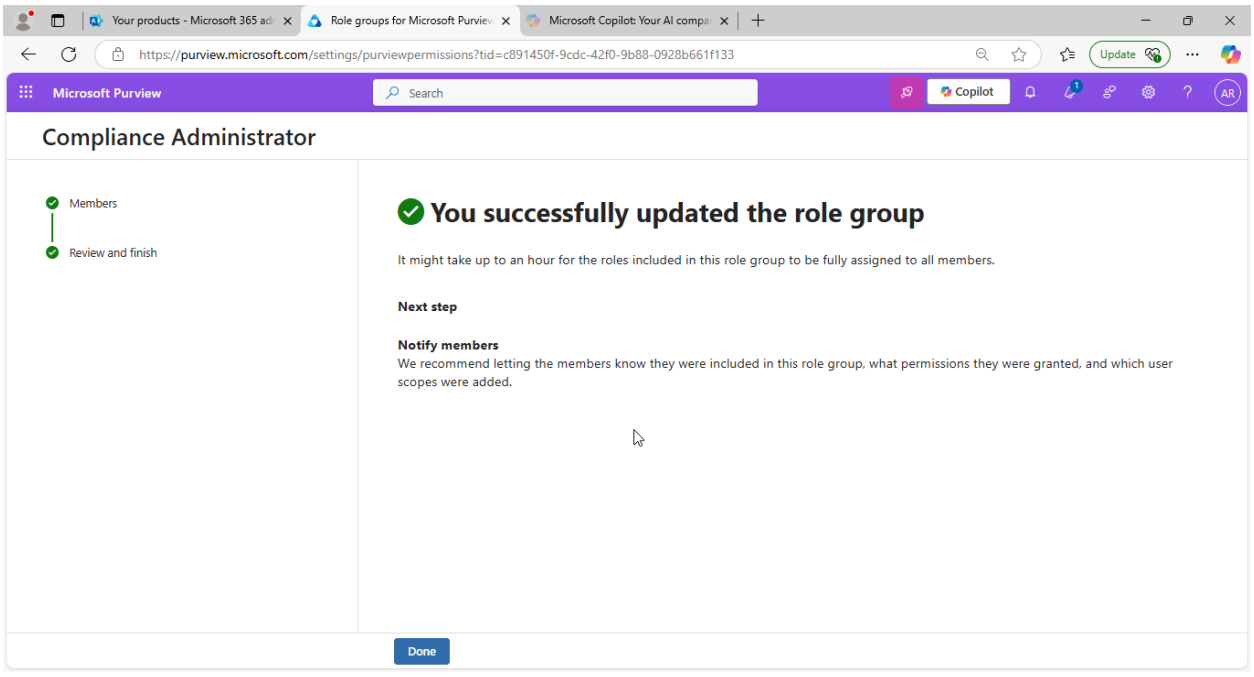


Student Name: ……. Term: ……..
Student ID: ……..

I assign the role to GA

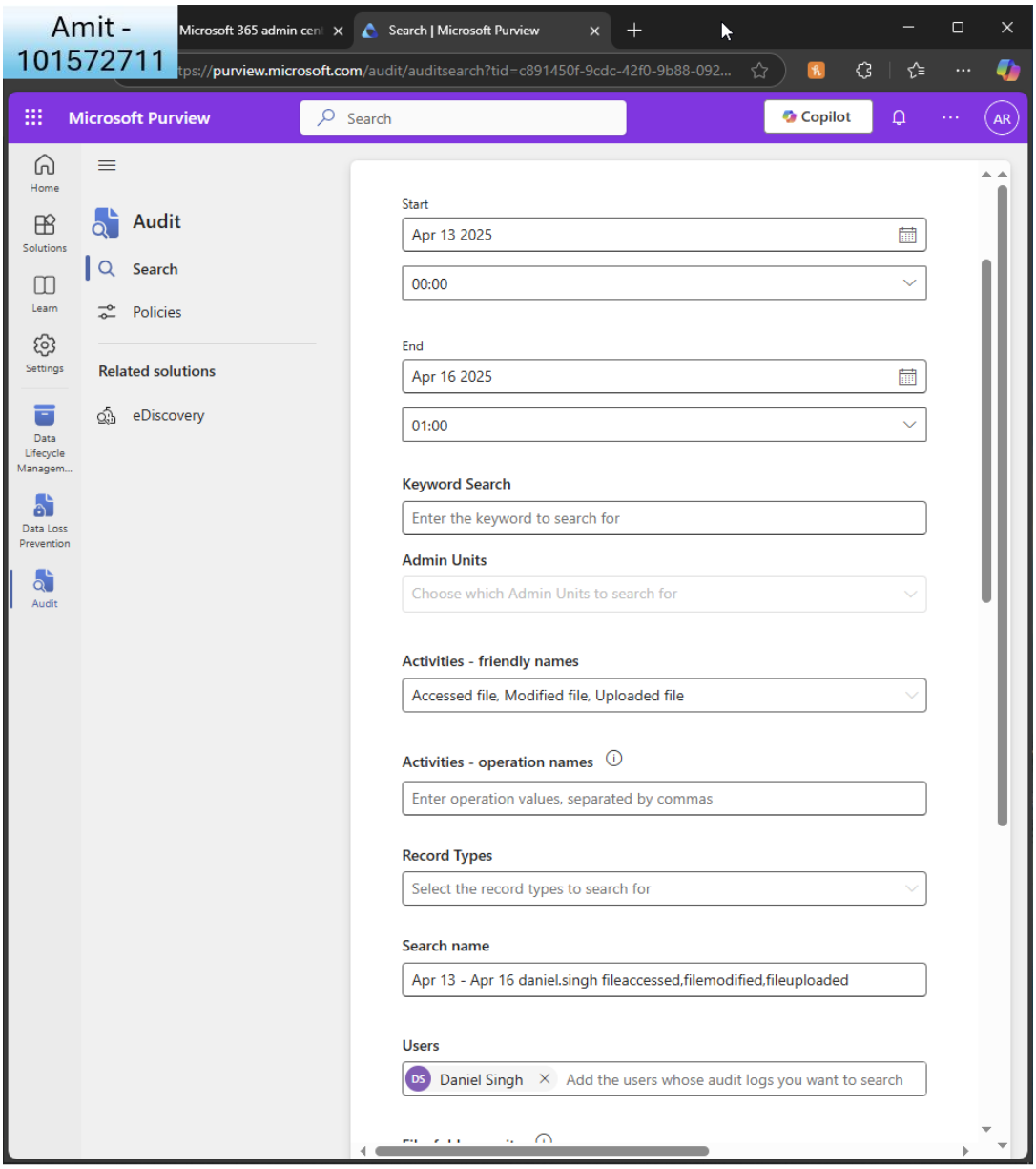


I click 'save'



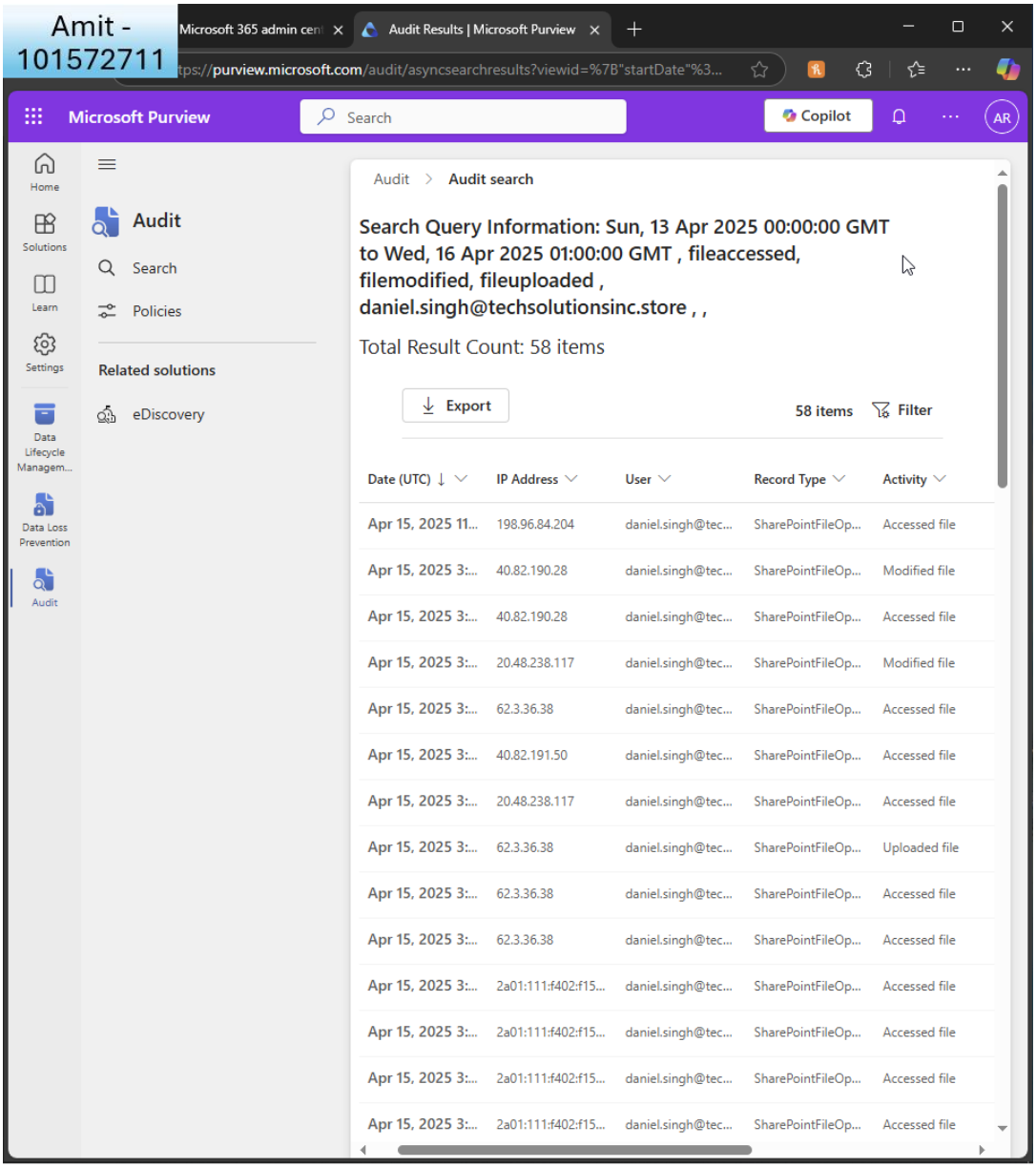
Student Name: ……. Term: ……..
Student ID: ……..

I see the confirmation



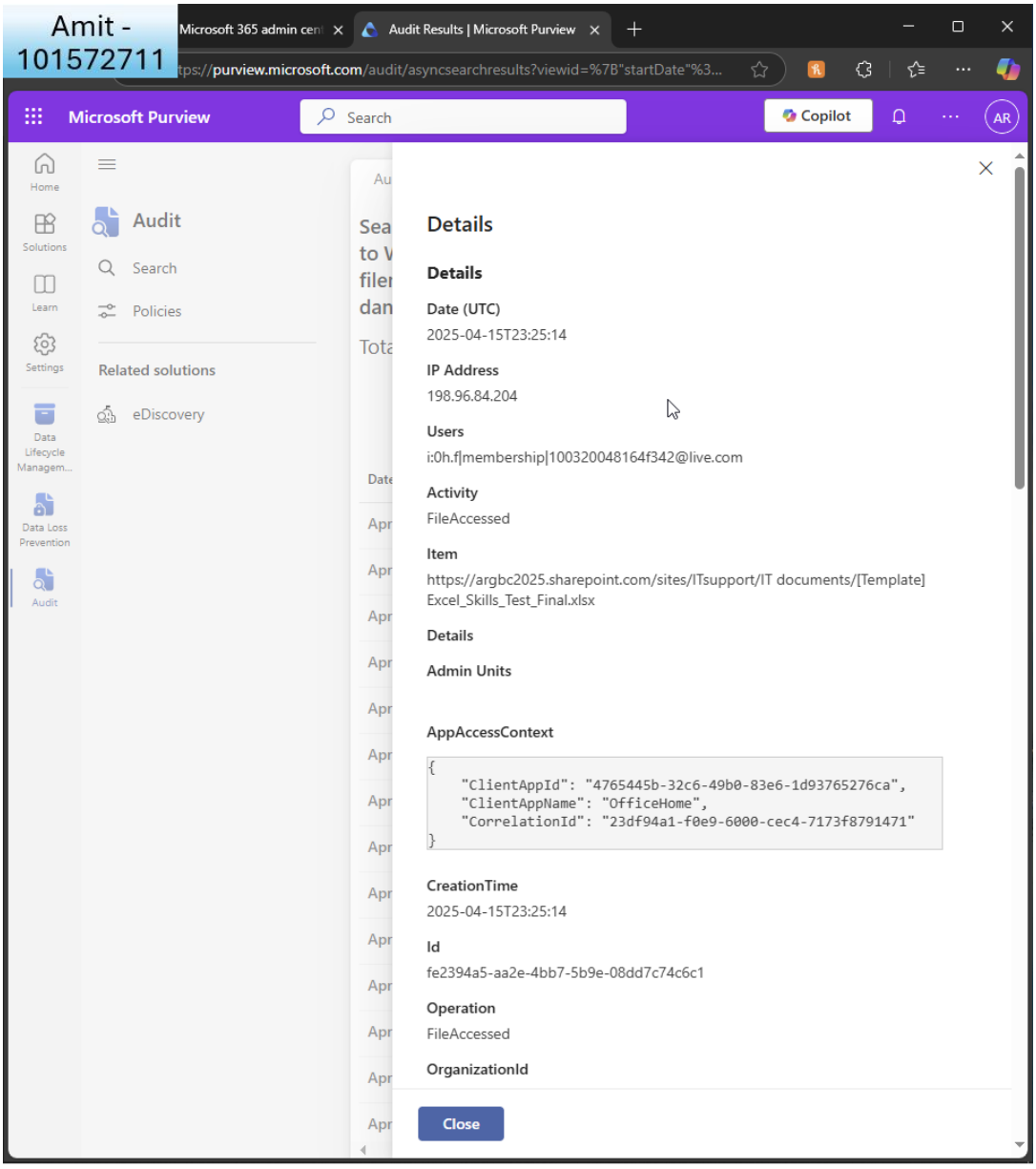
Student Name: ……. Term: ……..
Student ID: ……..

And I create a search for any file that Daniel has accessed, uploaded or modified in the past 3 days



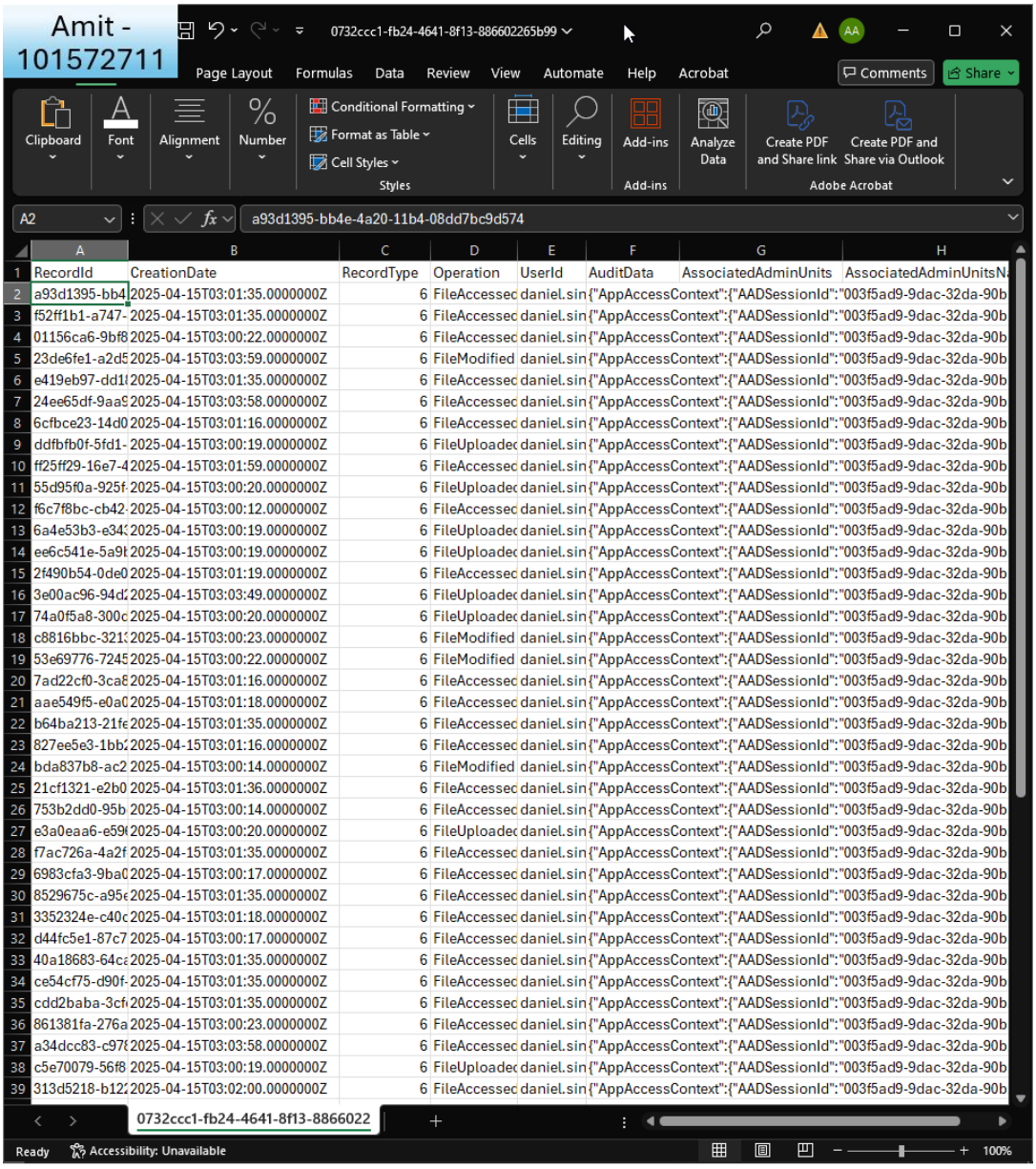
I receive the results

Student Name: ……. Term: ……..
Student ID: ……..



I click on the latest, for example

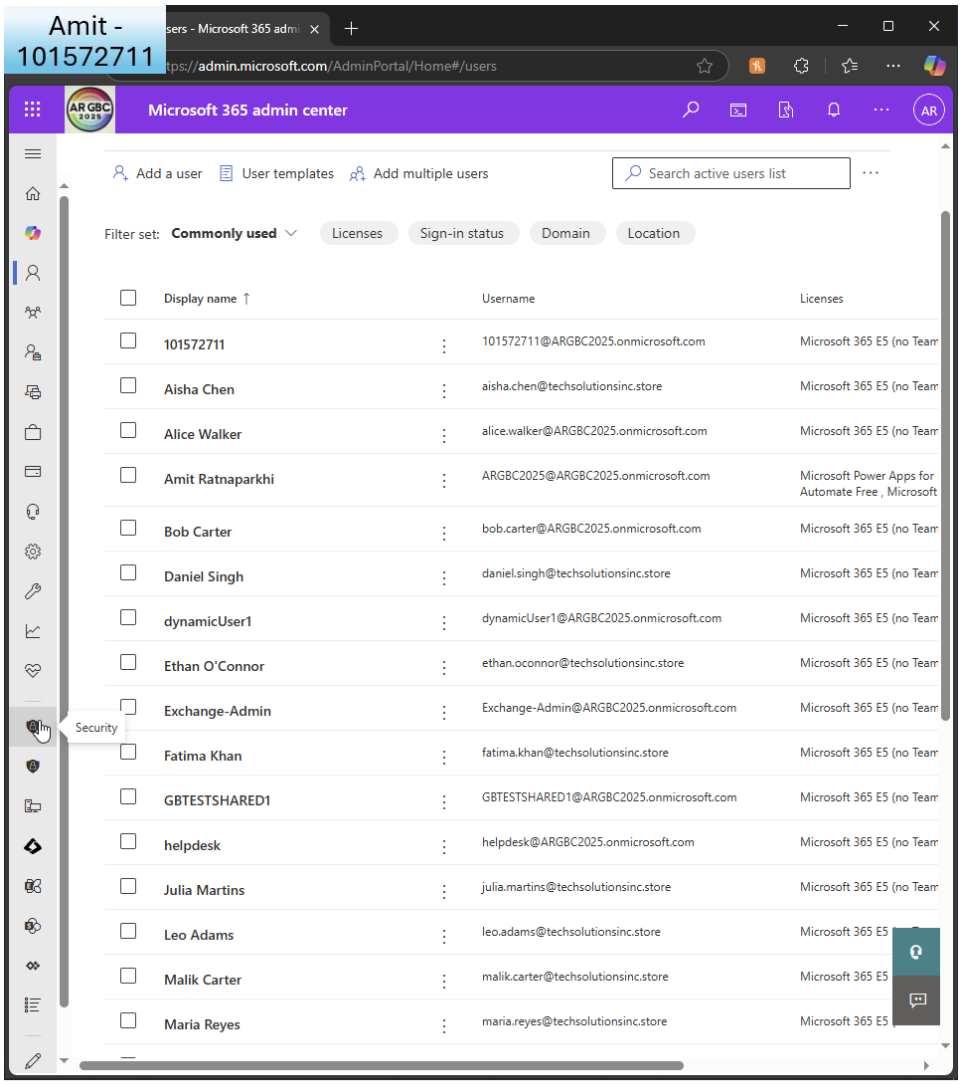
Student Name: ……. Term: ……..
Student ID: ……..



I export the logs as CSV and open in Excel to examine further

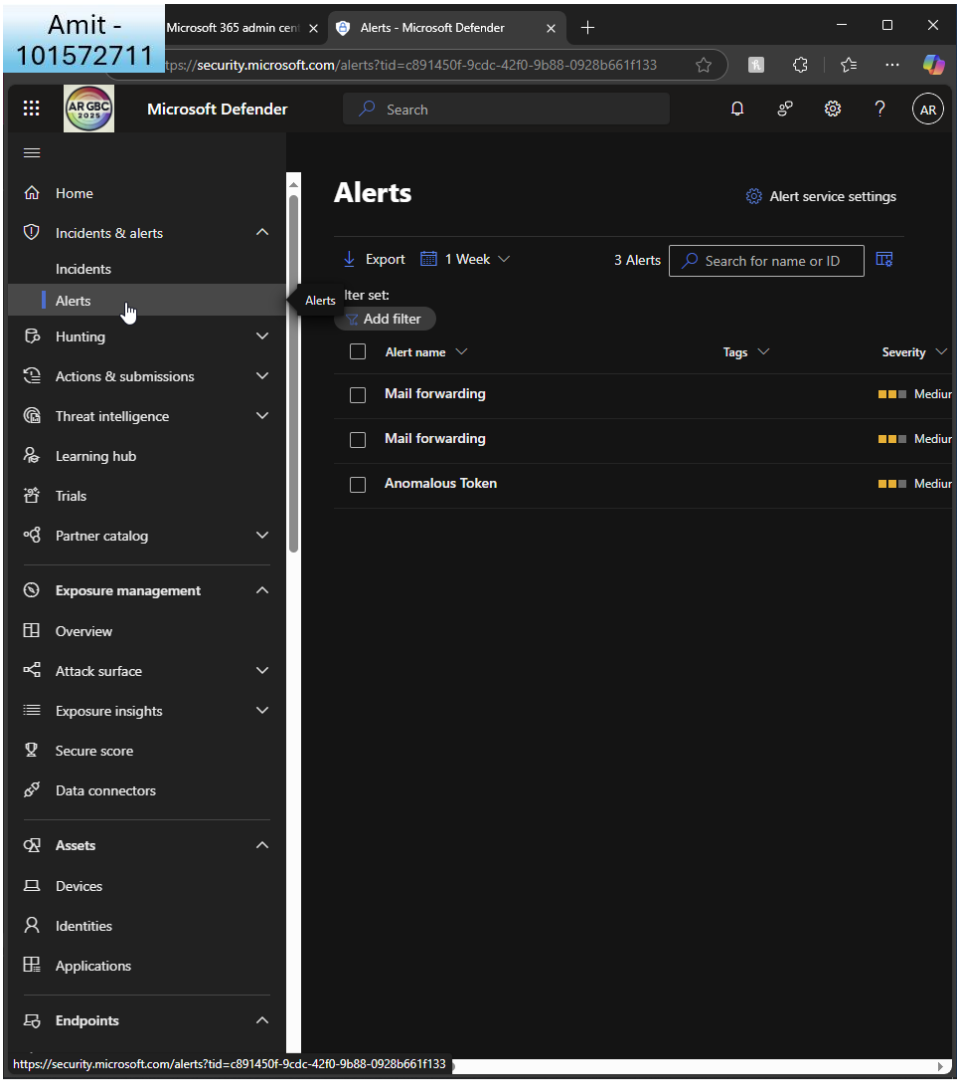
Student Name: ……. Term: ……..
Student ID: ……..

2. **Set Up Alerts**:
    - Configure alert policies to notify administrators of suspicious activities, such as multiple failed login attempts or mass deletion of files.



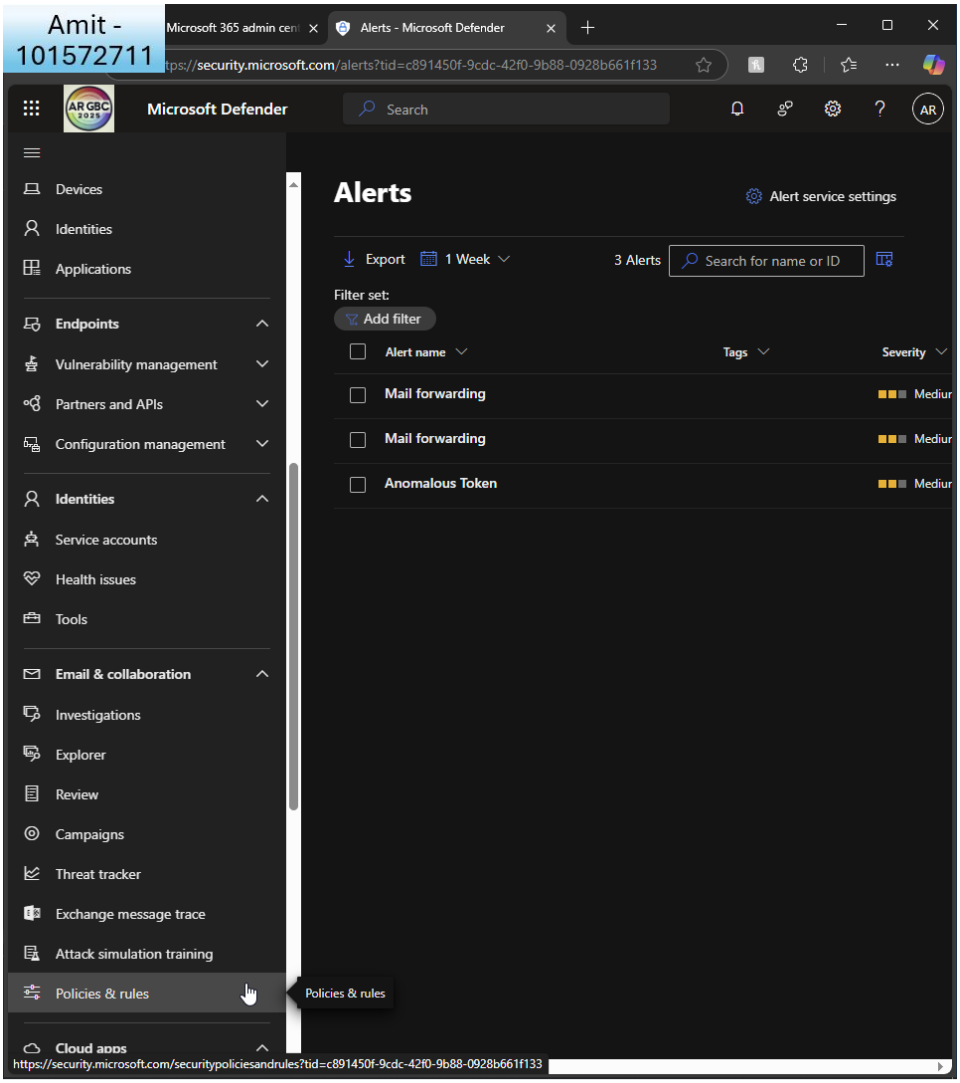
I go to Defender

Student Name: ……. Term: ……..
Student ID: ……..



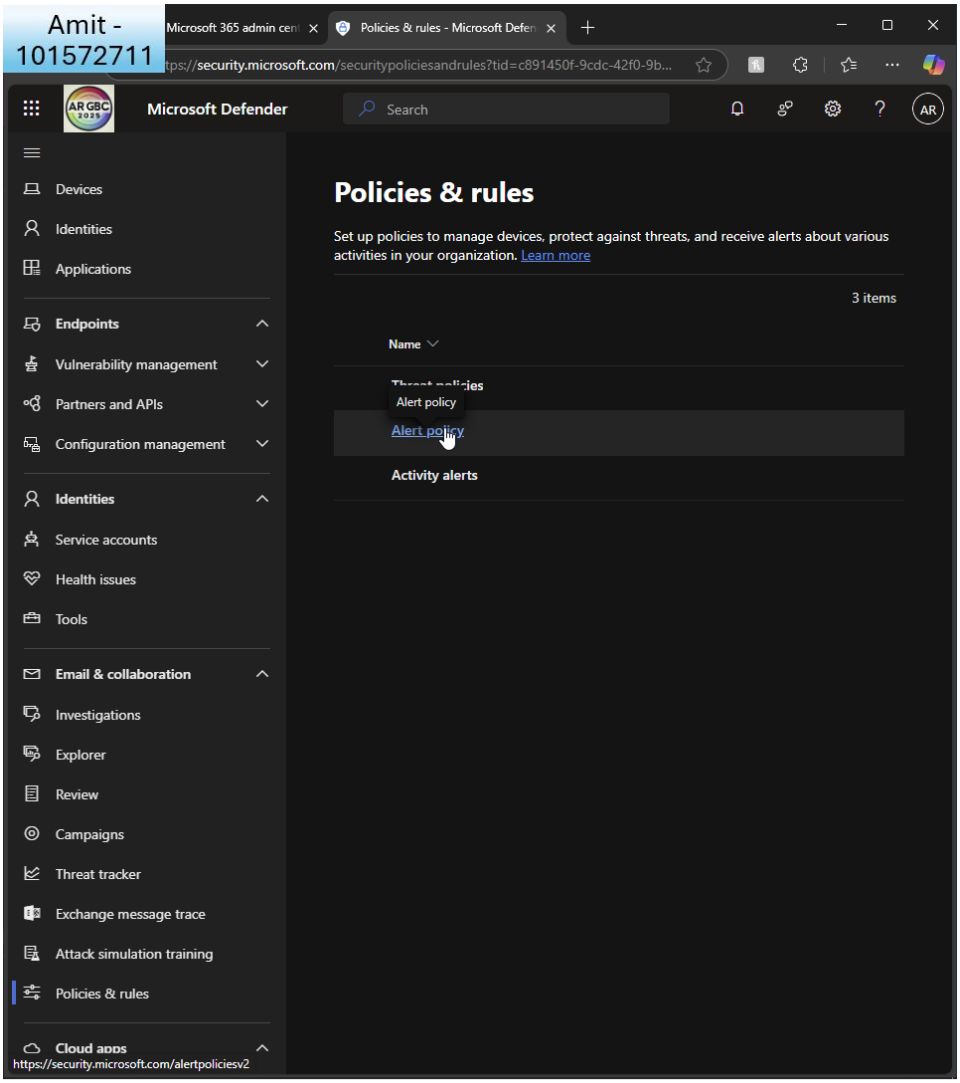
I create a policy for an alert

Student Name: ……. Term: ……..
Student ID: ……..



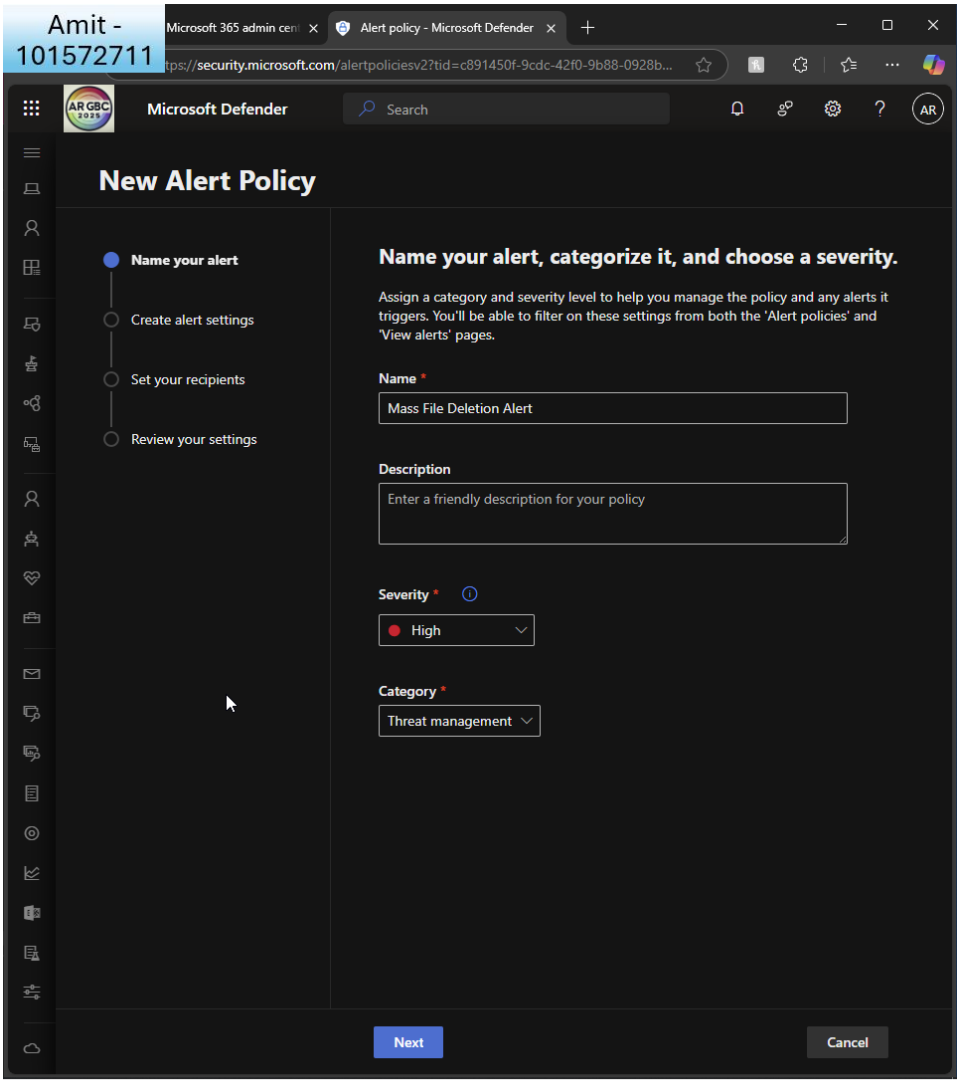
I go to 'policies & rules'

Student Name: ……. Term: ……..
Student ID: ……..



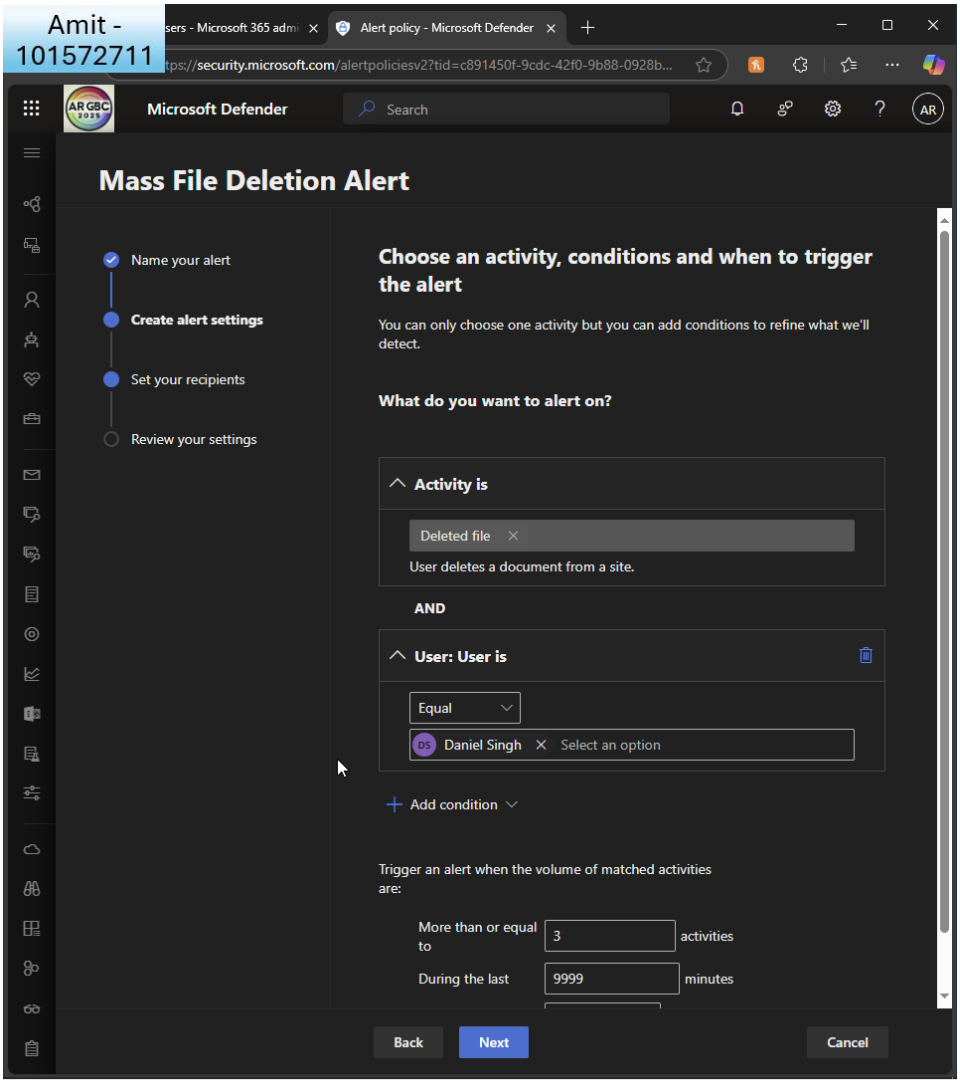
I click 'alert policy'

Student Name: ……. Term: ……..
Student ID: ……..



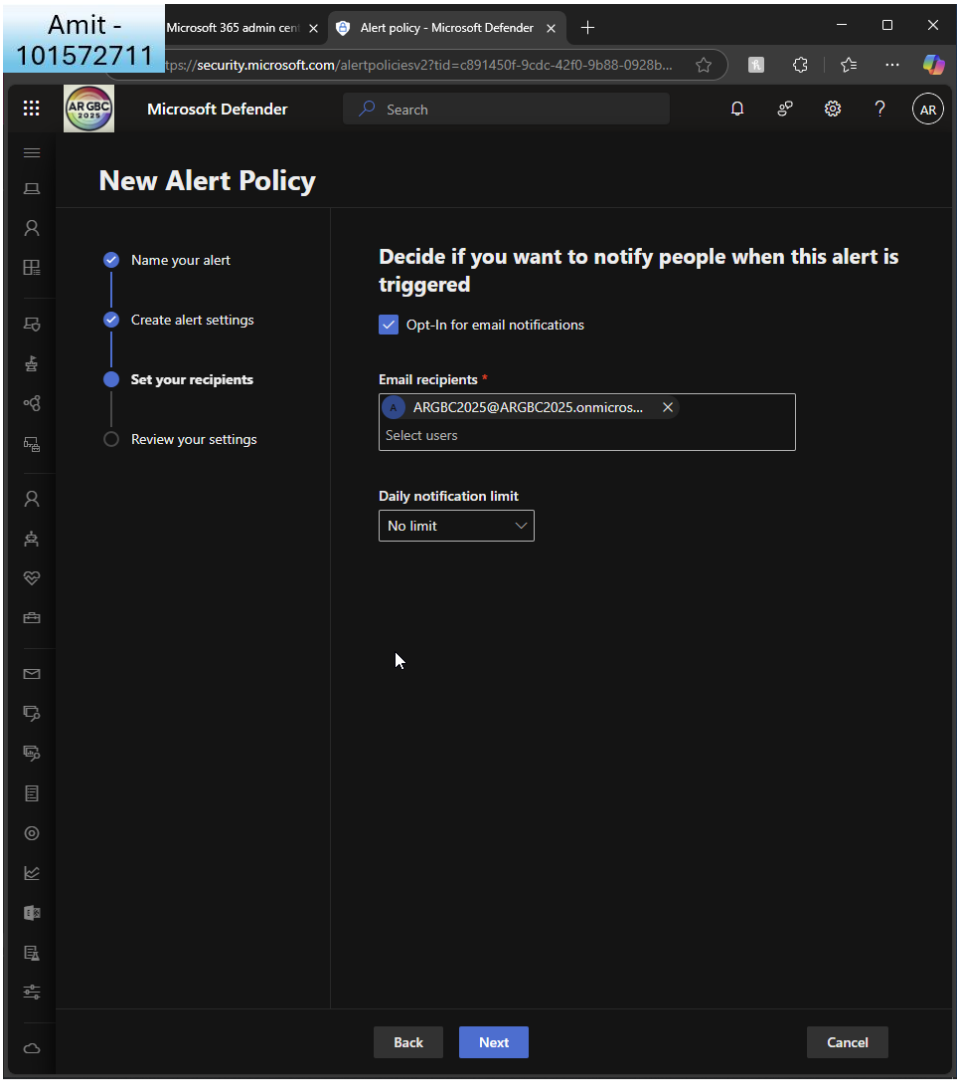
I name the policy and give it a high severity and categorise it under ’threat management’

Student Name: ……. Term: ……..
Student ID: ……..



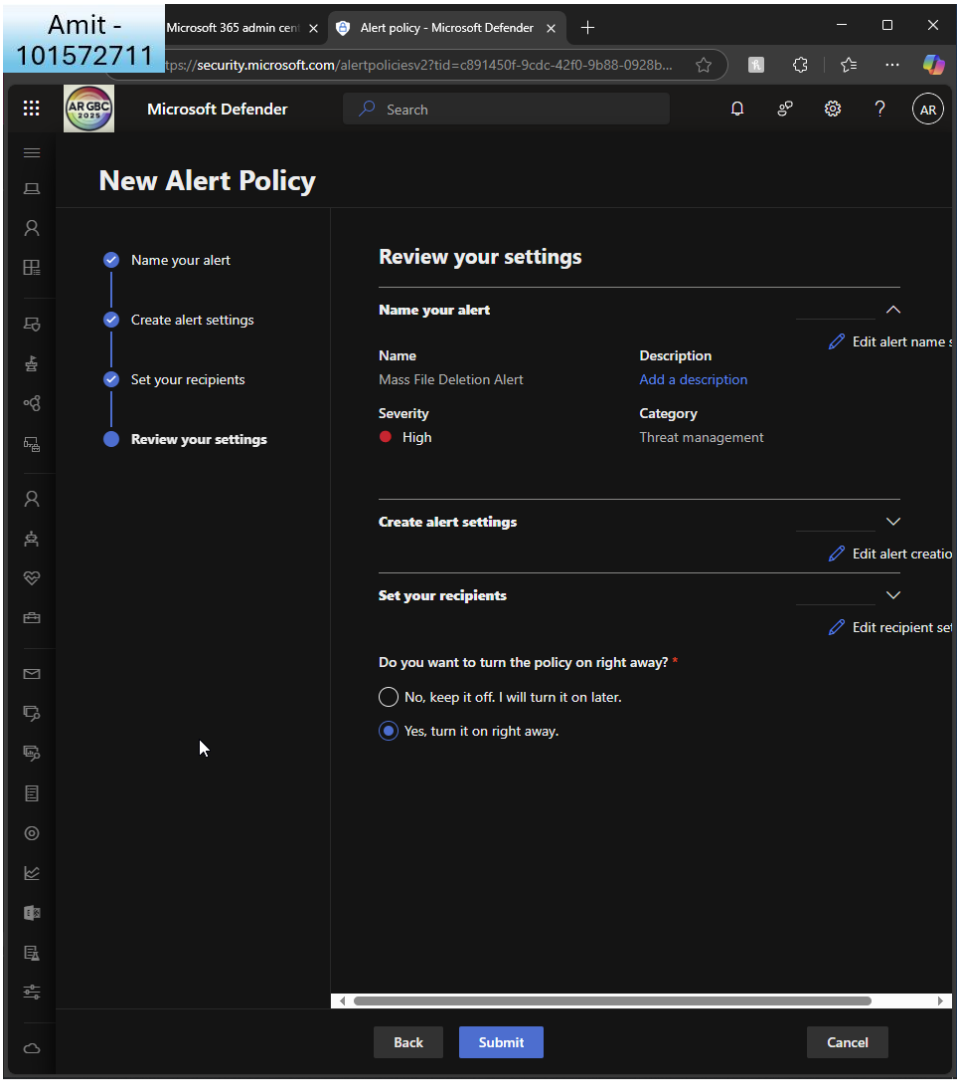
I choose to create a policy alert if files are deleted by user 'Daniel Singh'

Student Name: ……. Term: ……..
Student ID: ……..



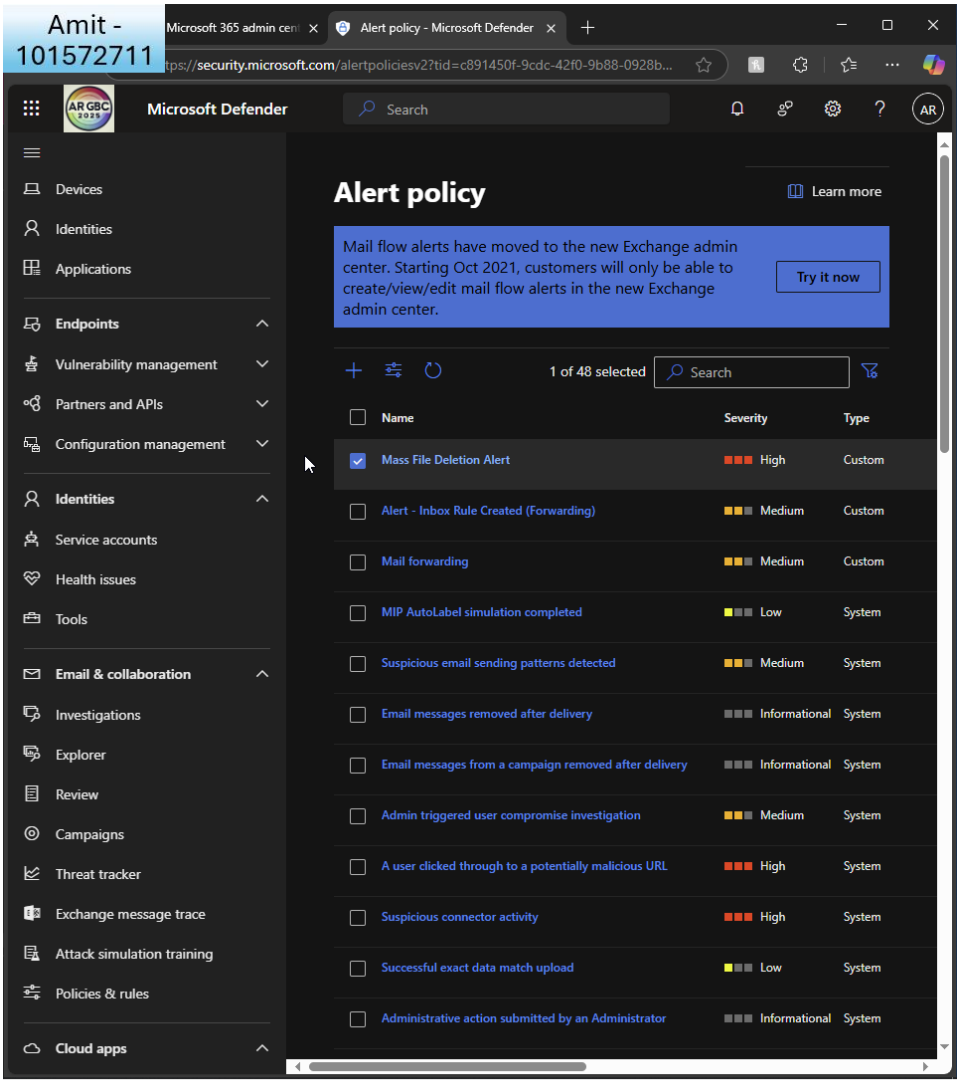
I set GA as a recipient of notification

Student Name: ……. Term: ……..
Student ID: ……..



I review settings and turn it on straight away

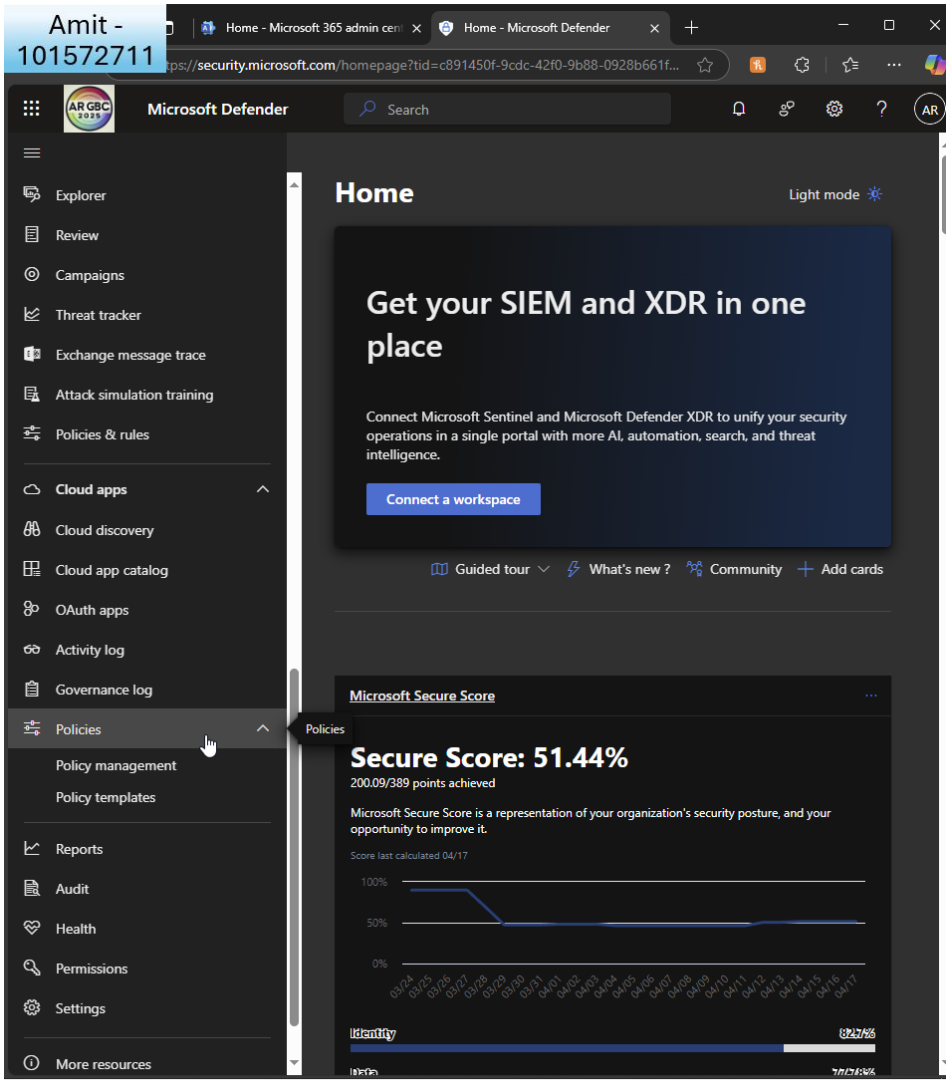
Student Name: ……. Term: ……..
Student ID: ……..



I can see my new alert policy

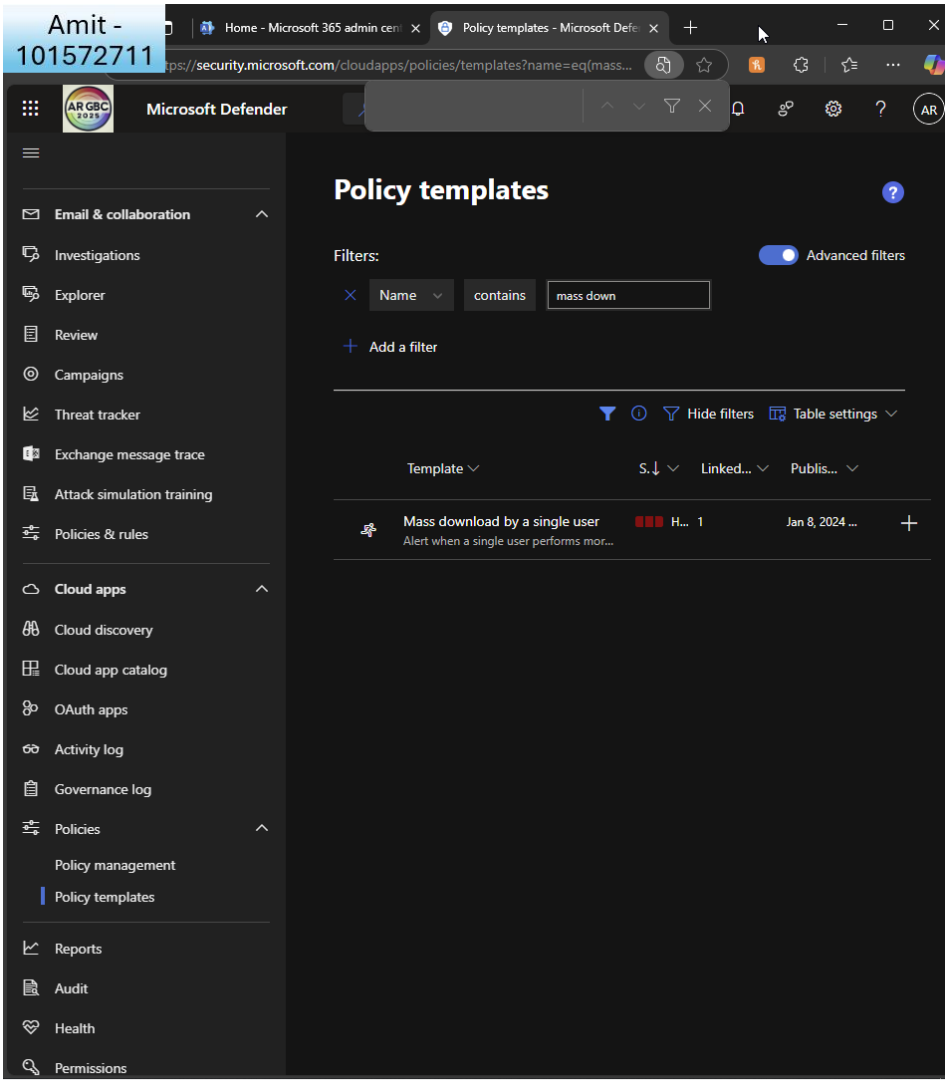
I realise that the policy was not created in the correct place. It was created under 'email and collaborations' and I now realise it must be created under 'MS defender for cloud apps'. I choose to create an alert for 'mass download by a single user'.

Student Name: ……. Term: ……..
Student ID: ……..



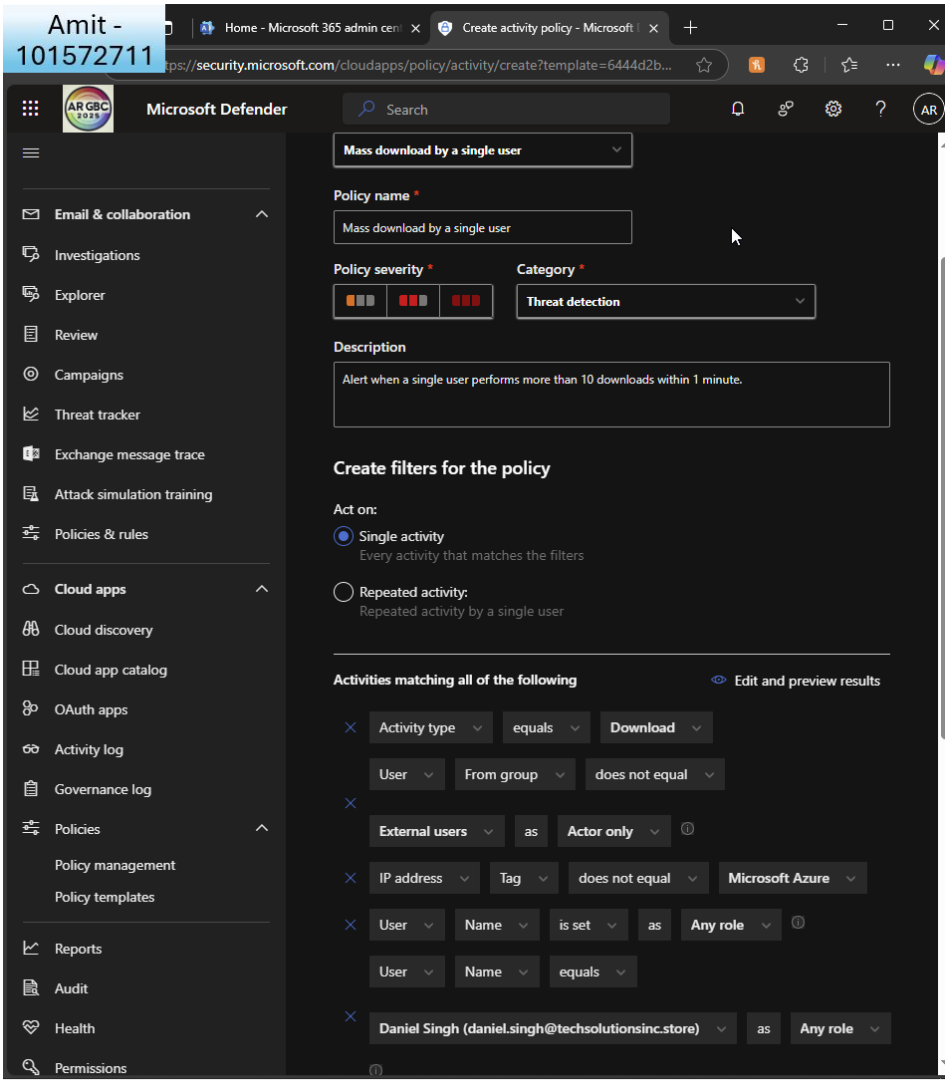
In Defender, I go to ’cloud apps - policies’

Student Name: ……. Term: ……..
Student ID: ……..



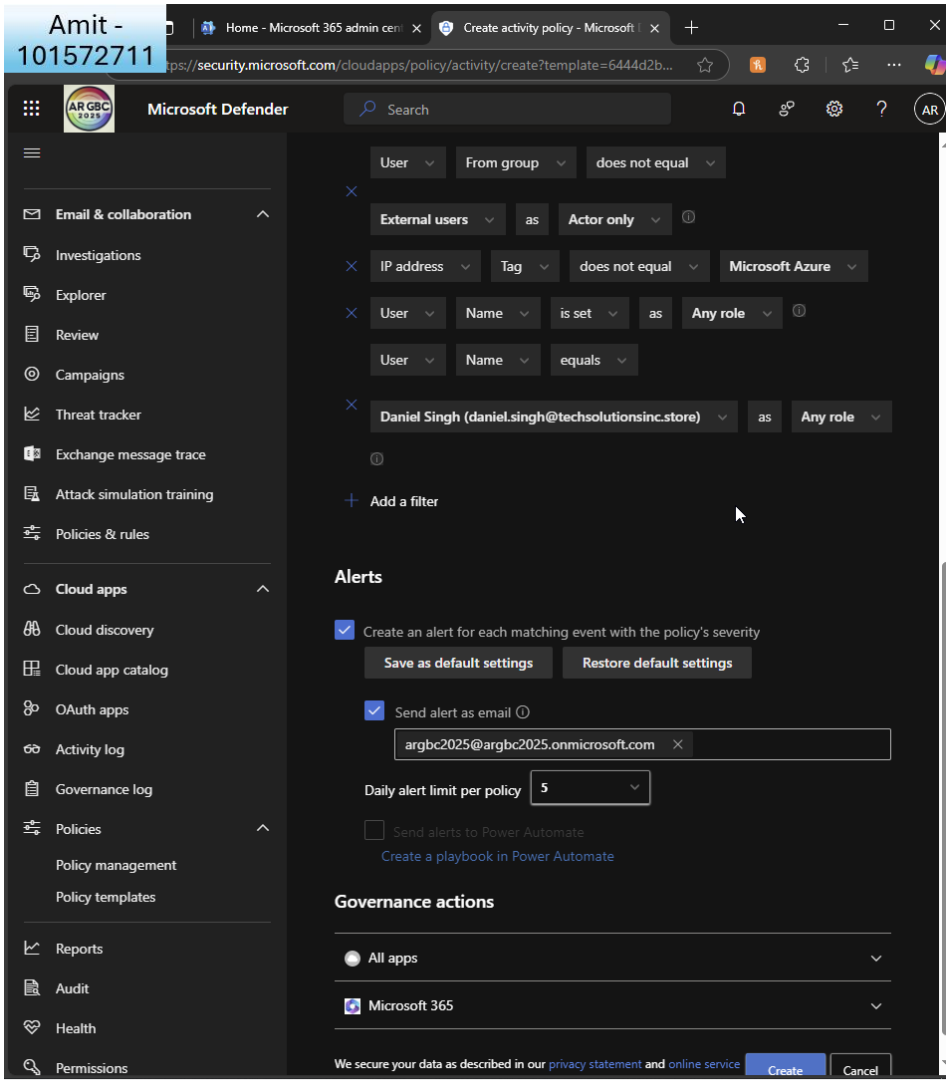
I search for a policy template named ’mass download by a single user’

Student Name: ……. Term: ……..
Student ID: ……..



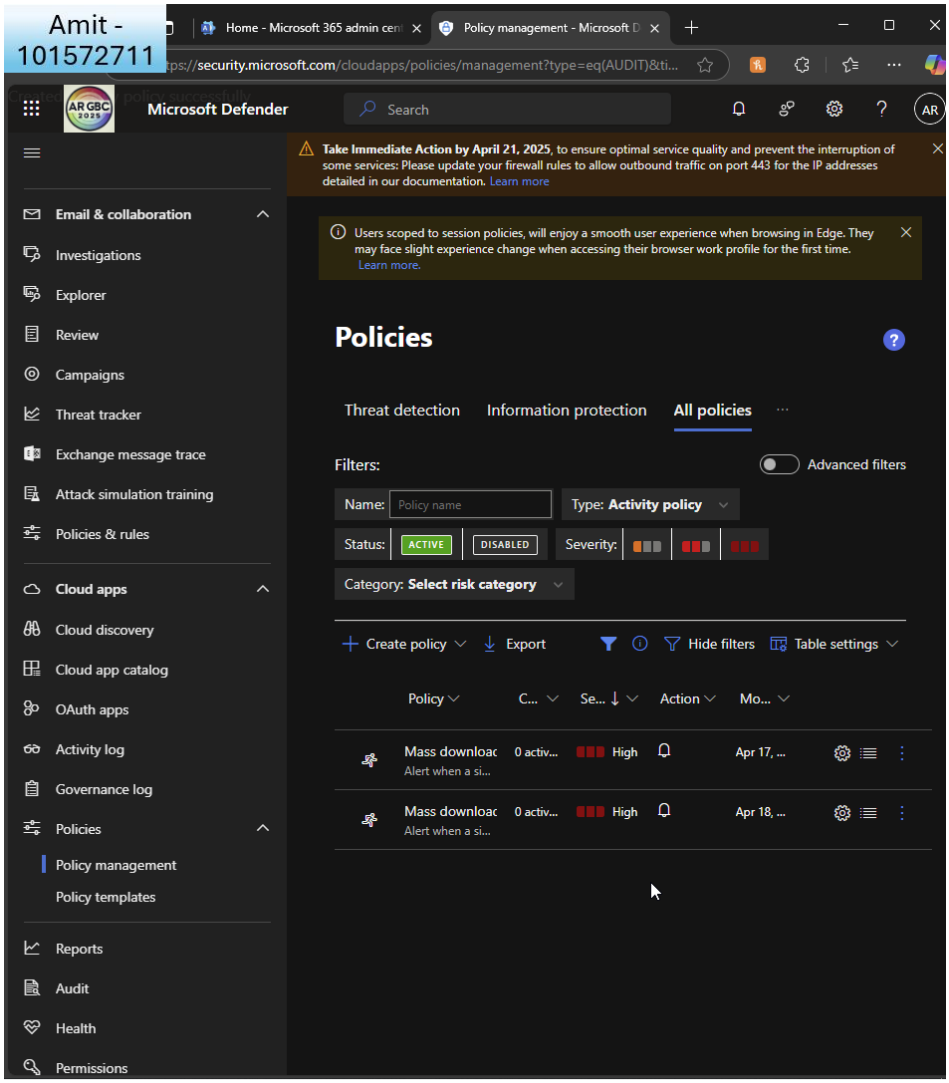
I edit the policy to target user ’Daniel’

Student Name: ……. Term: ……..
Student ID: ……..



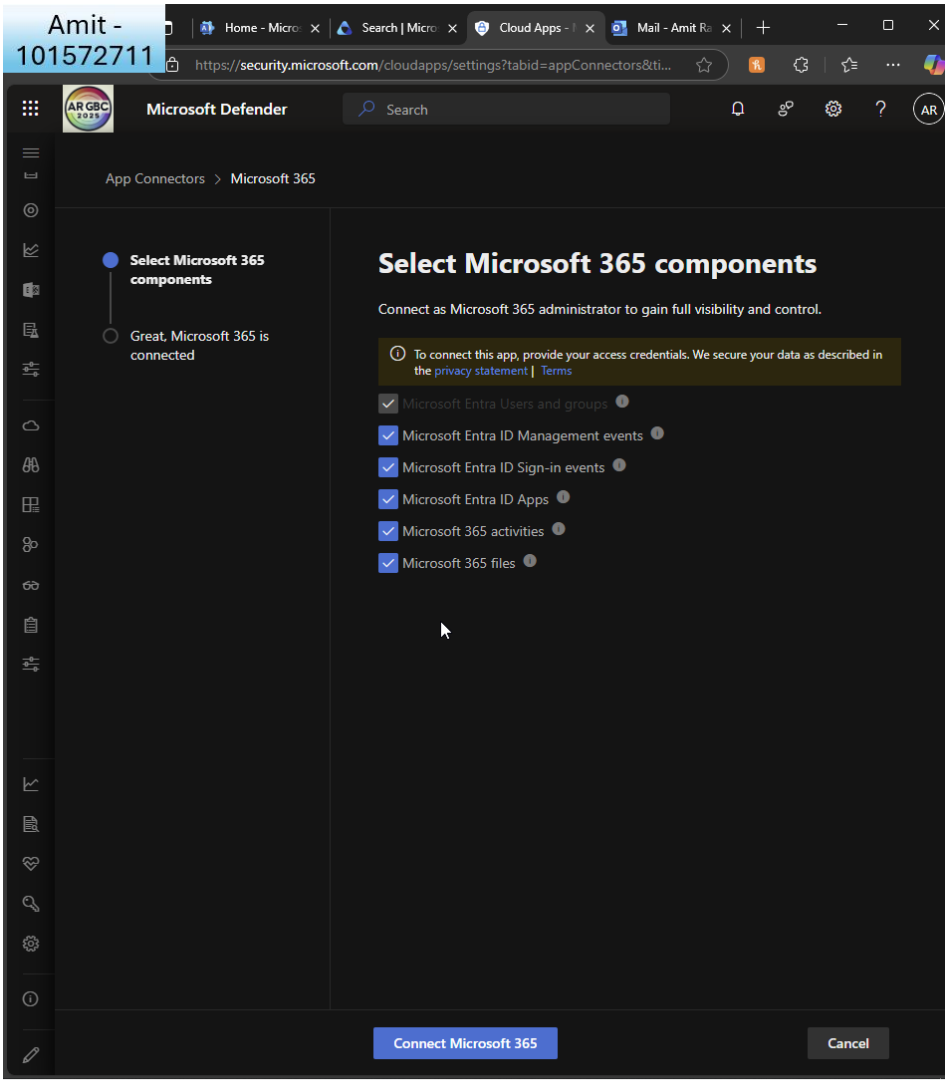
I make sure GA gets sent the alert

Student Name: ……. Term: ……..
Student ID: ……..



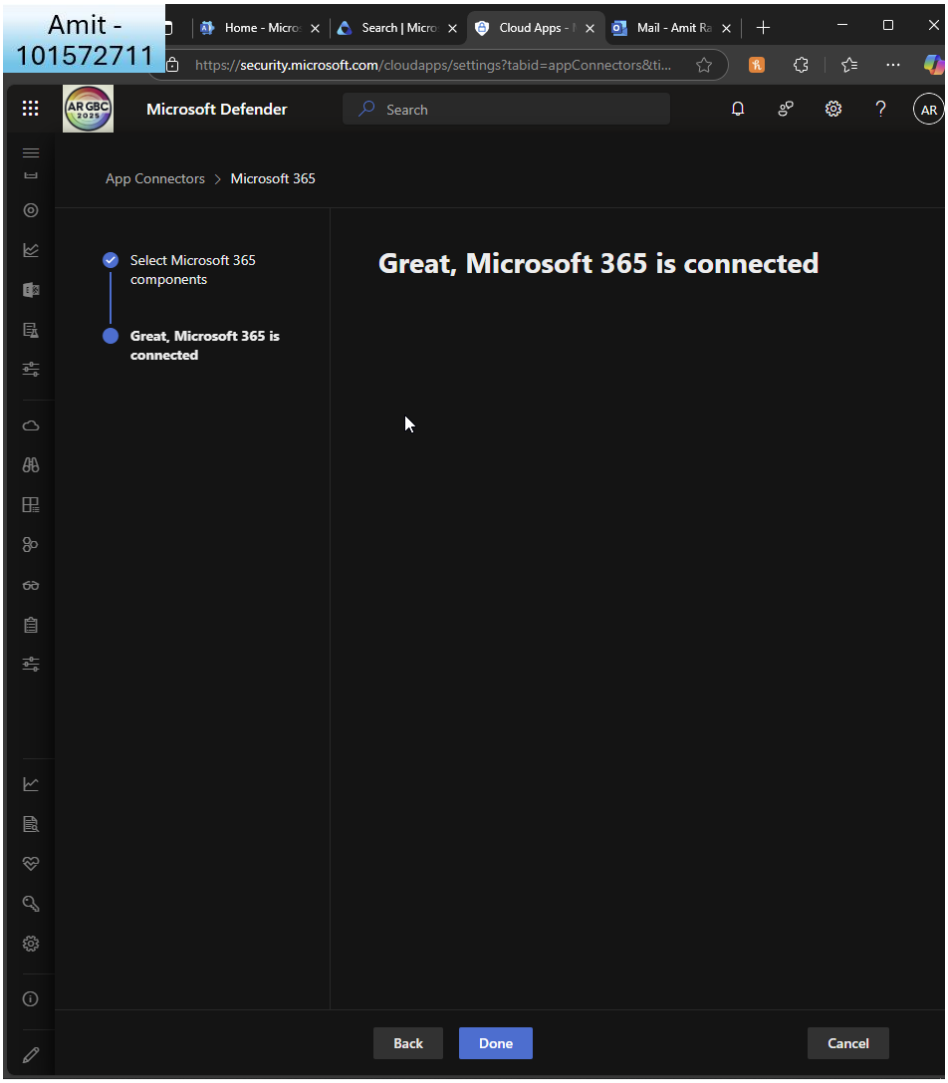
I can see my new policy listed

Student Name: ……. Term: ……..
Student ID: ……..



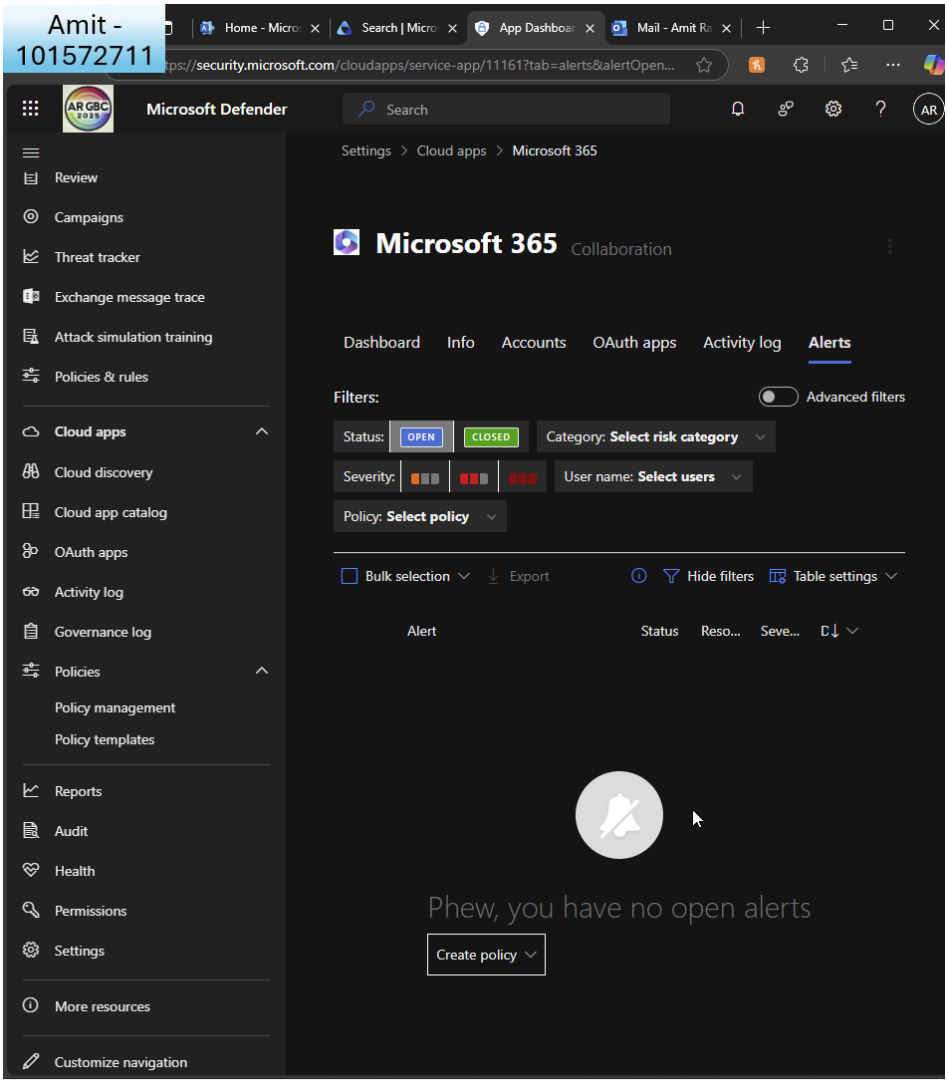
The alert was not showing in 'activity logs' so I ensured that the app connector was active for MS365 components

Student Name: ……. Term: ……..
Student ID: ……..



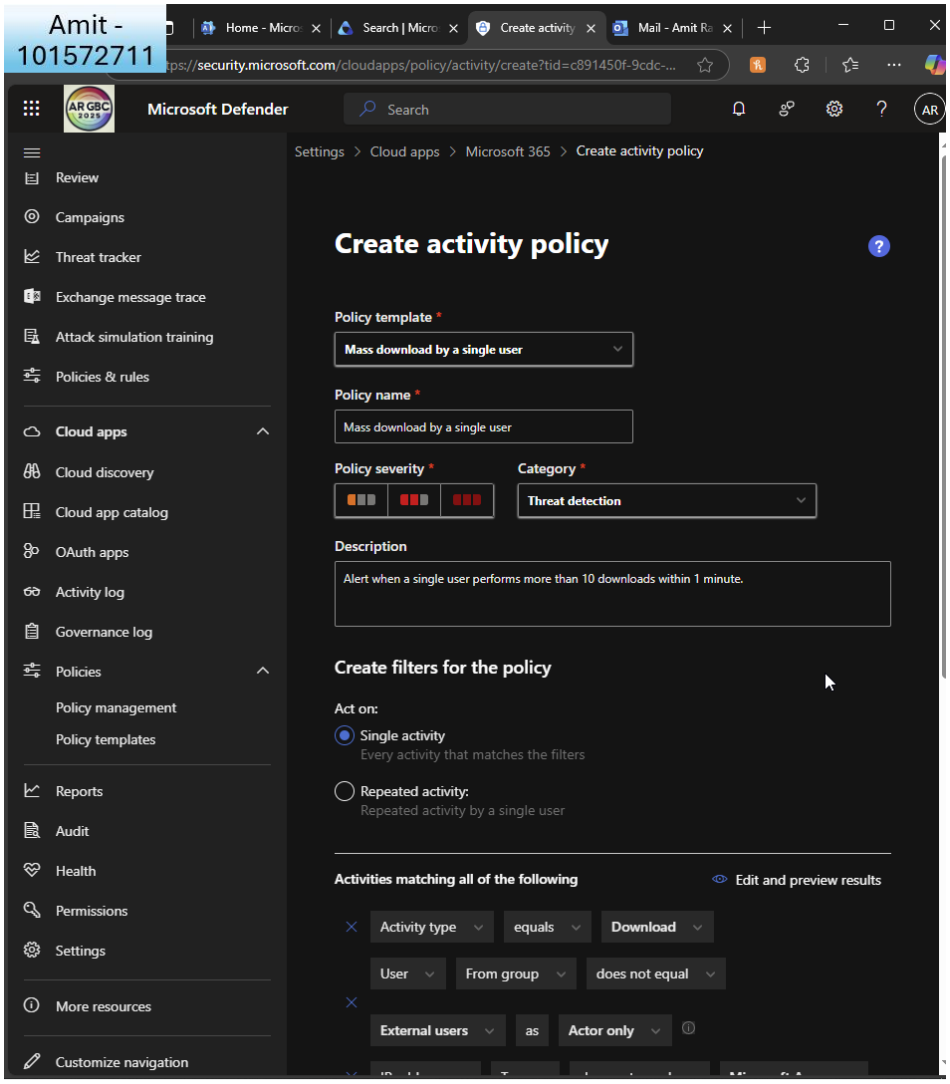
I see MS365 is now connected

Student Name: ……. Term: ……..
Student ID: ……..



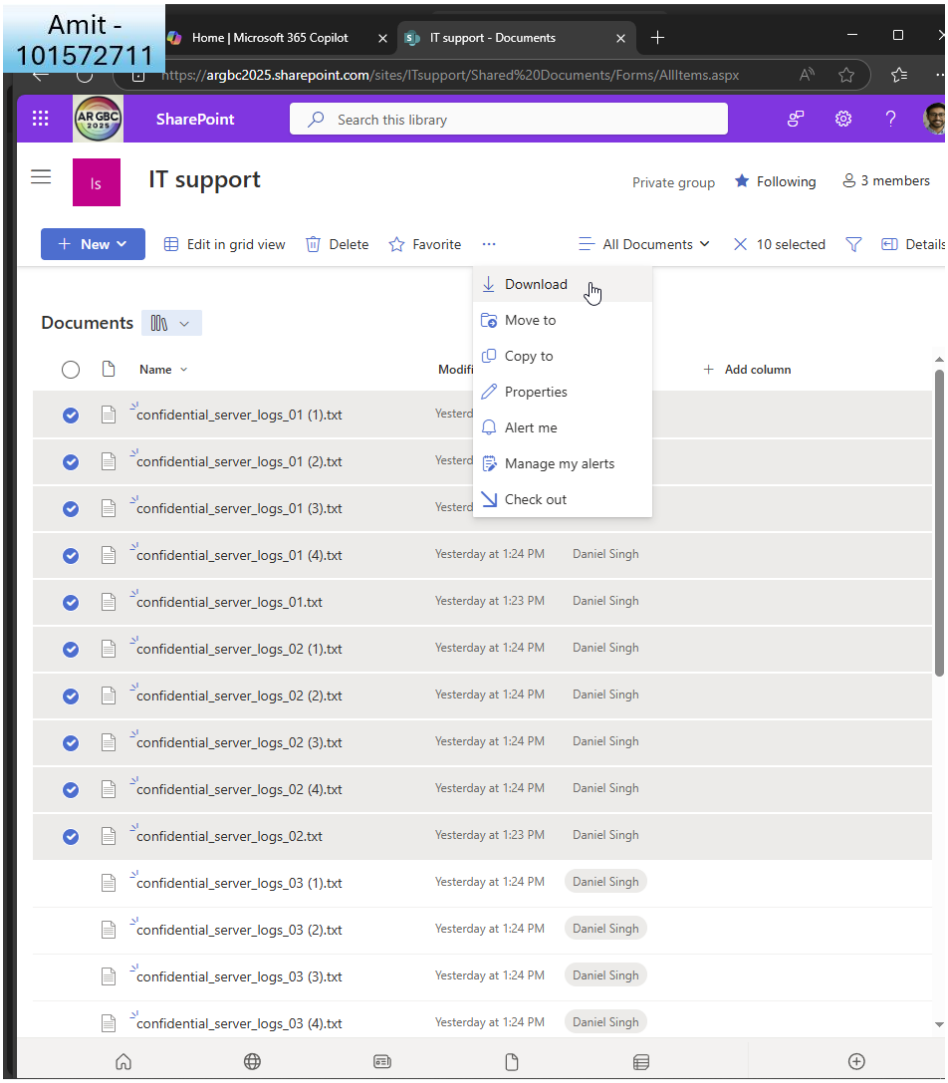
I create the policy directly in the app connector page to trigger an alert

Student Name: ……. Term: ……..
Student ID: ……..



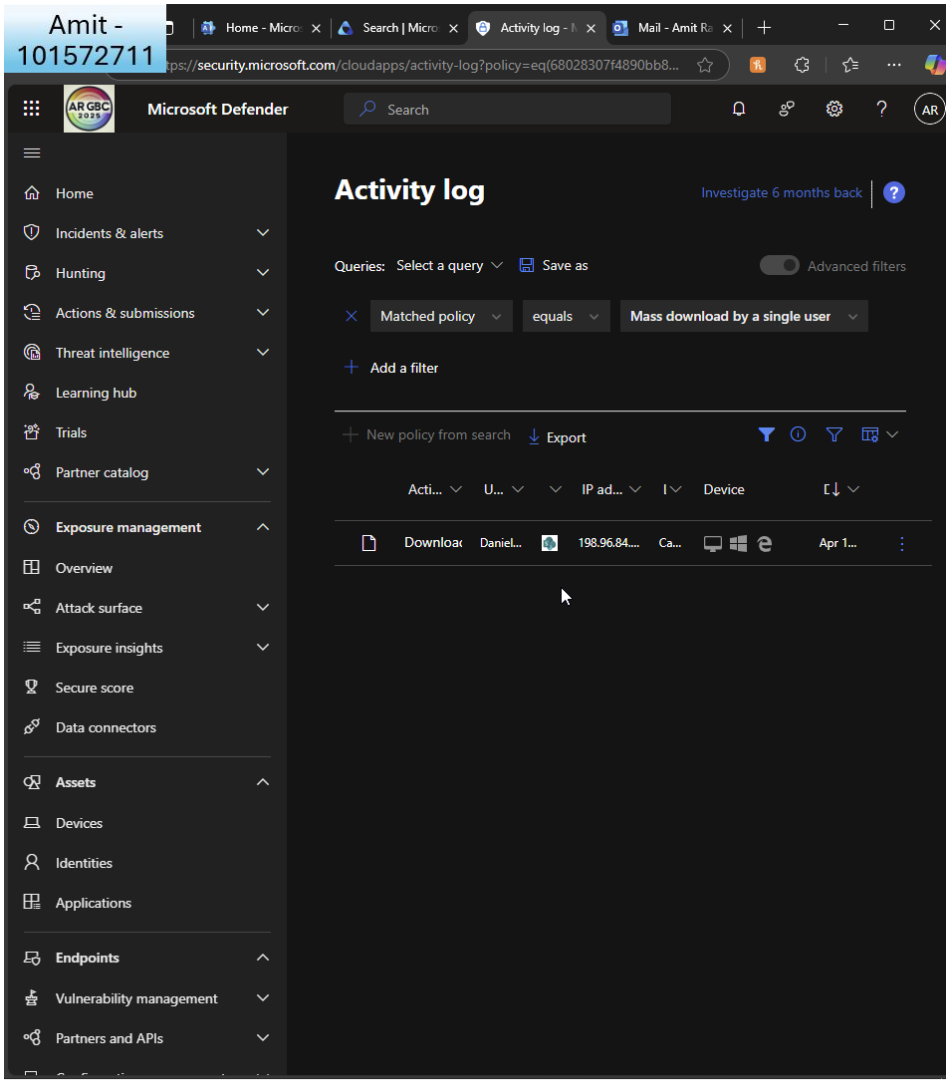
I match the previous policy of ’mass download by single user’

Student Name: ……. Term: ……..
Student ID: ……..



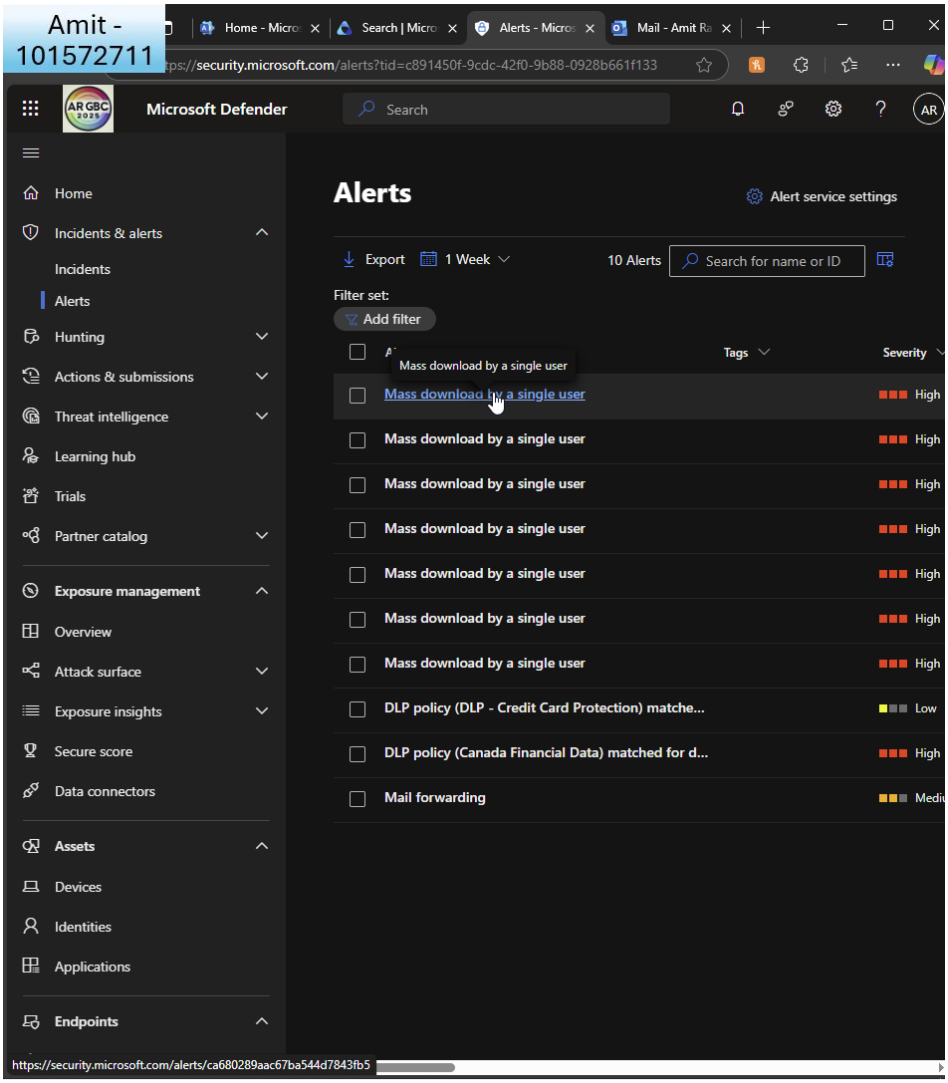
I log in as Daniel and mass download files

Student Name: ……. Term: ……..
Student ID: ……..



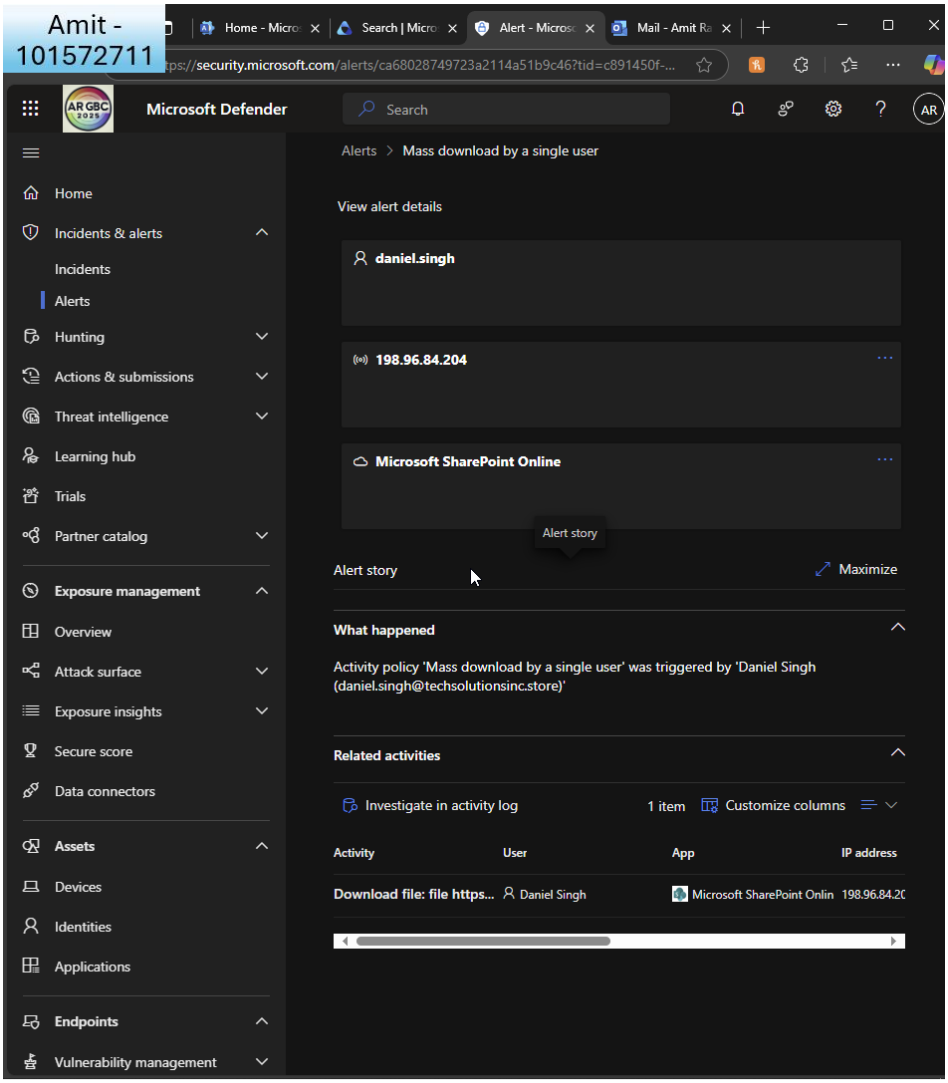
I can see in the cloud apps activity log, there is a record of the download

Student Name: ……. Term: …….
Student ID: …….



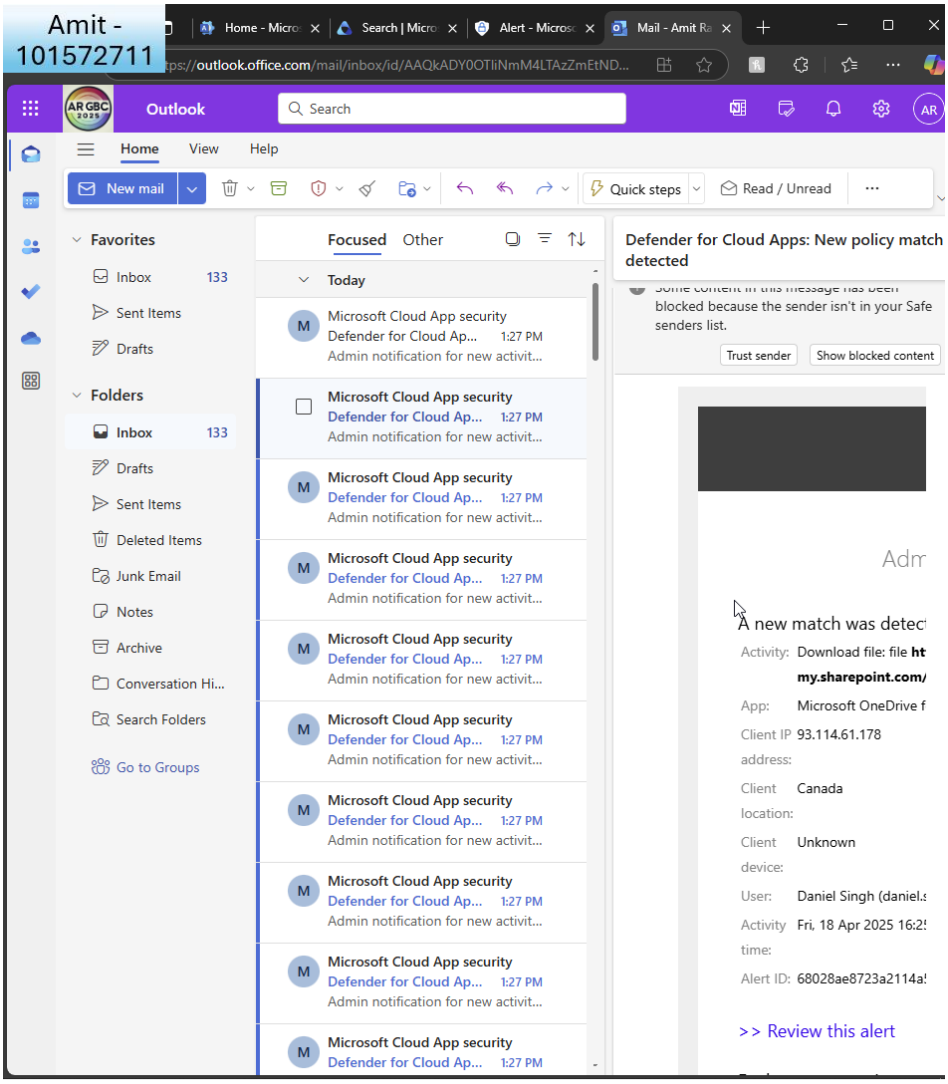
I wait a few minutes and can now see the alert in Defender

Student Name: ……. Term: ……..
Student ID: ……..



If I click on one, it shows the alert was caused by Daniel downloading mass files

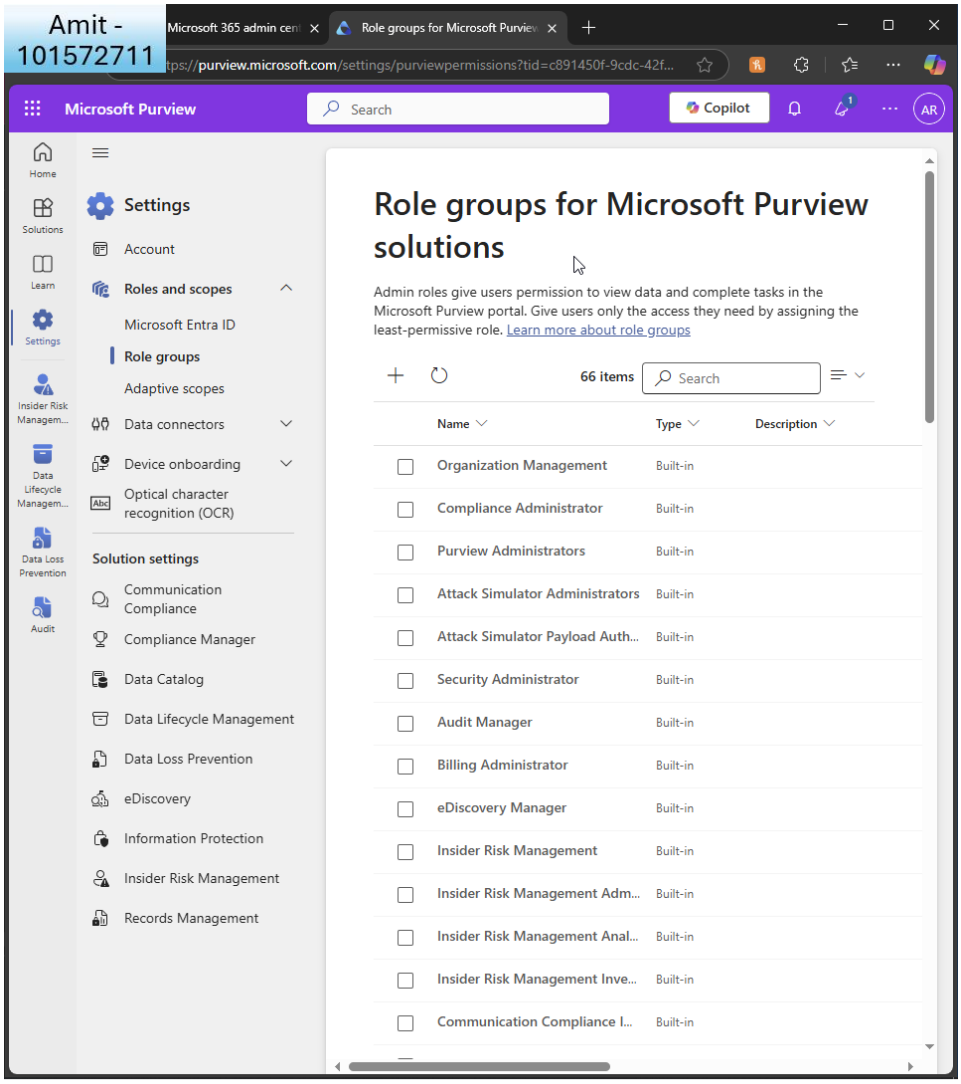
Student Name: ……. Term: ……..
Student ID: ……..



I also receive the alert as a notification to GA

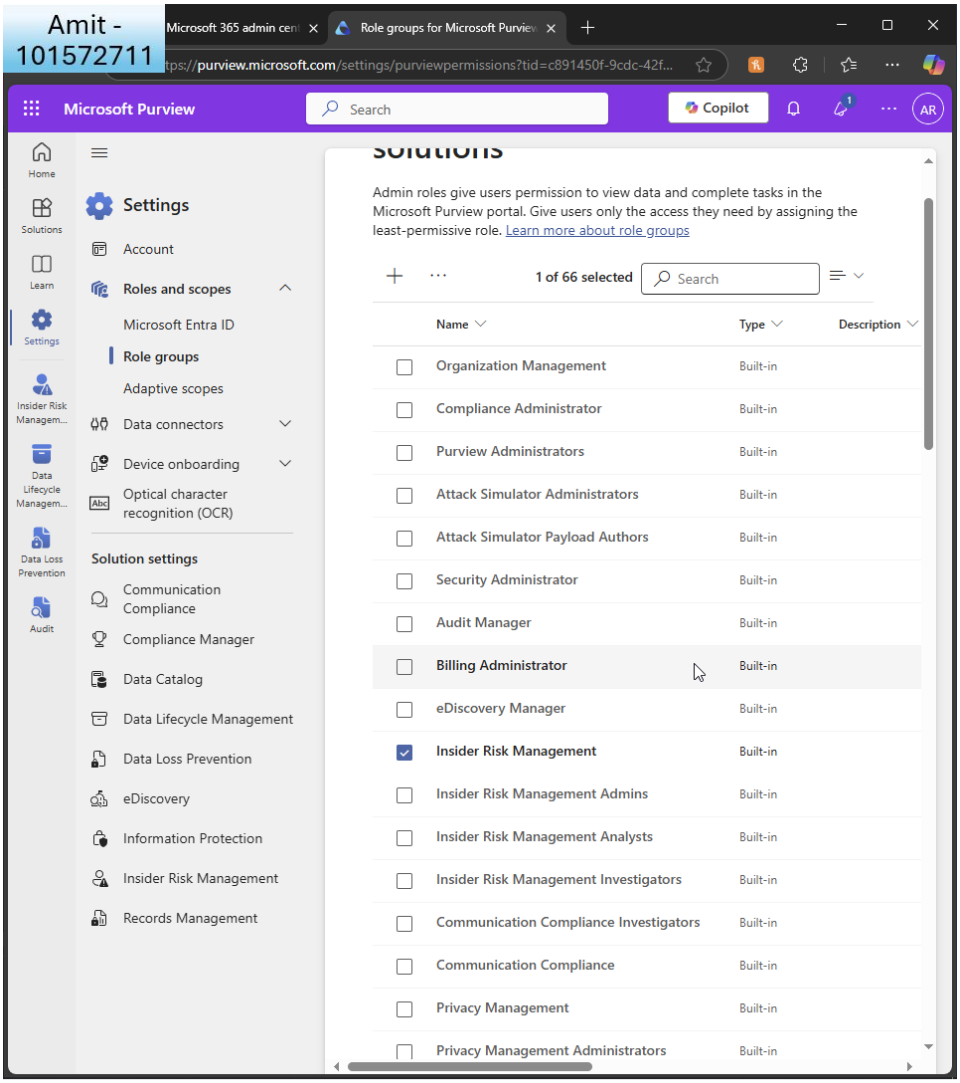
Student Name: ……. Term: ……..
Student ID: ……..

- Set up notifications for data loss prevention (DLP) policy breaches. (You can navigate to Insider risk management)



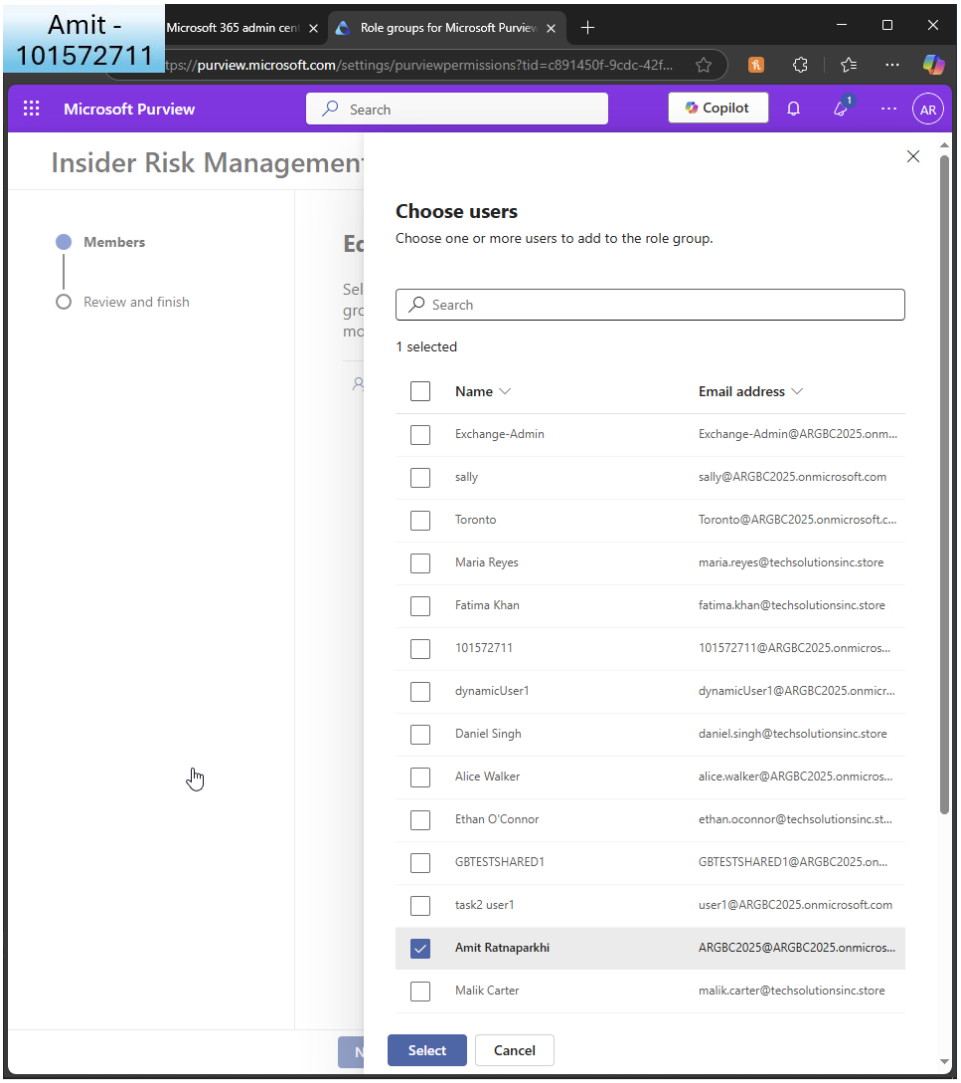
I see insider risk management role is not assigned by default to GA

Student Name: ……. Term: ……..
Student ID: ……..



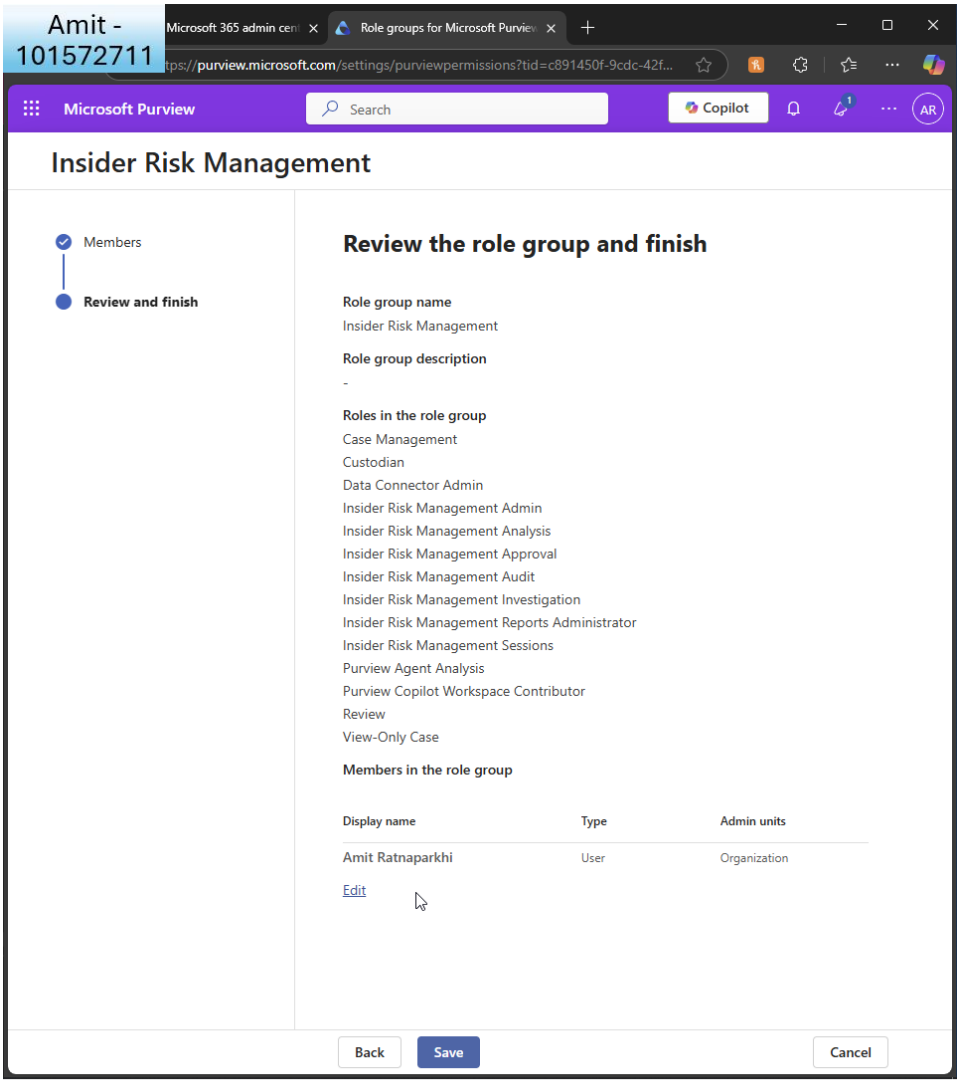
I click it

Student Name: ……. Term: ……..
Student ID: ……..



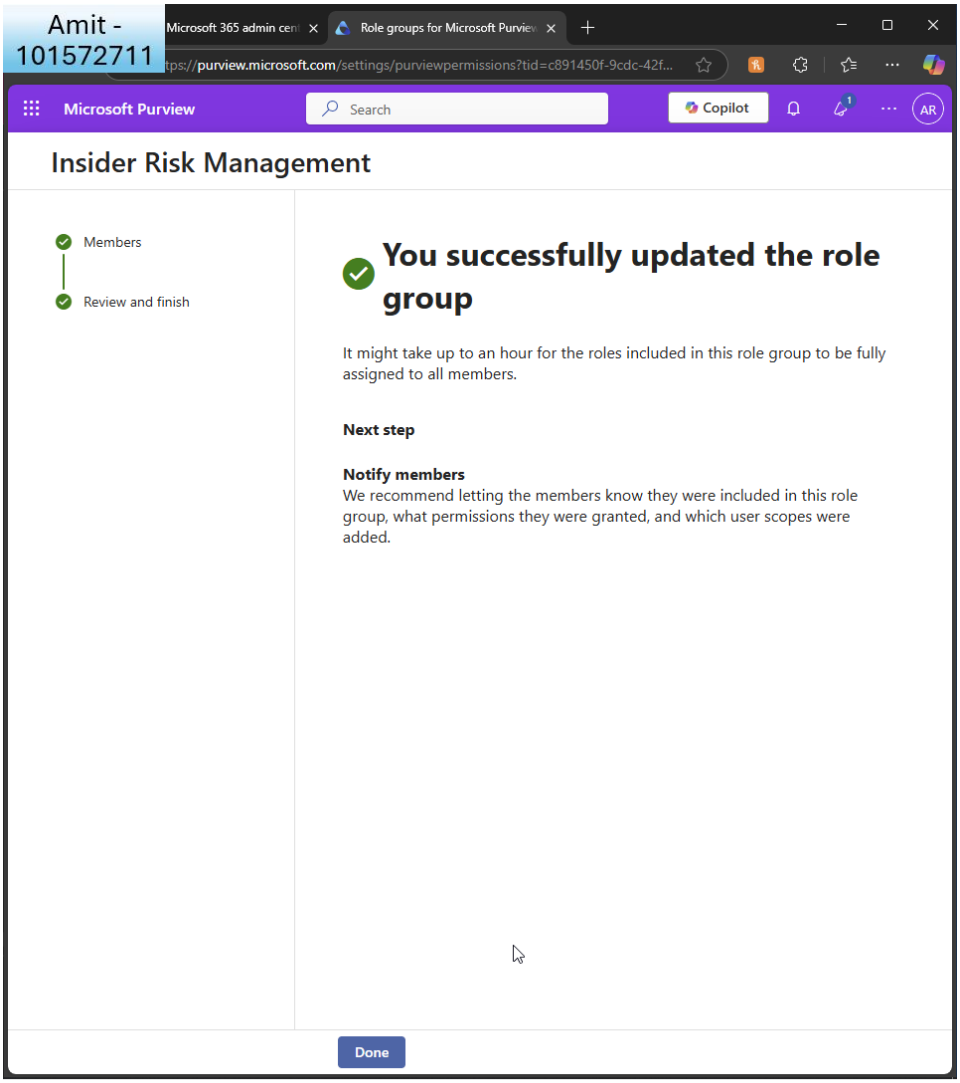
I choose GA as the user

Student Name: ……. Term: ……..
Student ID: ……..



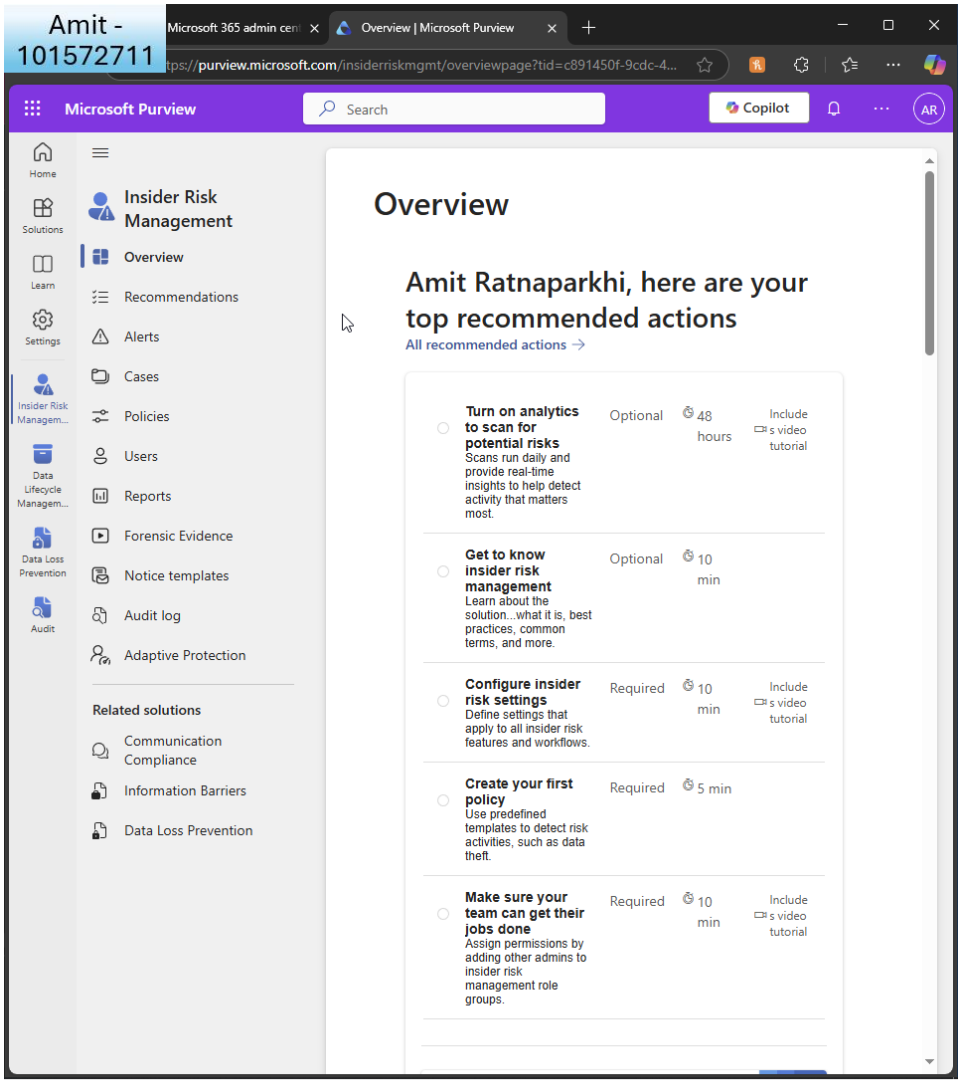
I review and finish

Student Name: ……. Term: ……..
Student ID: ……..



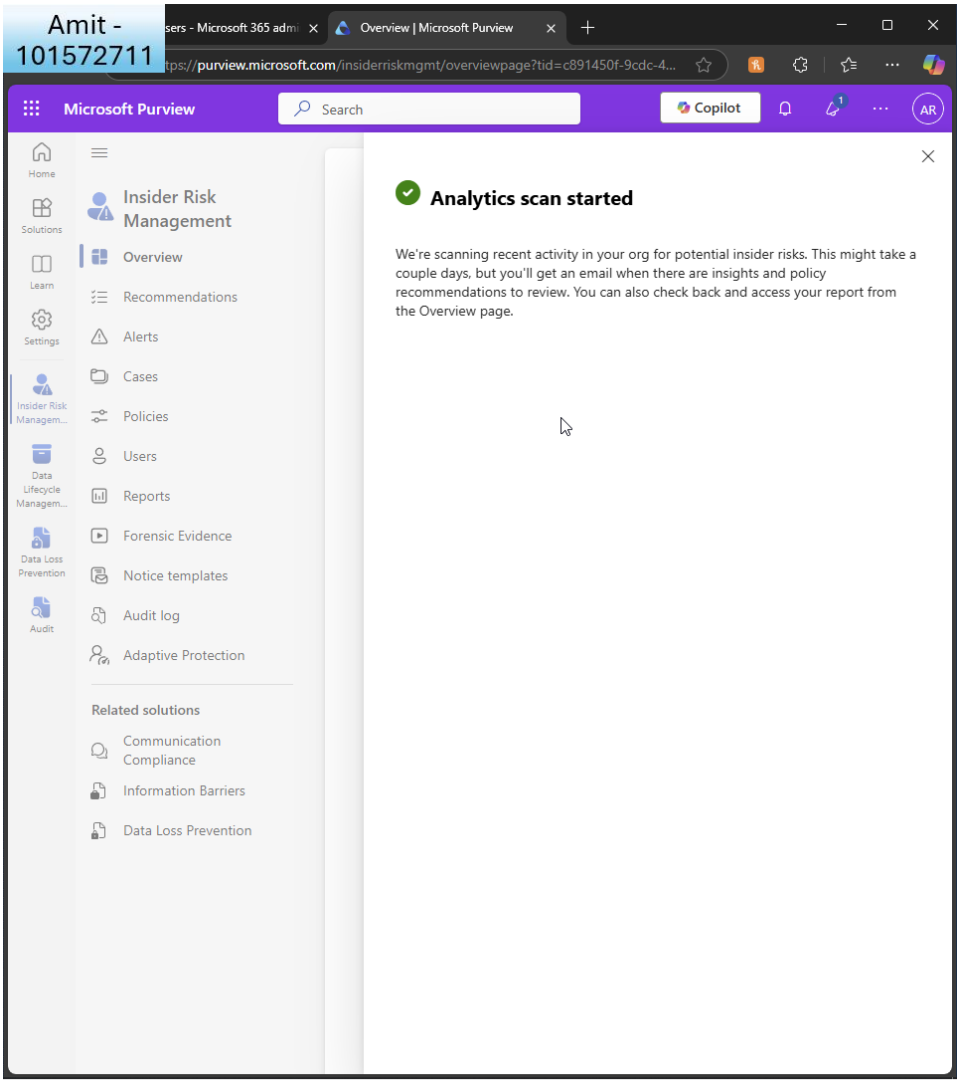
I see the confirmation

Student Name: ……. Term: ……..
Student ID: ……..



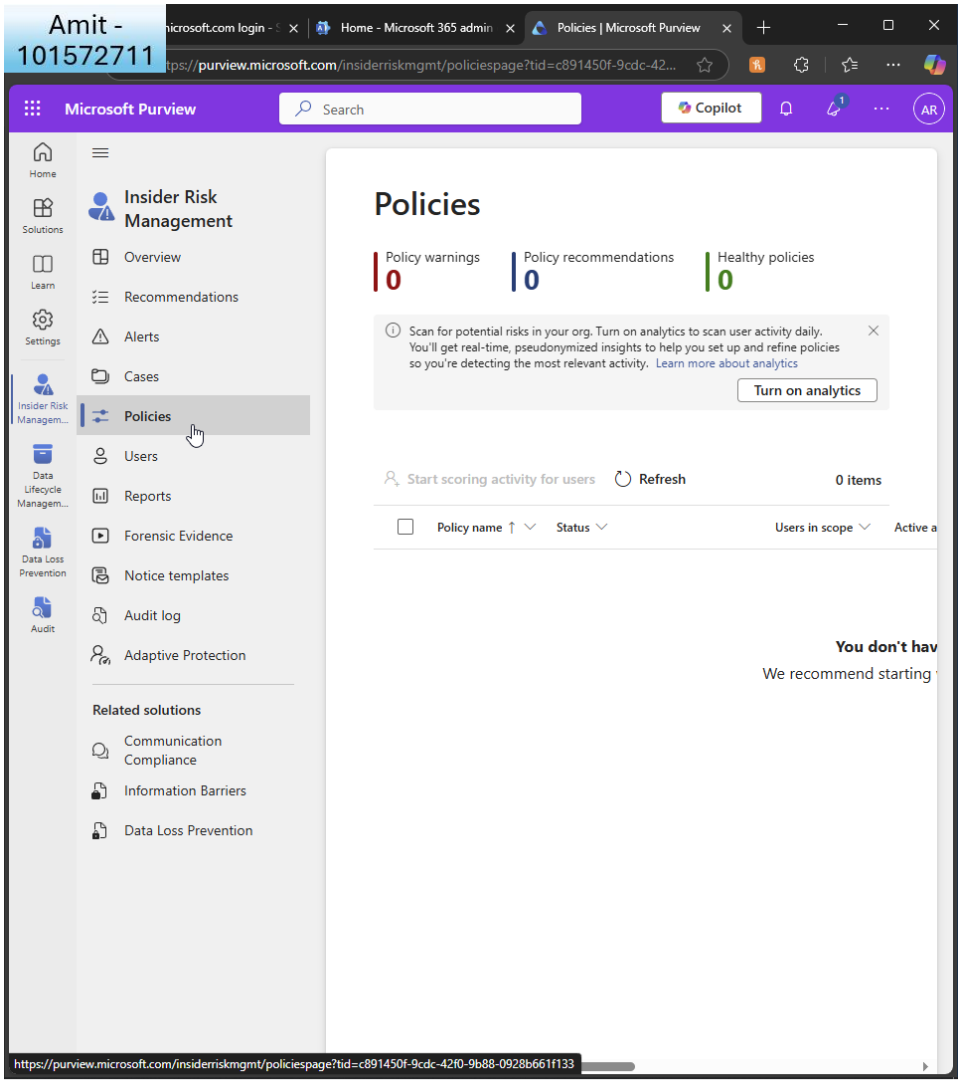
I see the IRM console and enable ’analytics to scan for potential risks’

Student Name: ……. Term: ……..
Student ID: ……..



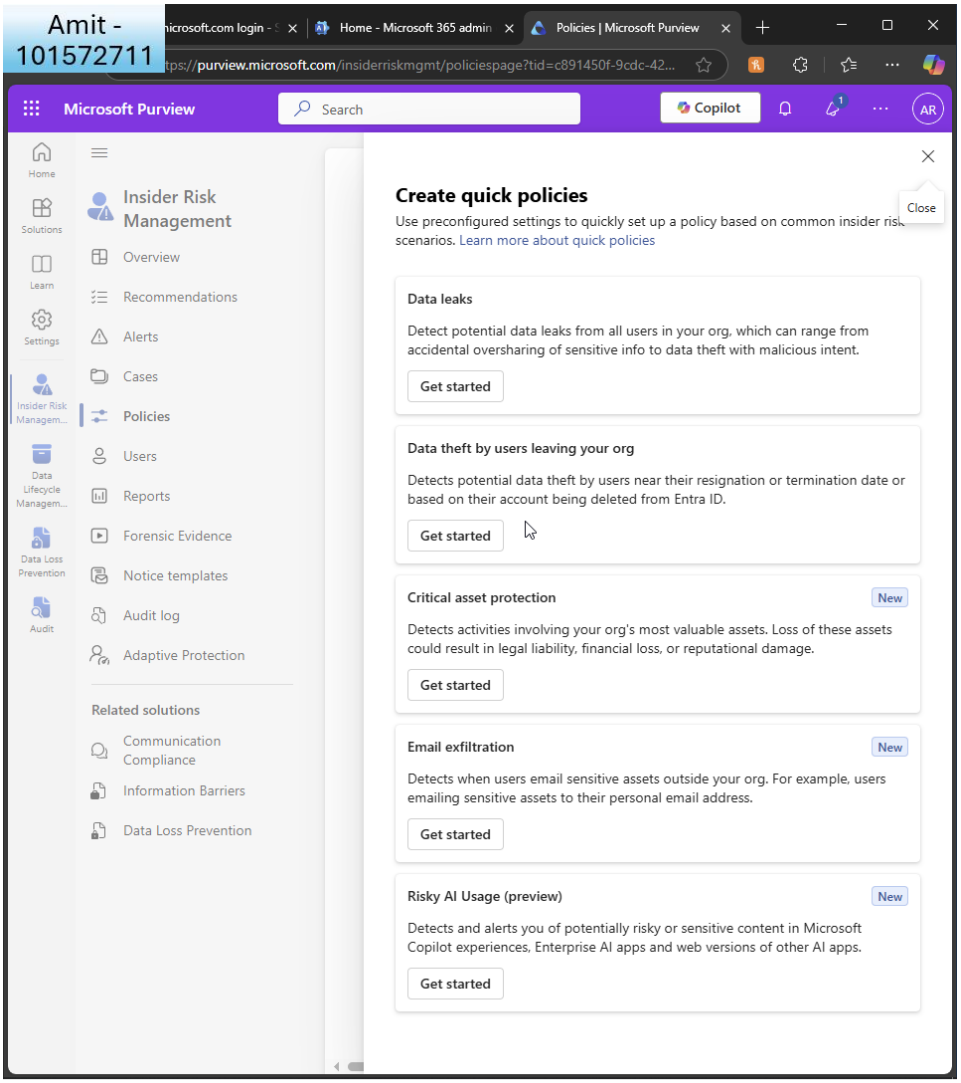
I can see it will take up to 48 hours to scan

Student Name: ……. Term: ……..
Student ID: ……..



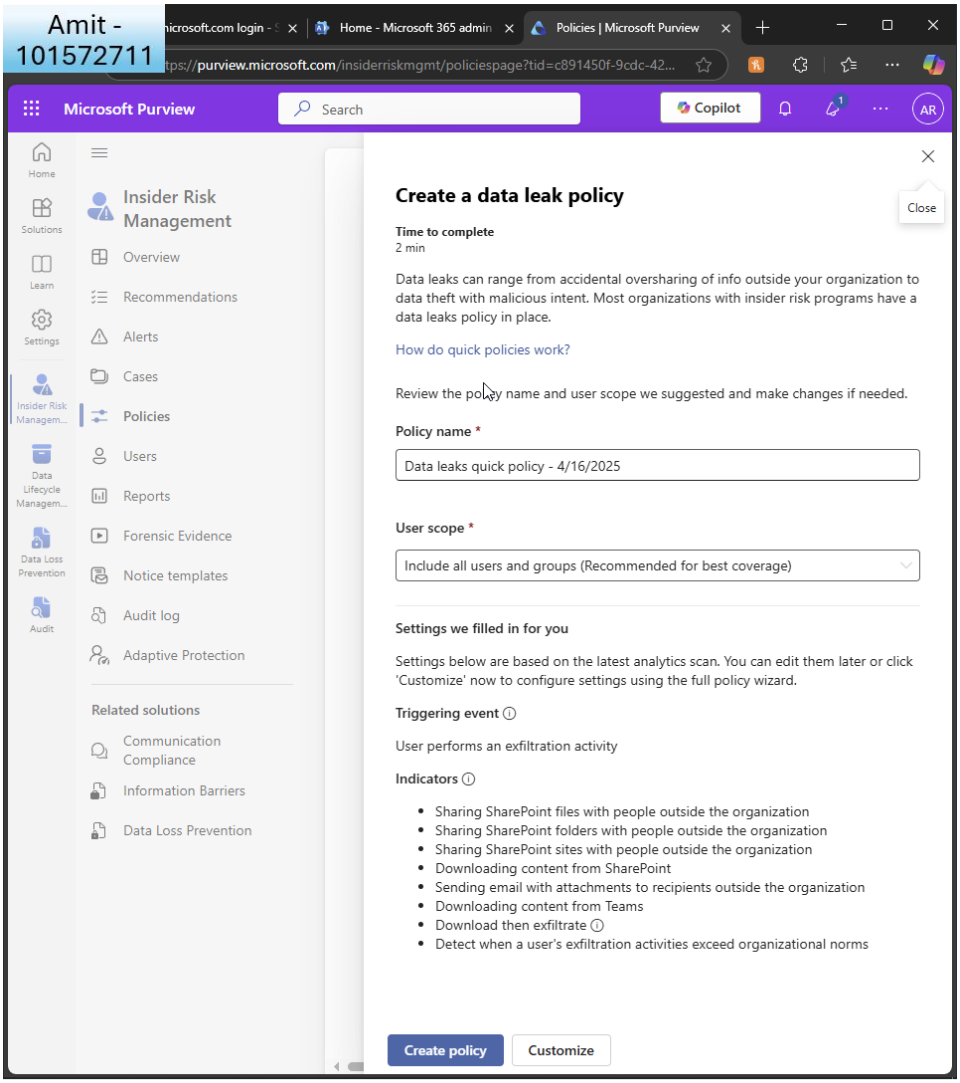
I create my policy

Student Name: ……. Term: ……..
Student ID: ……..



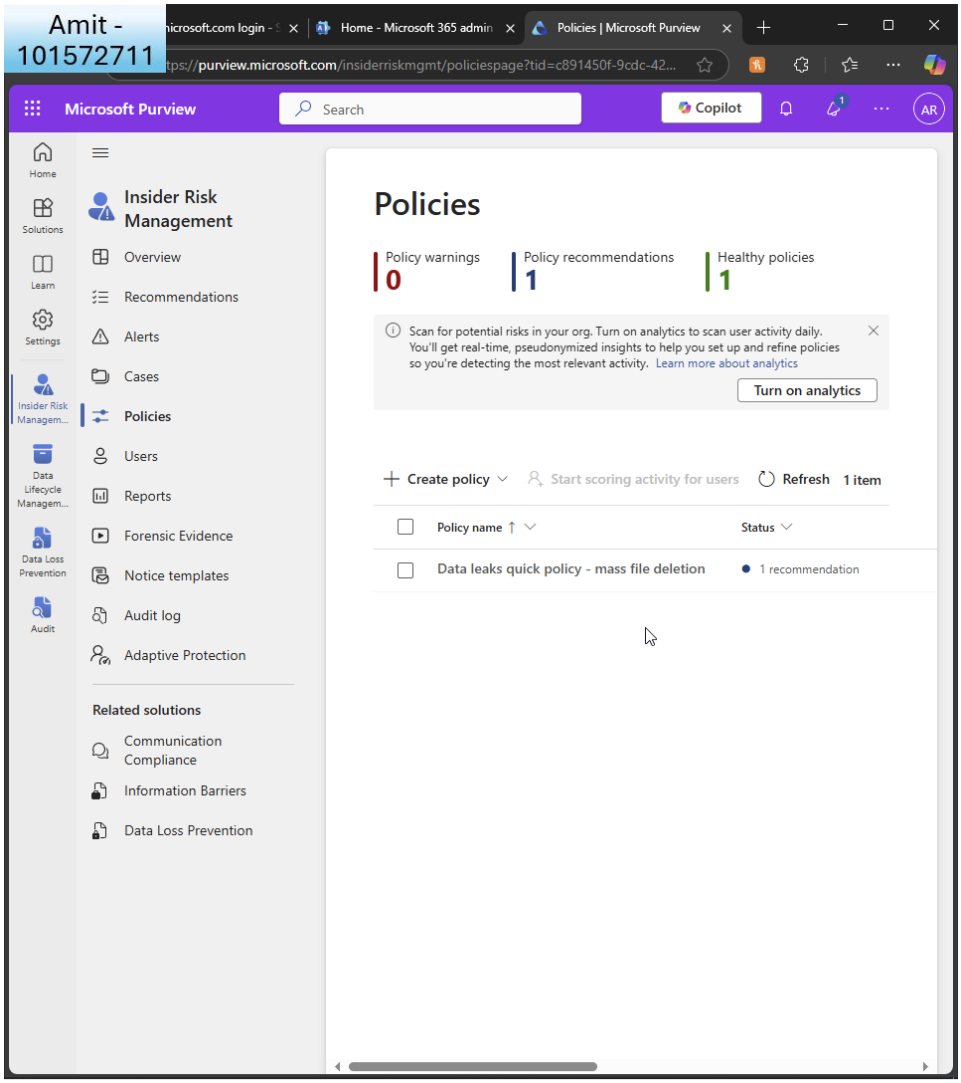
I create a quick policy

Student Name: ……. Term: ……..
Student ID: ……..



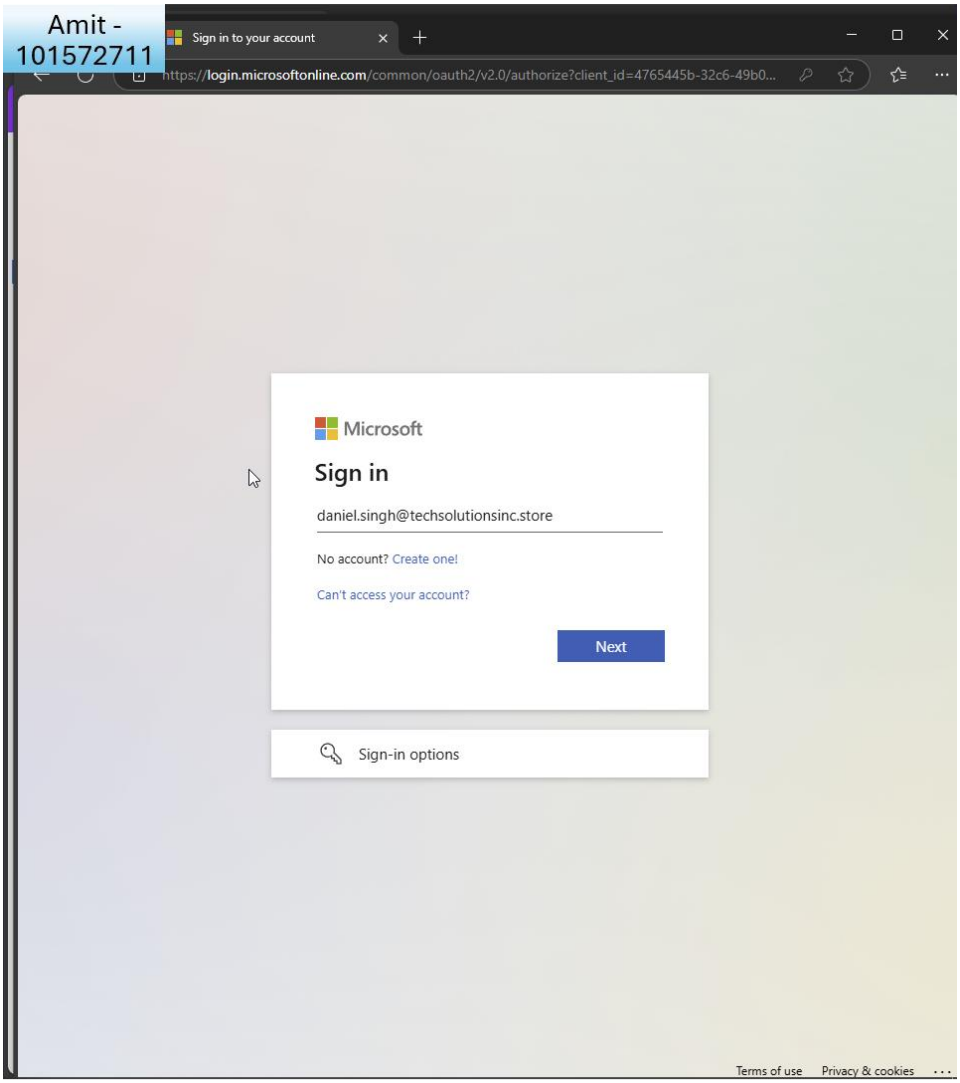
I create a 'data leak' policy

Student Name: ……. Term: …….
Student ID: …….



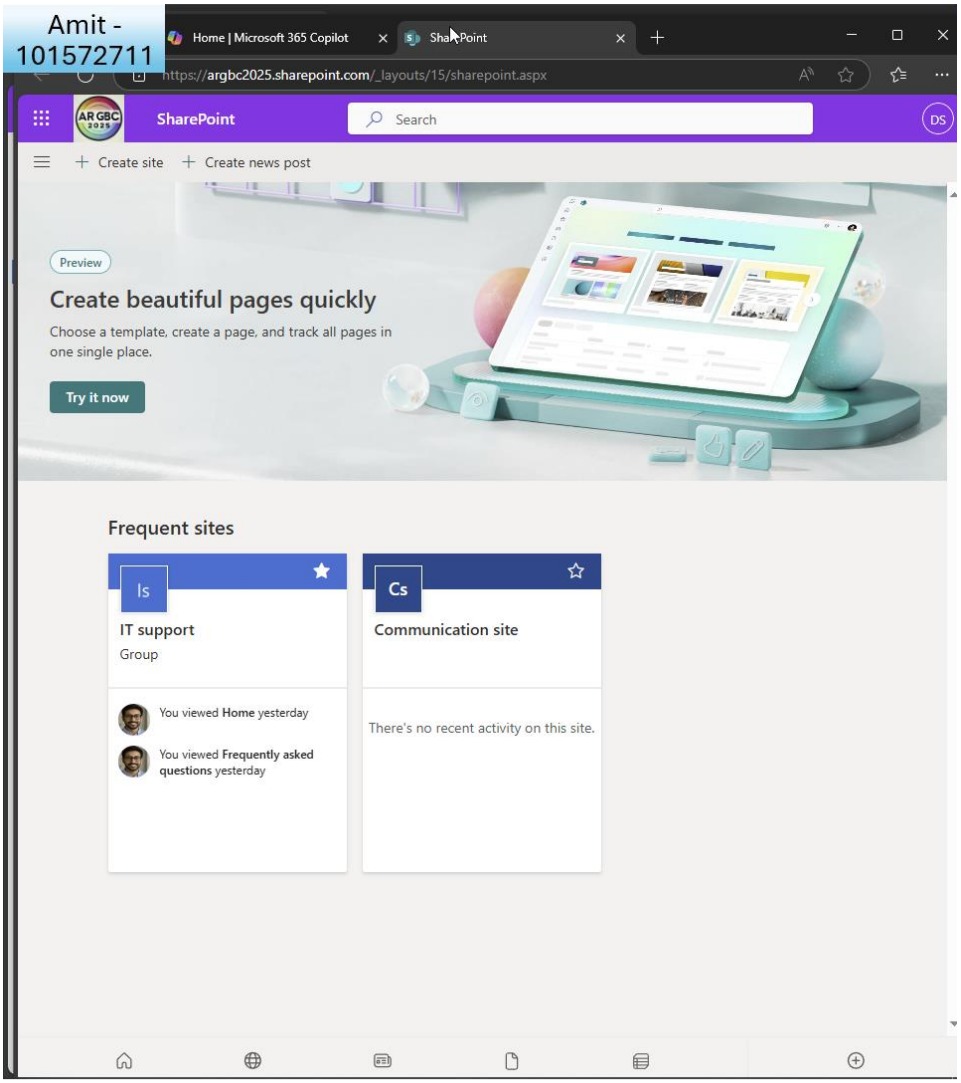
I see the new policy

Student Name: ……. Term: ……..
Student ID: ……..



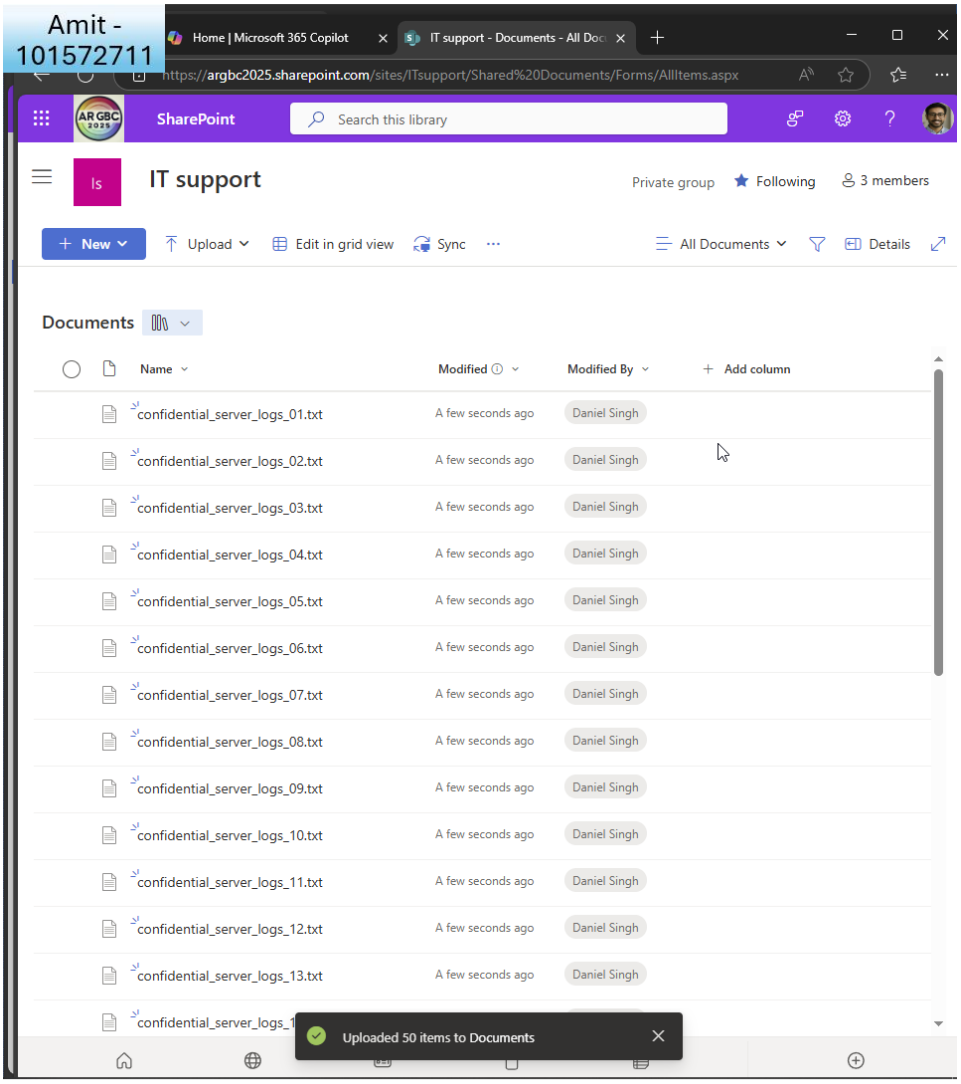
To simulate I sign in as Daniel

Student Name: ……. Term: ……..
Student ID: ……..



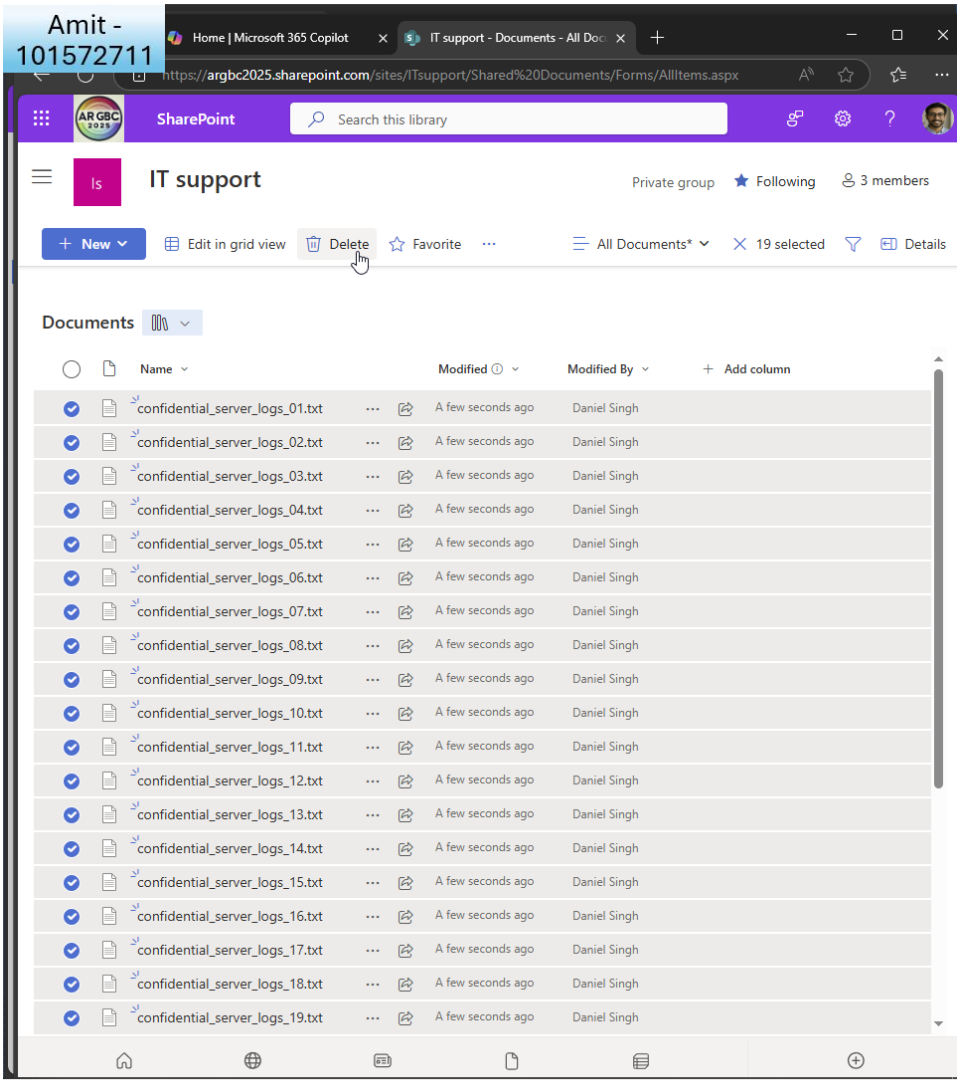
I go to IT support page to upload many documents

Student Name: ……. Term: …….
Student ID: ……..



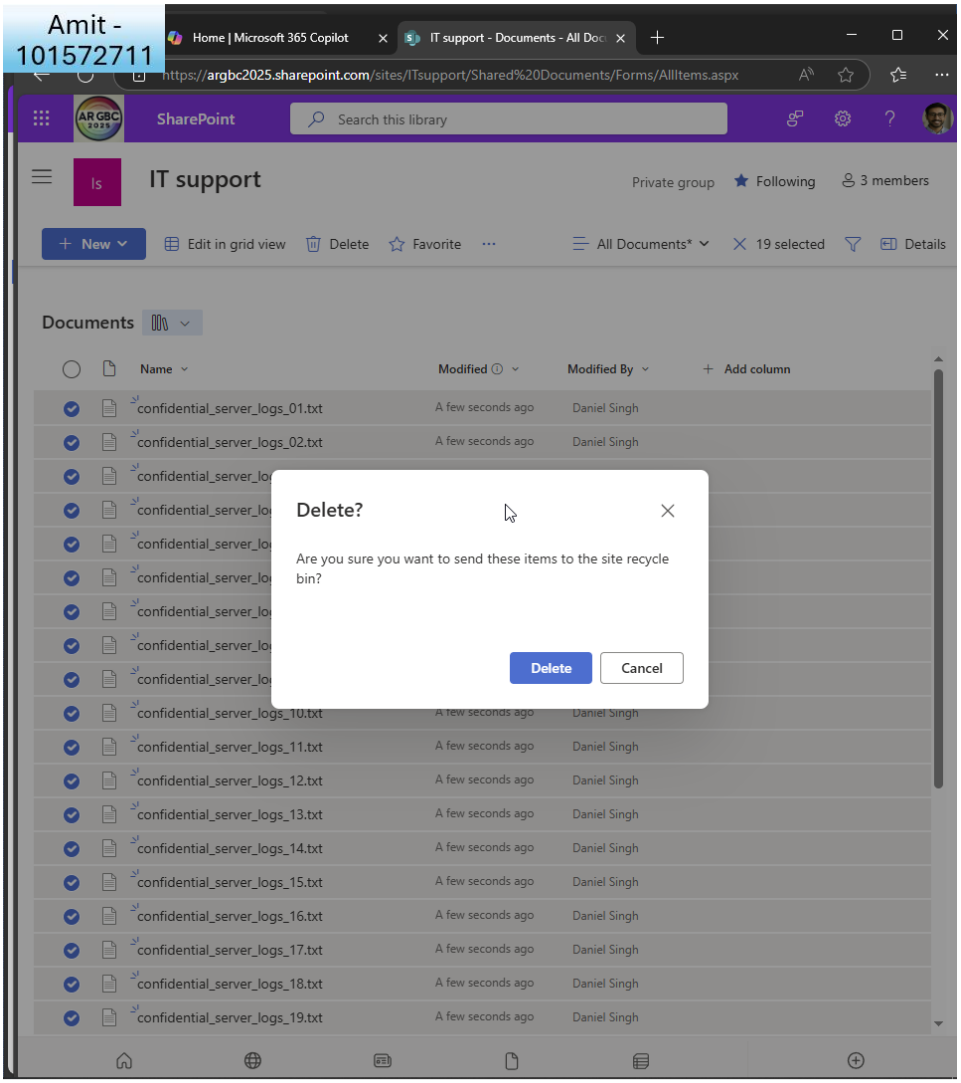
Here are the files

Student Name: ……. Term: ……..
Student ID: ……..



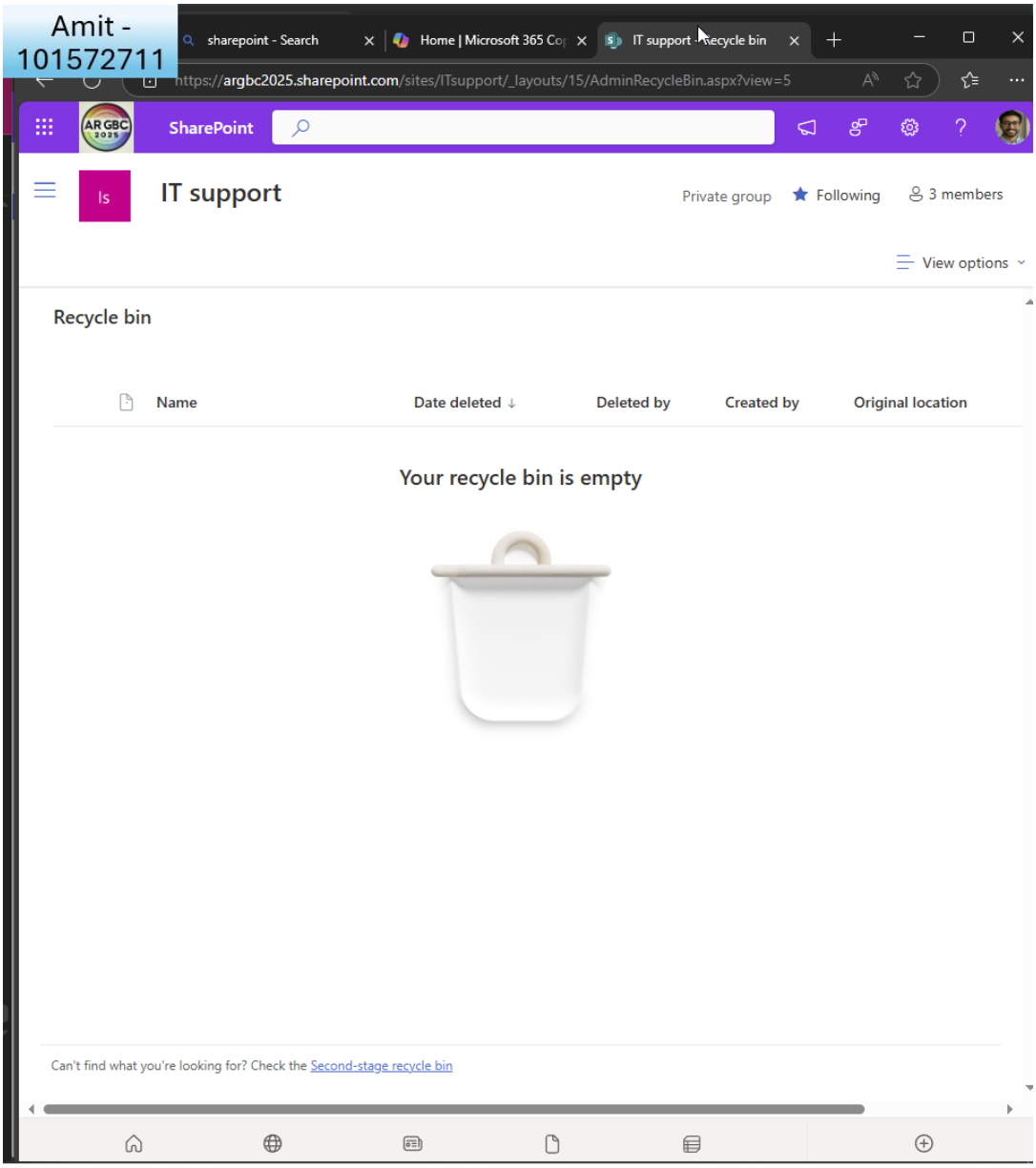
I delete multiple files

Student Name: ……. Term: ……..
Student ID: ……..



I see the confirmation and now wait up to 48 hours for the scan to show as an alert.

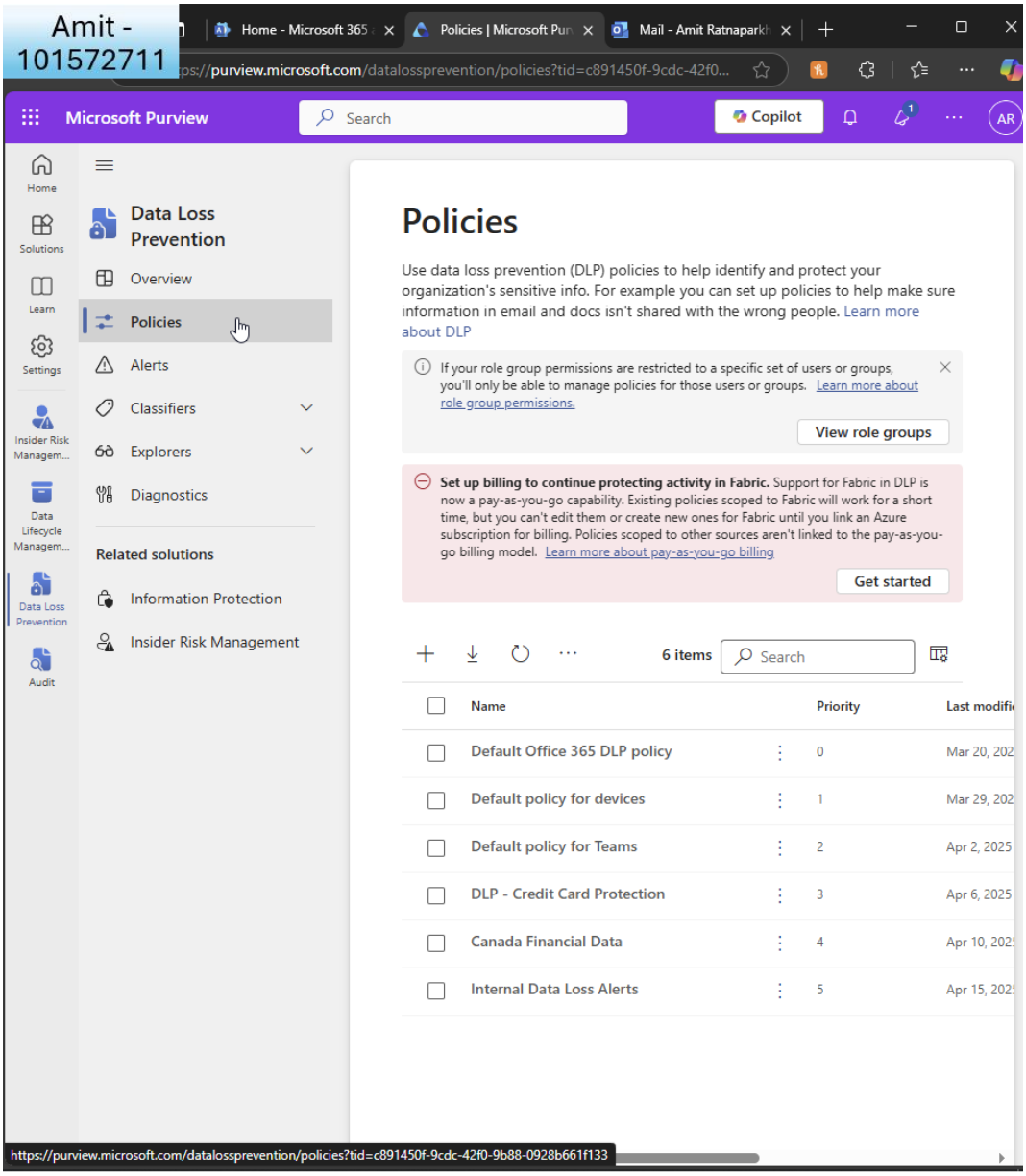
Student Name: ……. Term: ……..
Student ID: ……..



for good measure I also delete from recycle bin and now wait an hour for the alert to trigger

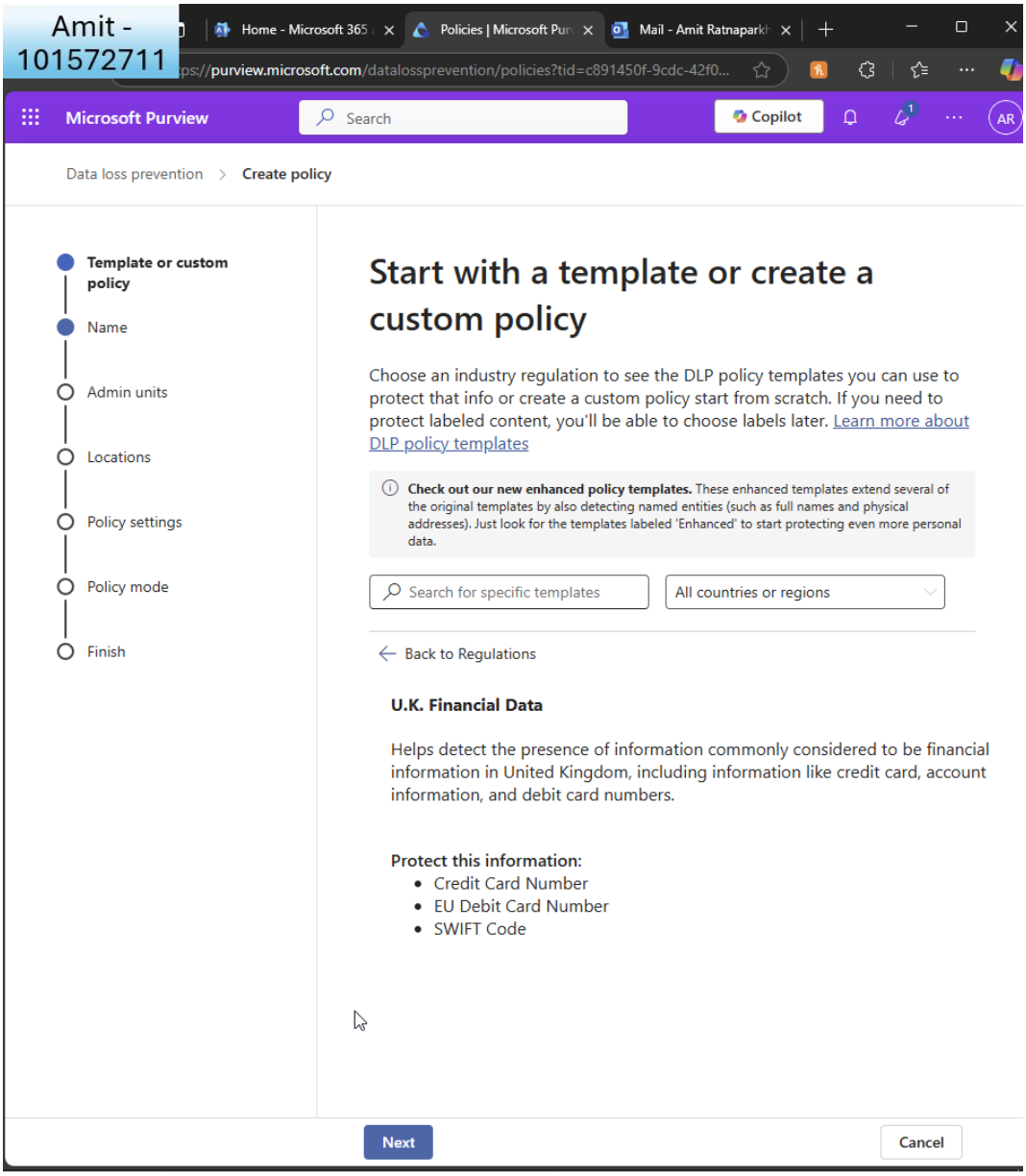
I realise that there is an issue with this DLP policy as I couldn't get to alert so I will start again with a brand new DLP policy:

Student Name: ……. Term: ……..
Student ID: ……..



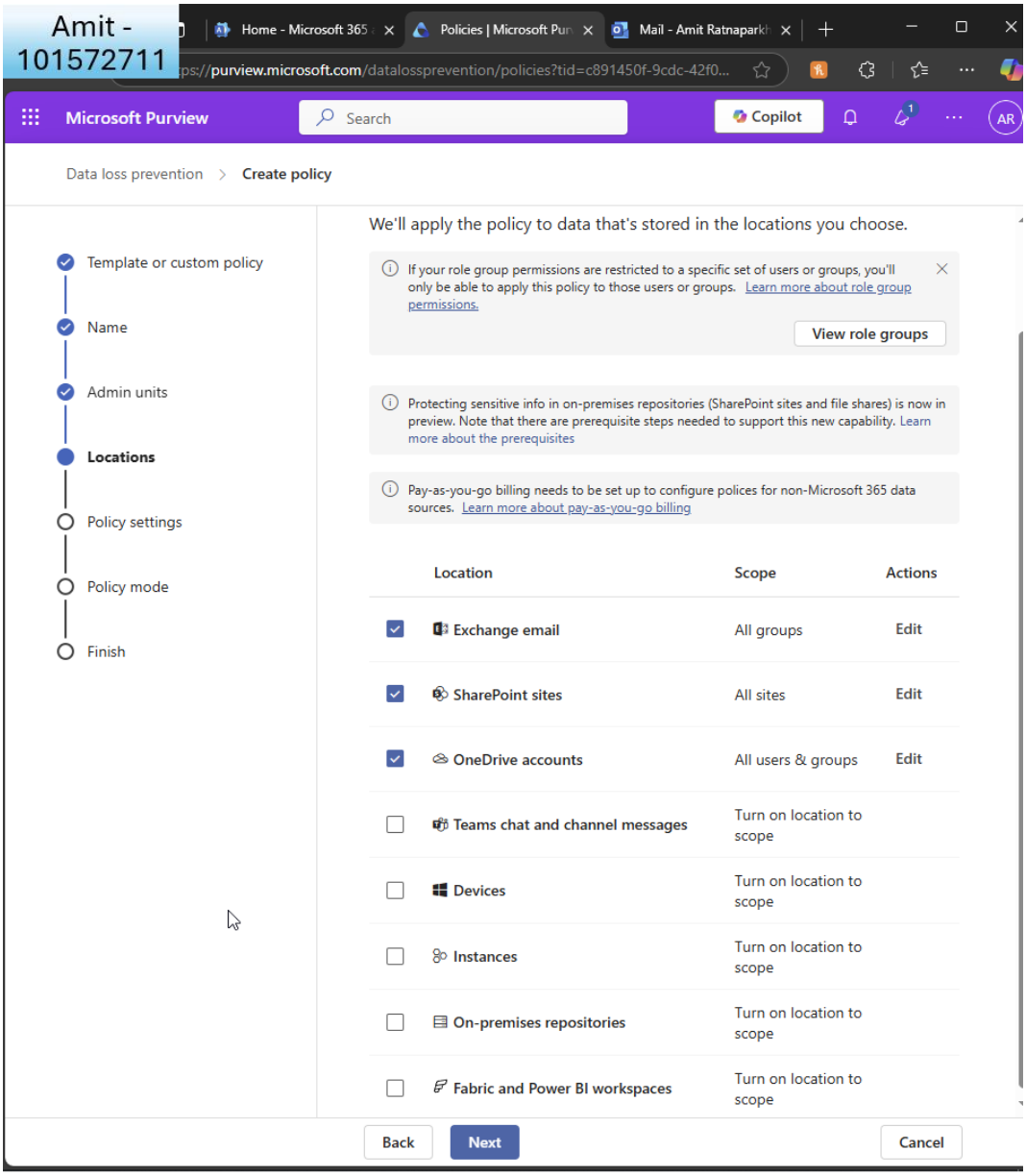
I create a new DLP policy

Student Name: ……. Term: ……..
Student ID: ……..



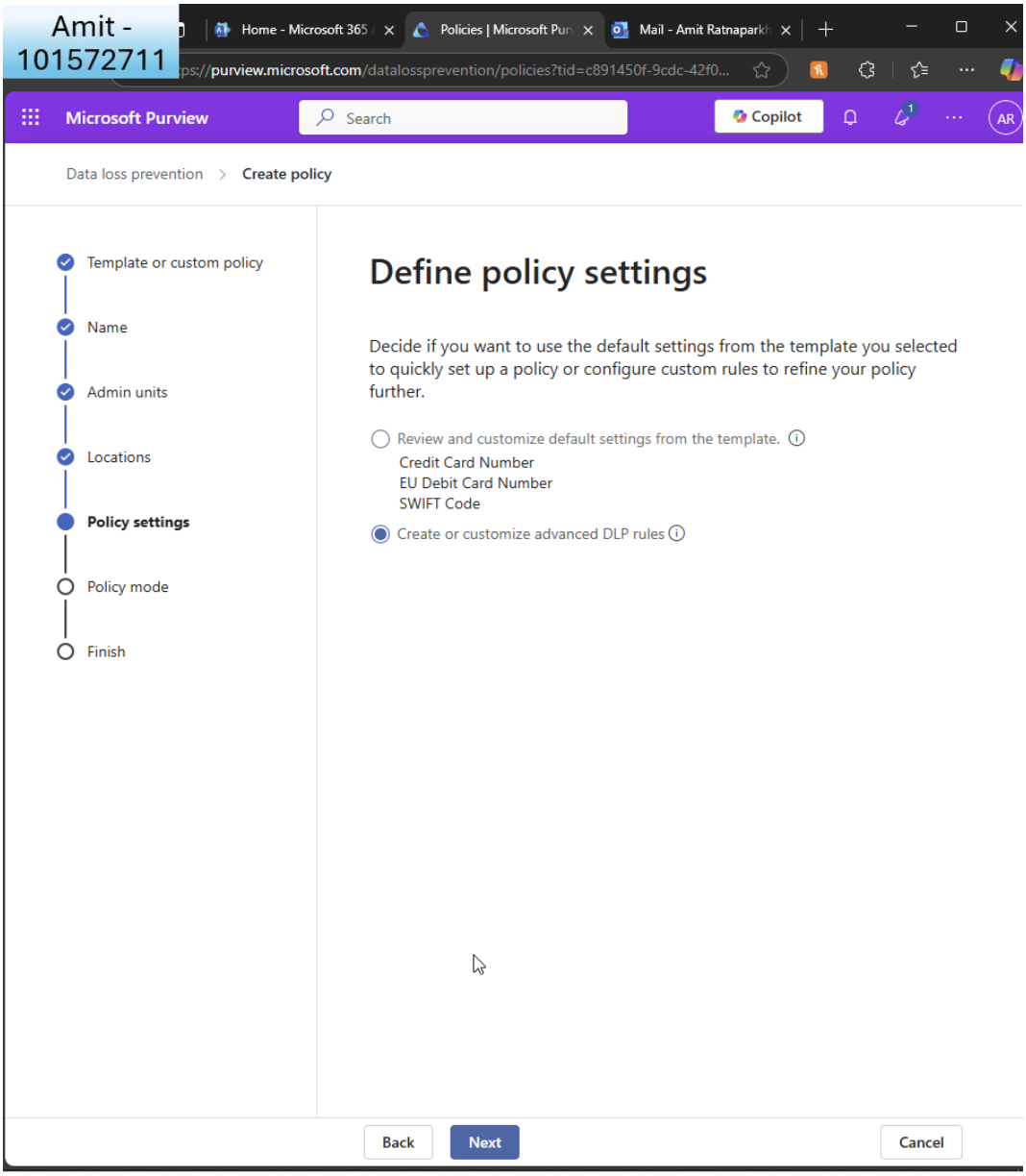
I choose UK financial date and choose a template

Student Name: ……. Term: ……..
Student ID: ……..



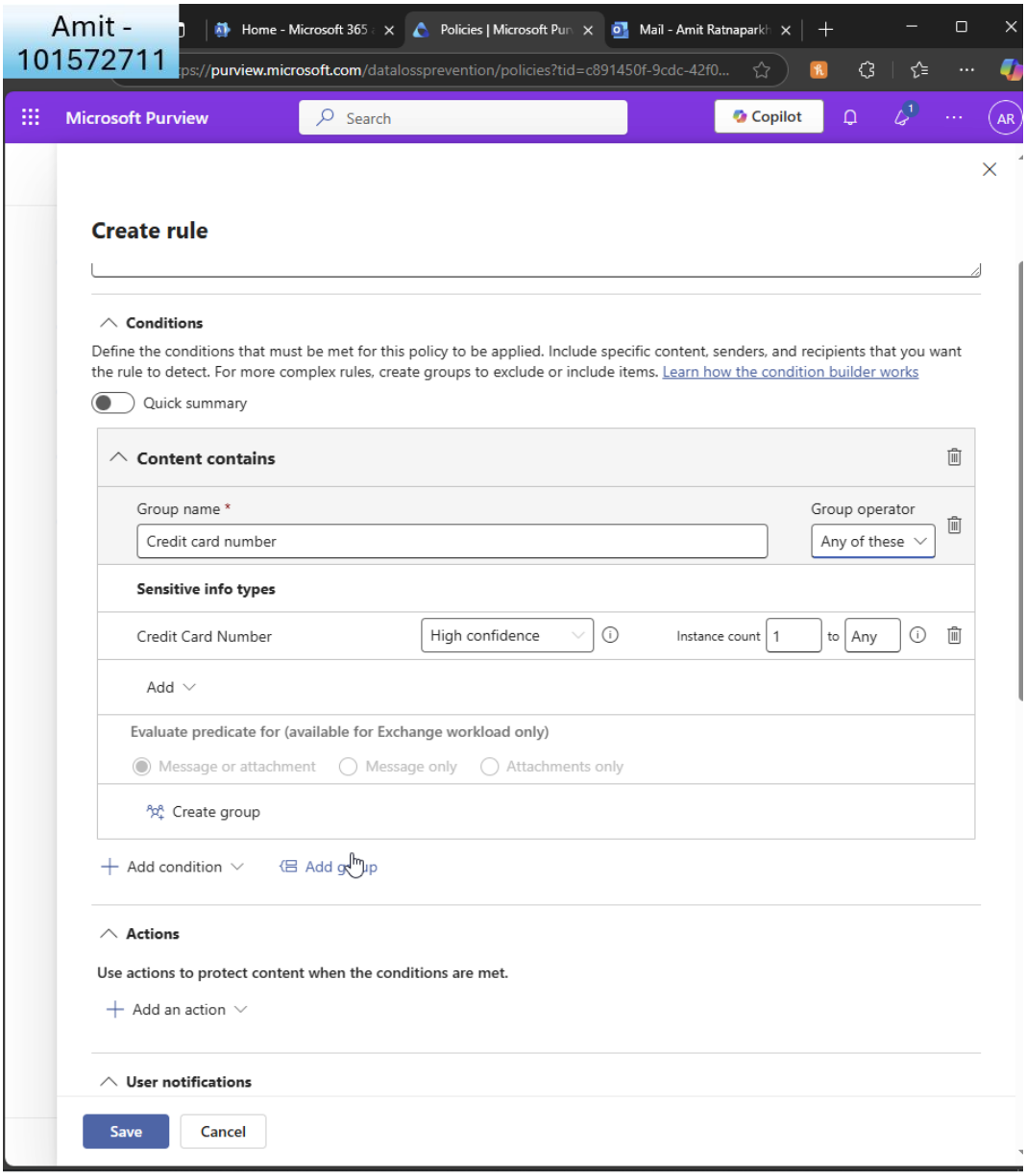
I ensure locations are correct

Student Name: ……. Term: ……..
Student ID: ……..



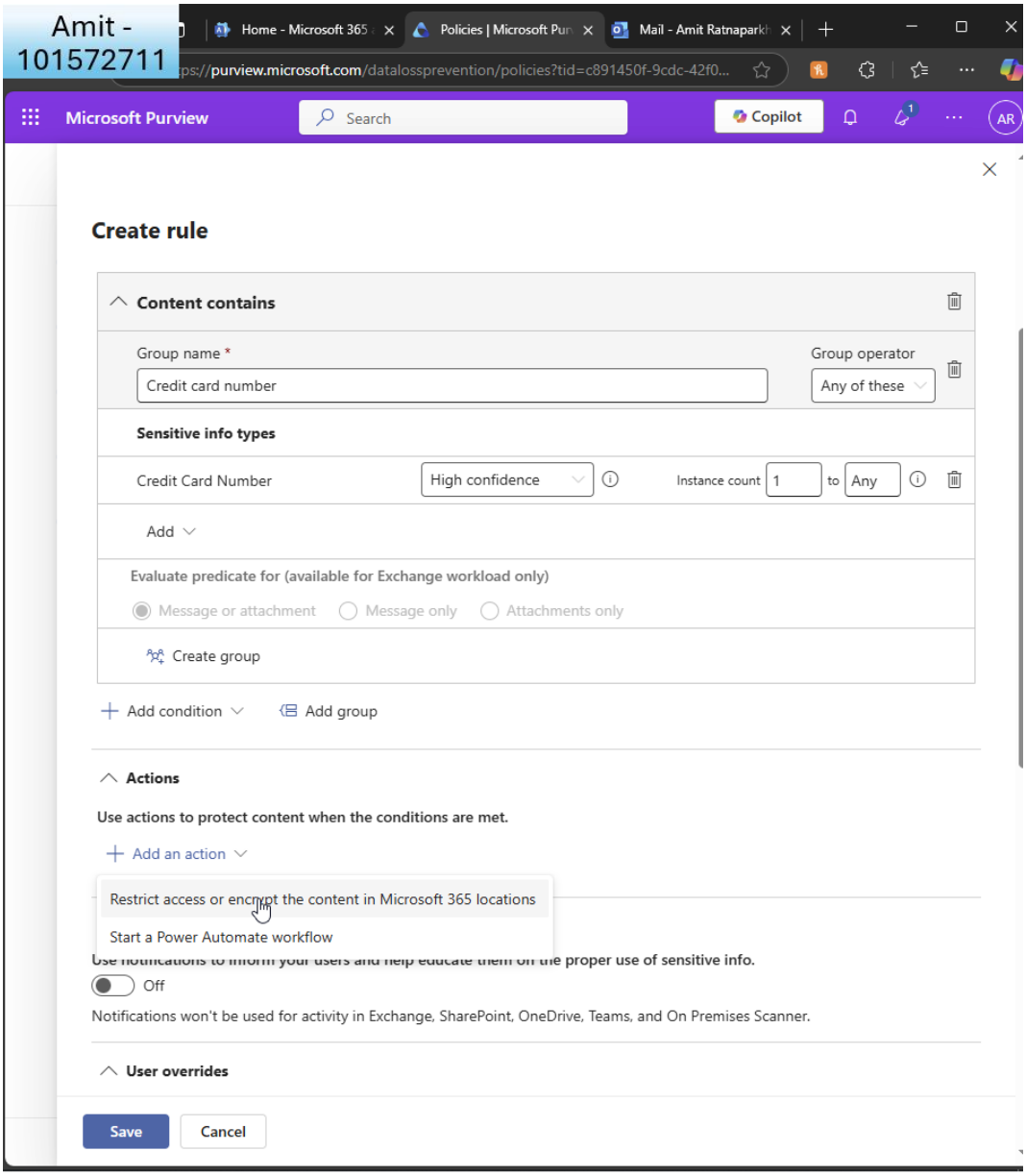
I define the policy settings and customise

Student Name: ……. Term: …….
Student ID: …….



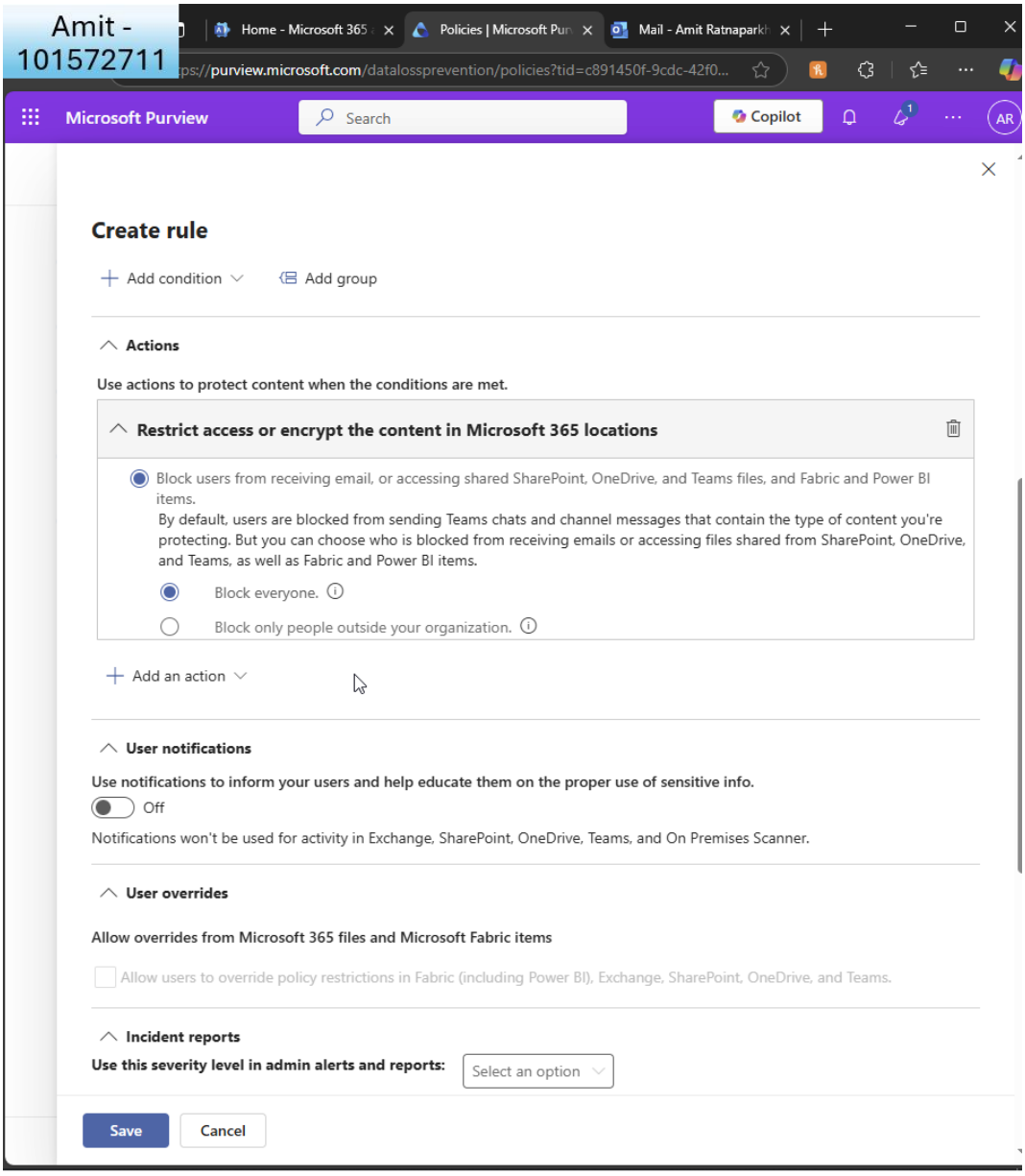
I create the rule for credit card numbers

Student Name: ……. Term: ……..
Student ID: ……..



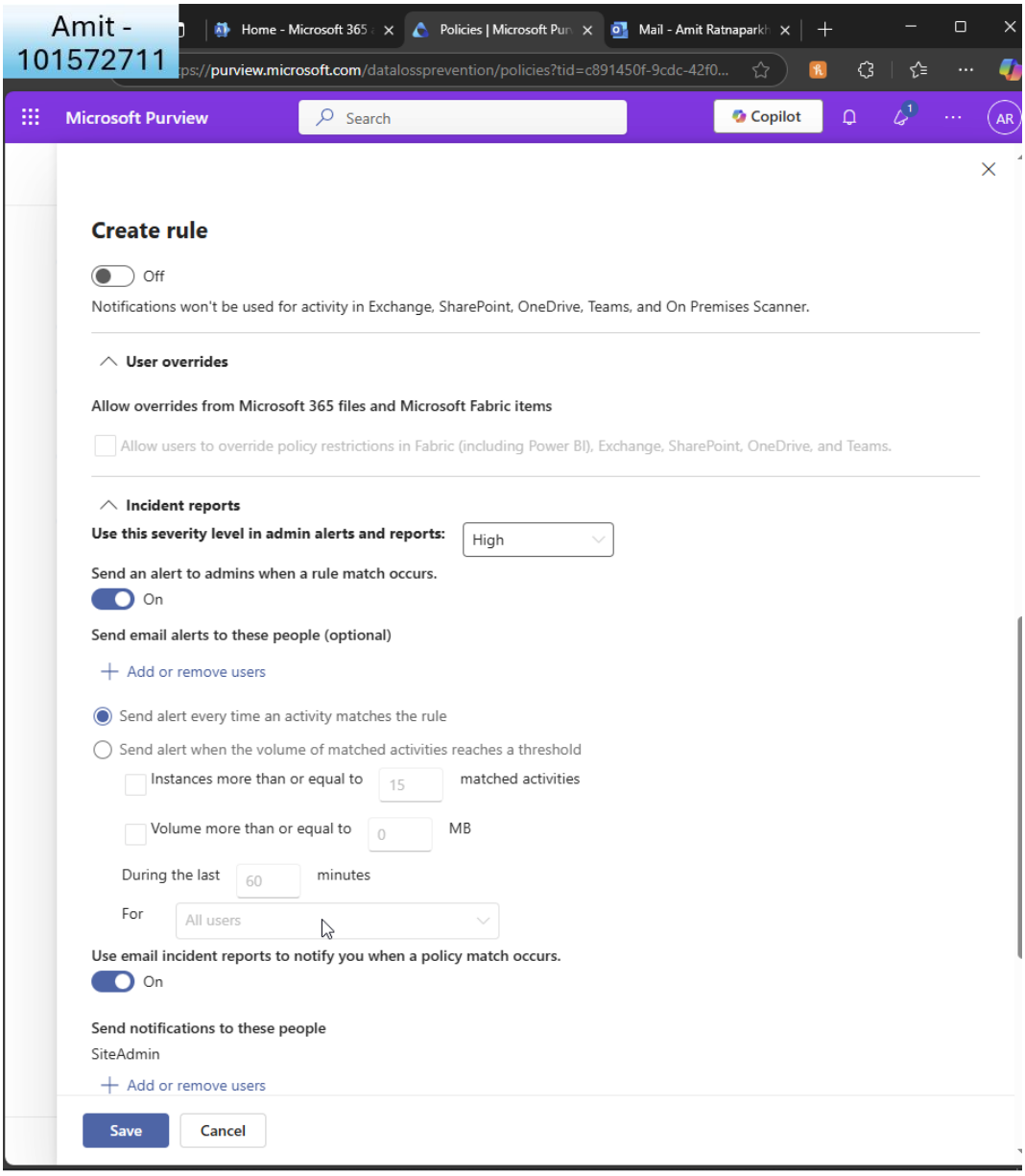
I restrict access for the user

Student Name: ……. Term: ……..
Student ID: ……..



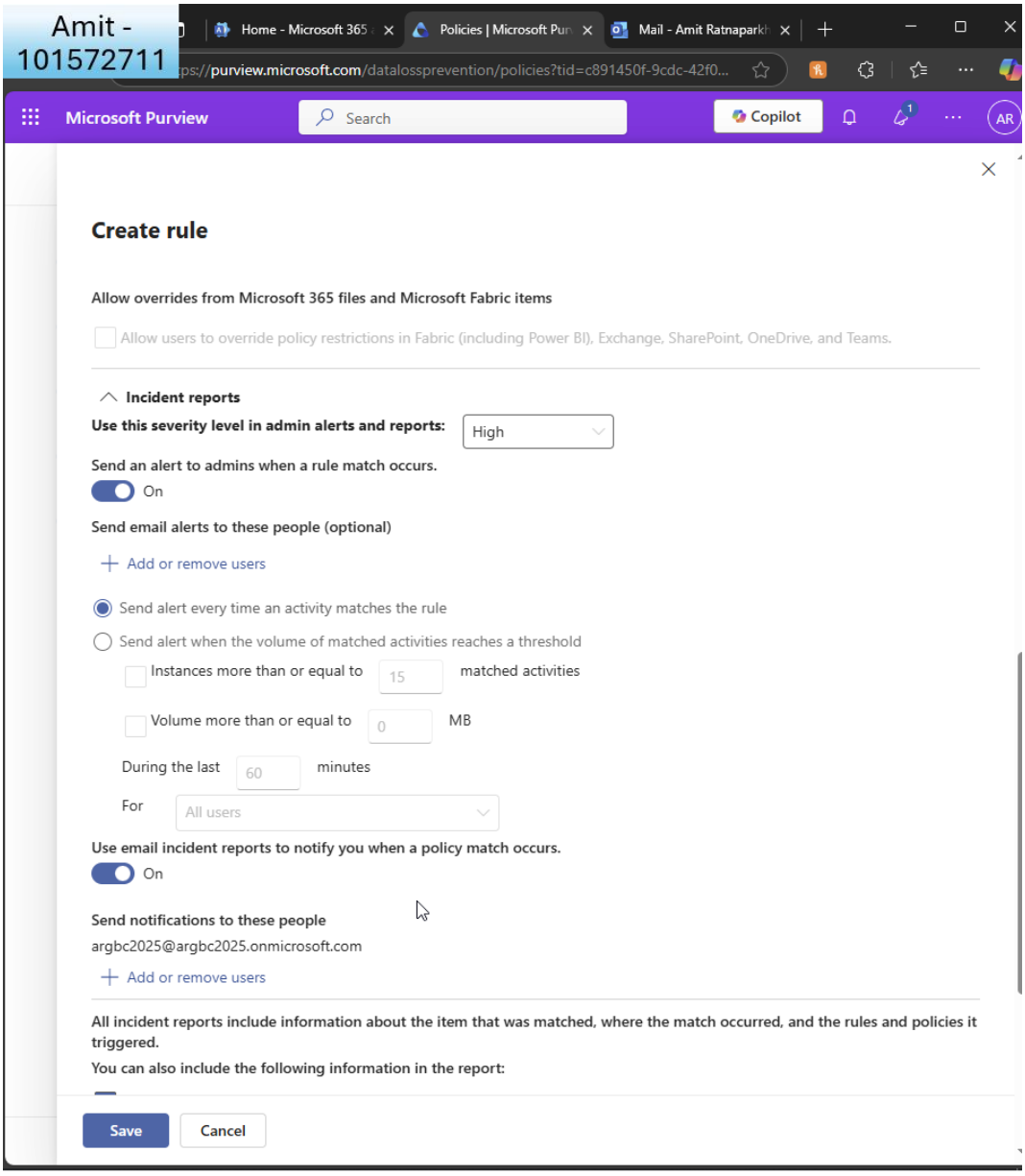
I choose 'block everyone'

Student Name: ……. Term: …….
Student ID: …….



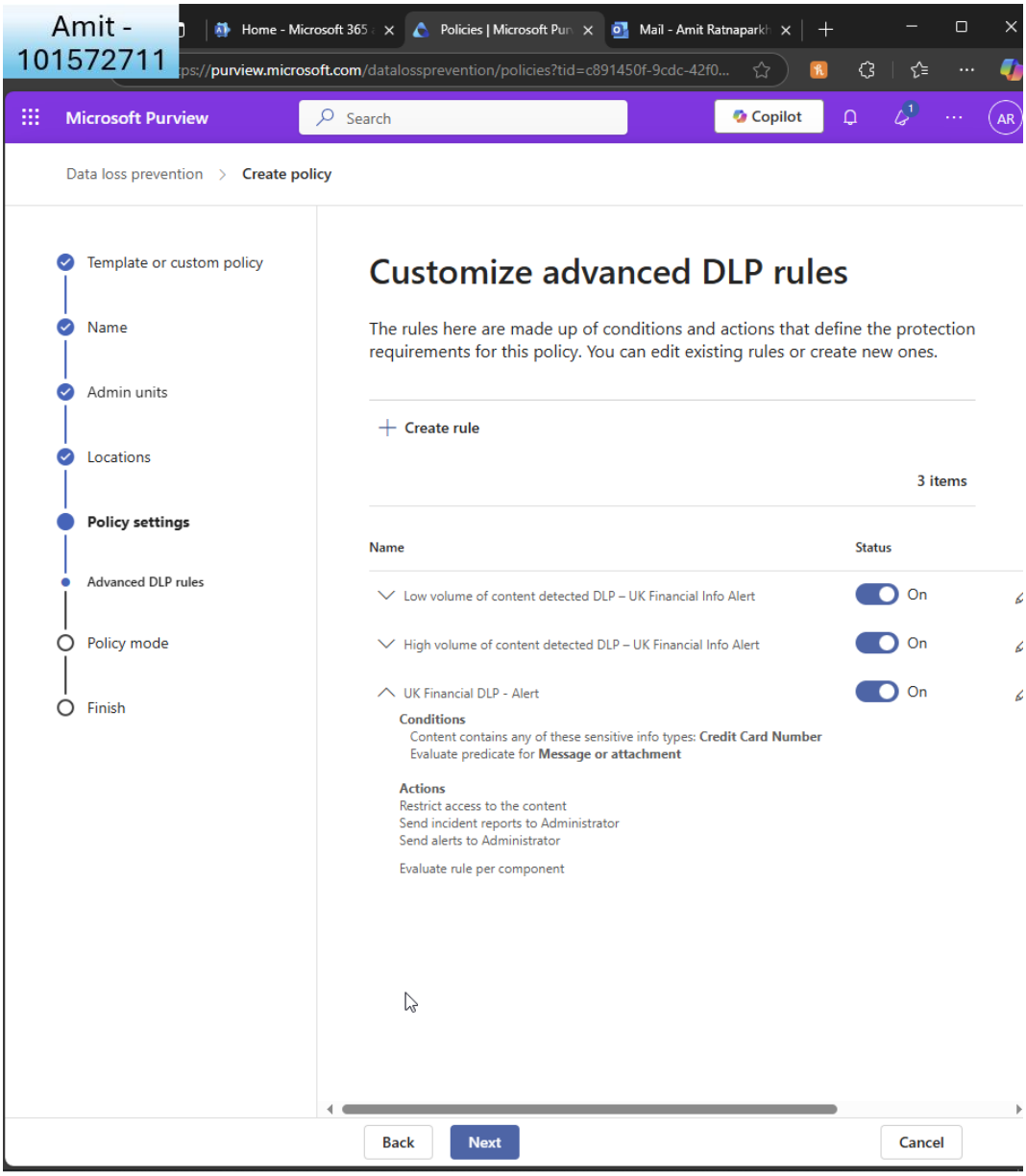
I choose to send alerts to admins

Student Name: ……. Term: ……..
Student ID: ……..



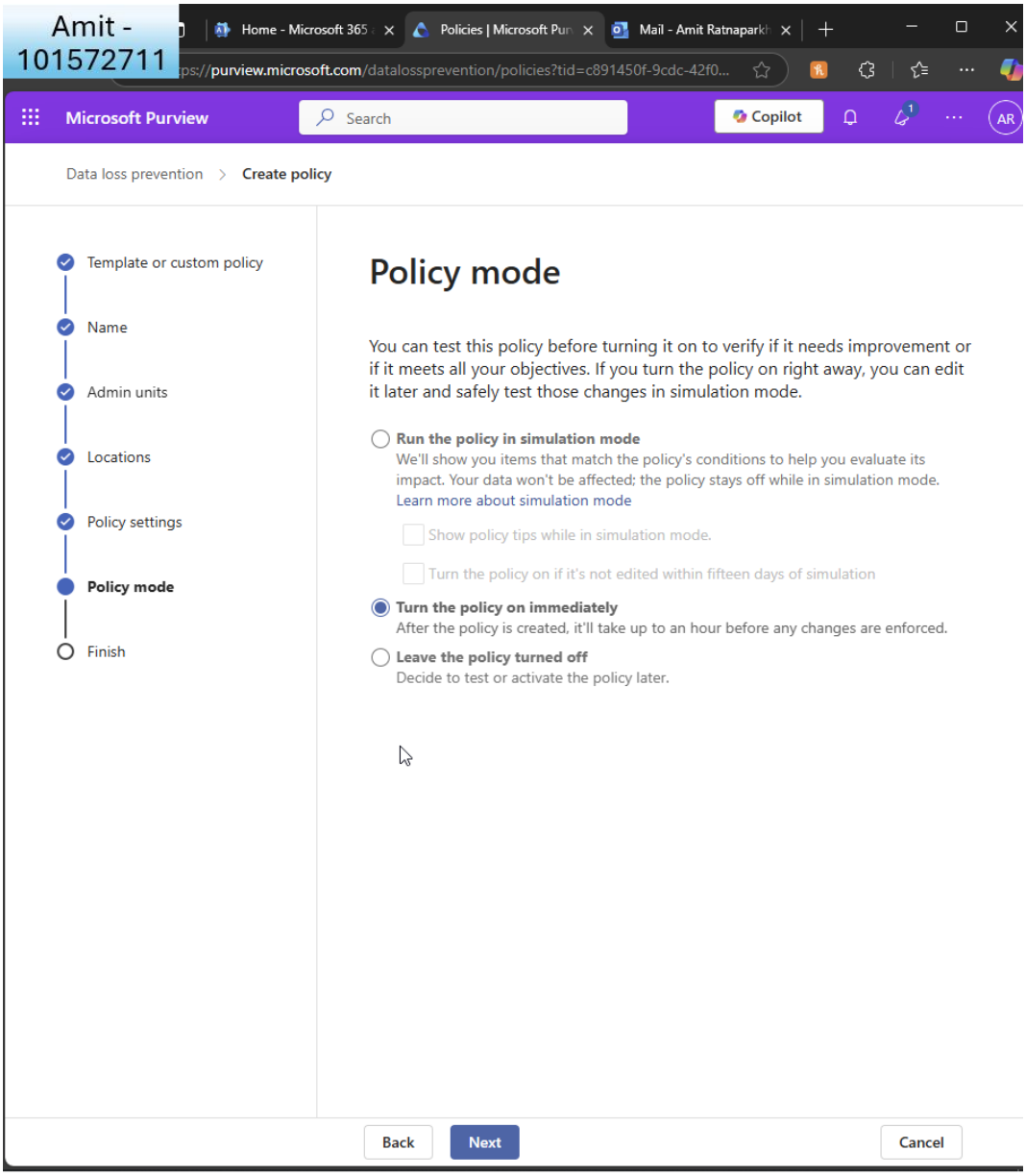
I make sure action is taken with rule match occurs

Student Name: ……. Term: ……..
Student ID: ……..



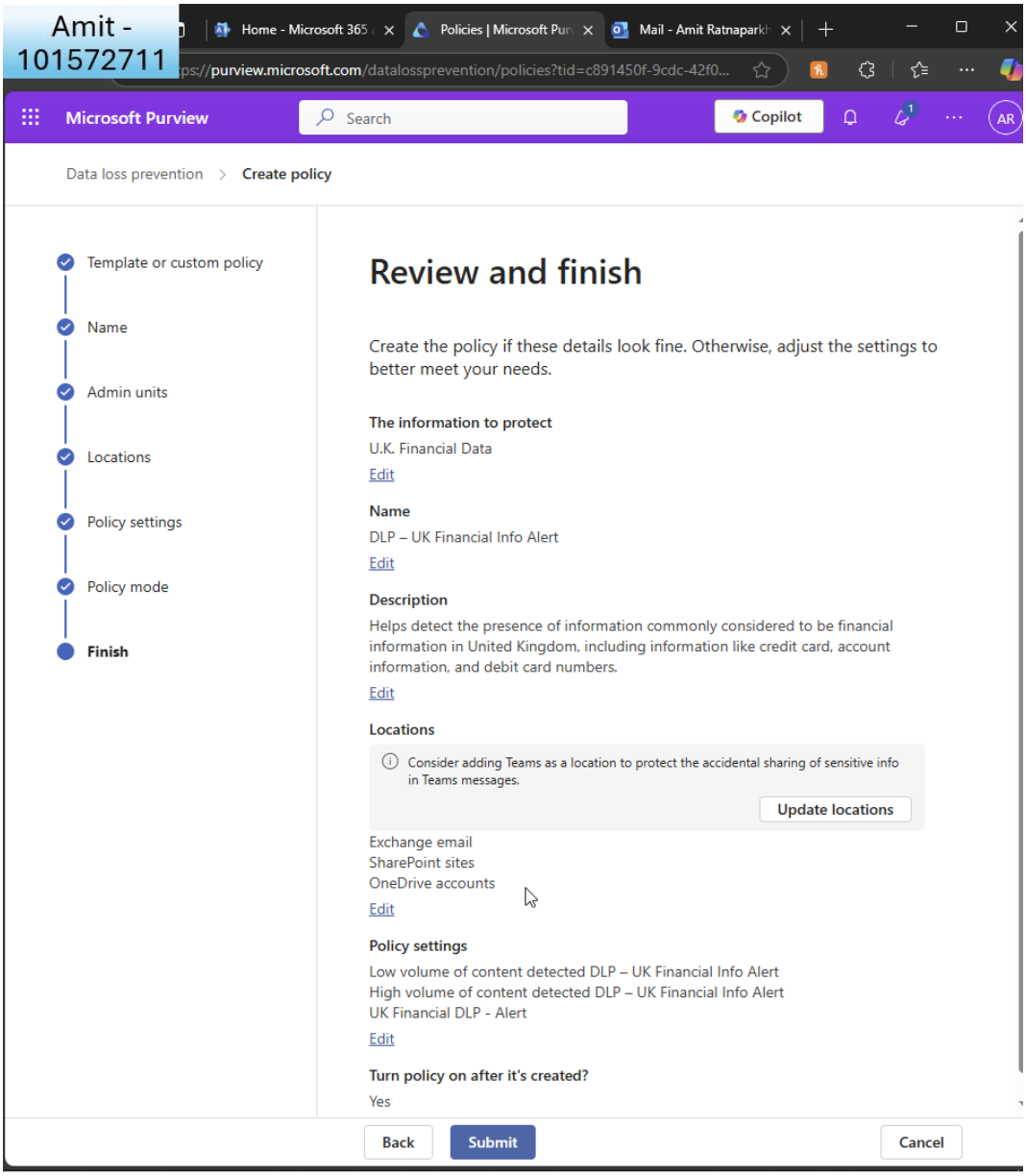
I review the customised options

Student Name: ……. Term: ……..
Student ID: ……..



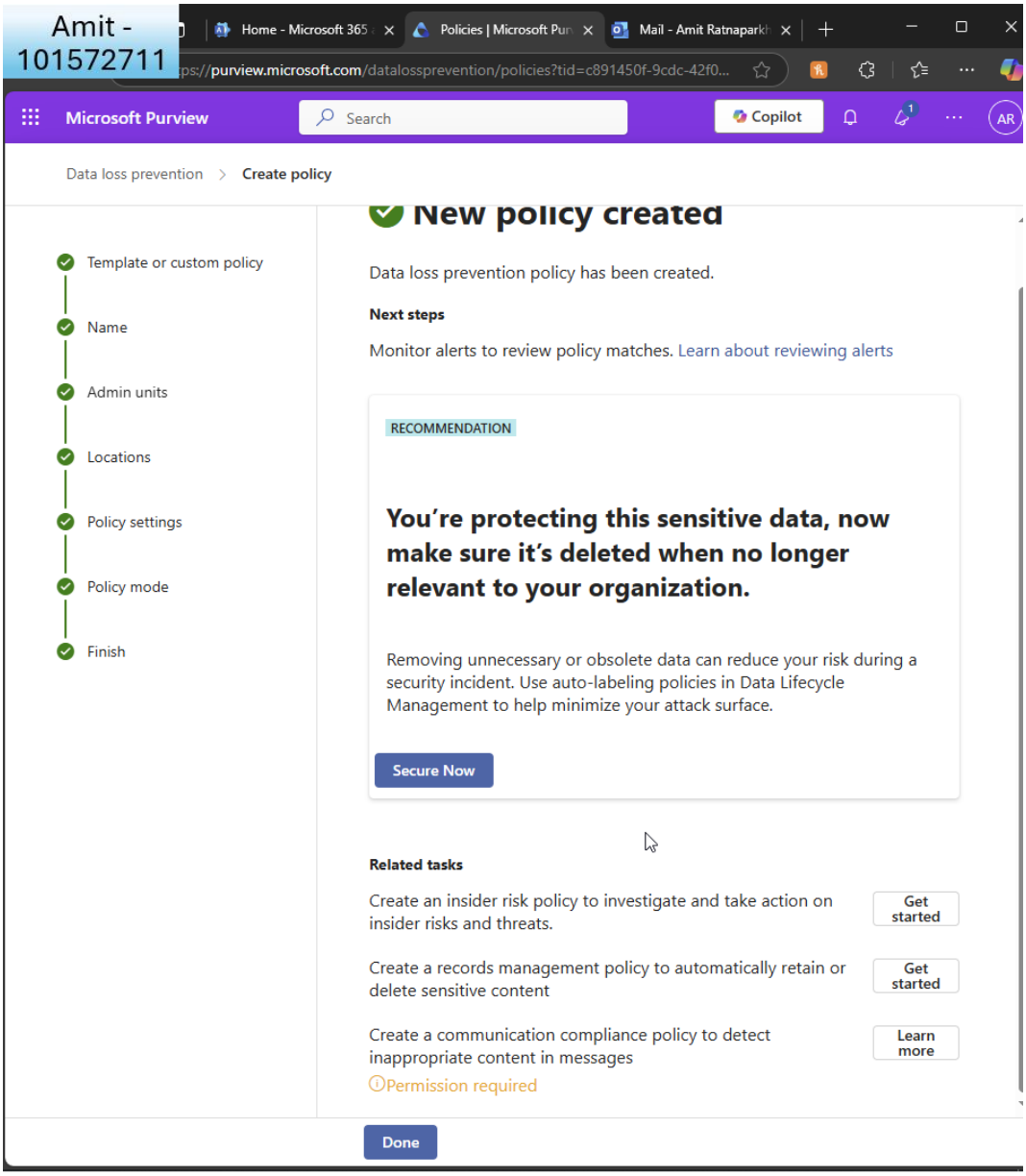
I turn the policy on

Student Name: ……. Term: ……..
Student ID: ……..



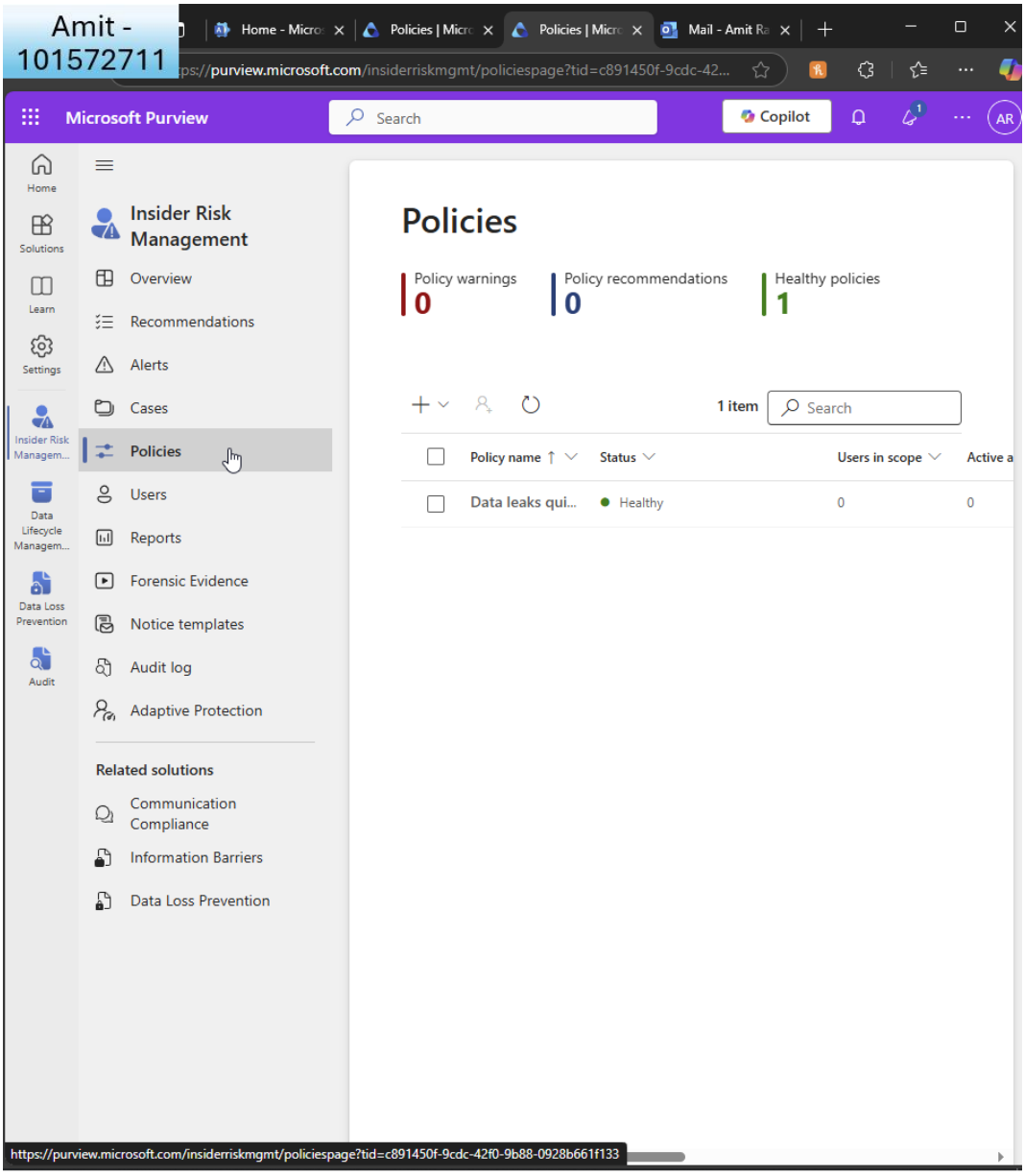
I review and finish

Student Name: ……. Term: ……..
Student ID: ……..



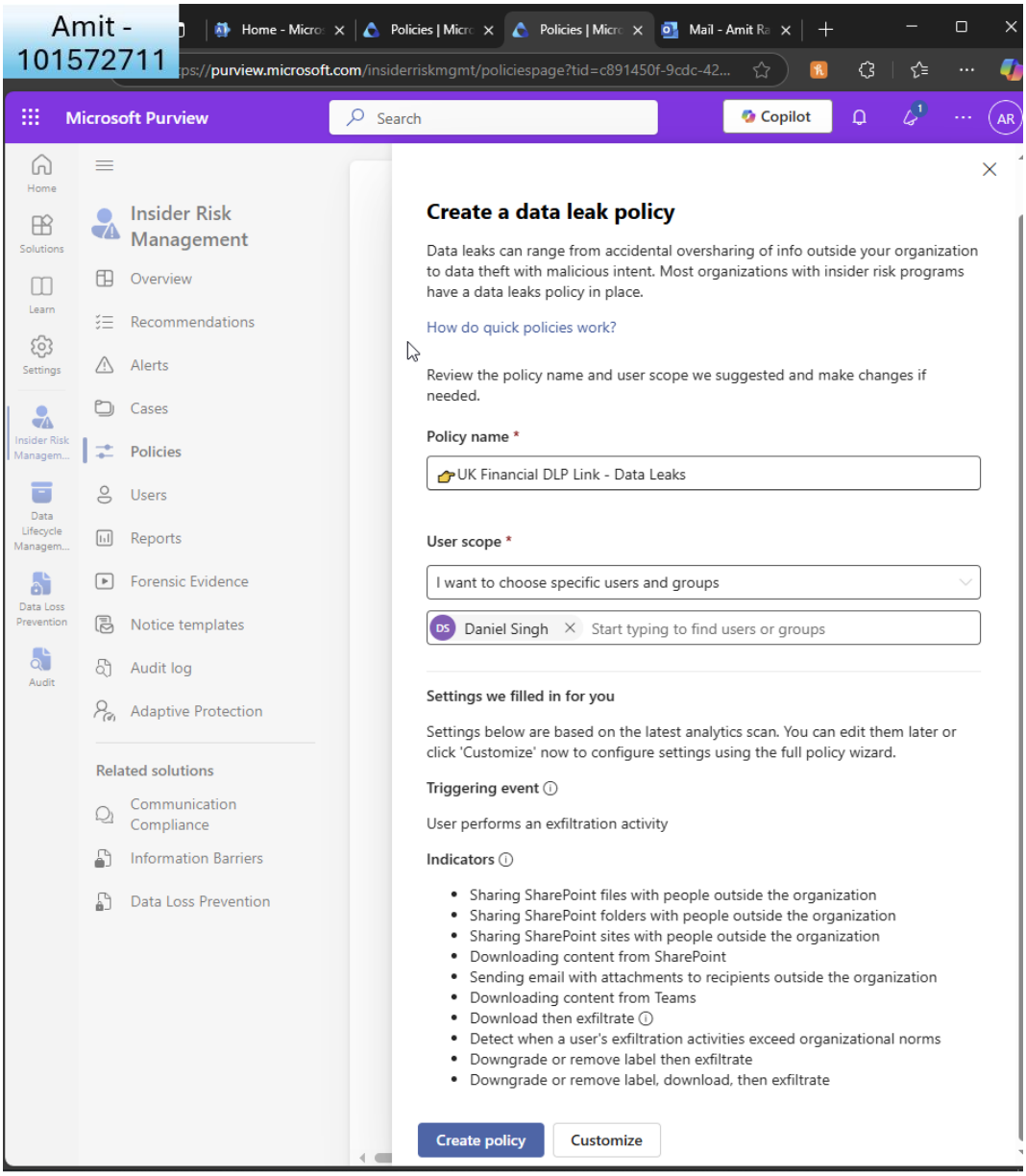
From here I directly go to creating an insider risk policy

Student Name: ……. Term: ……..
Student ID: ……..



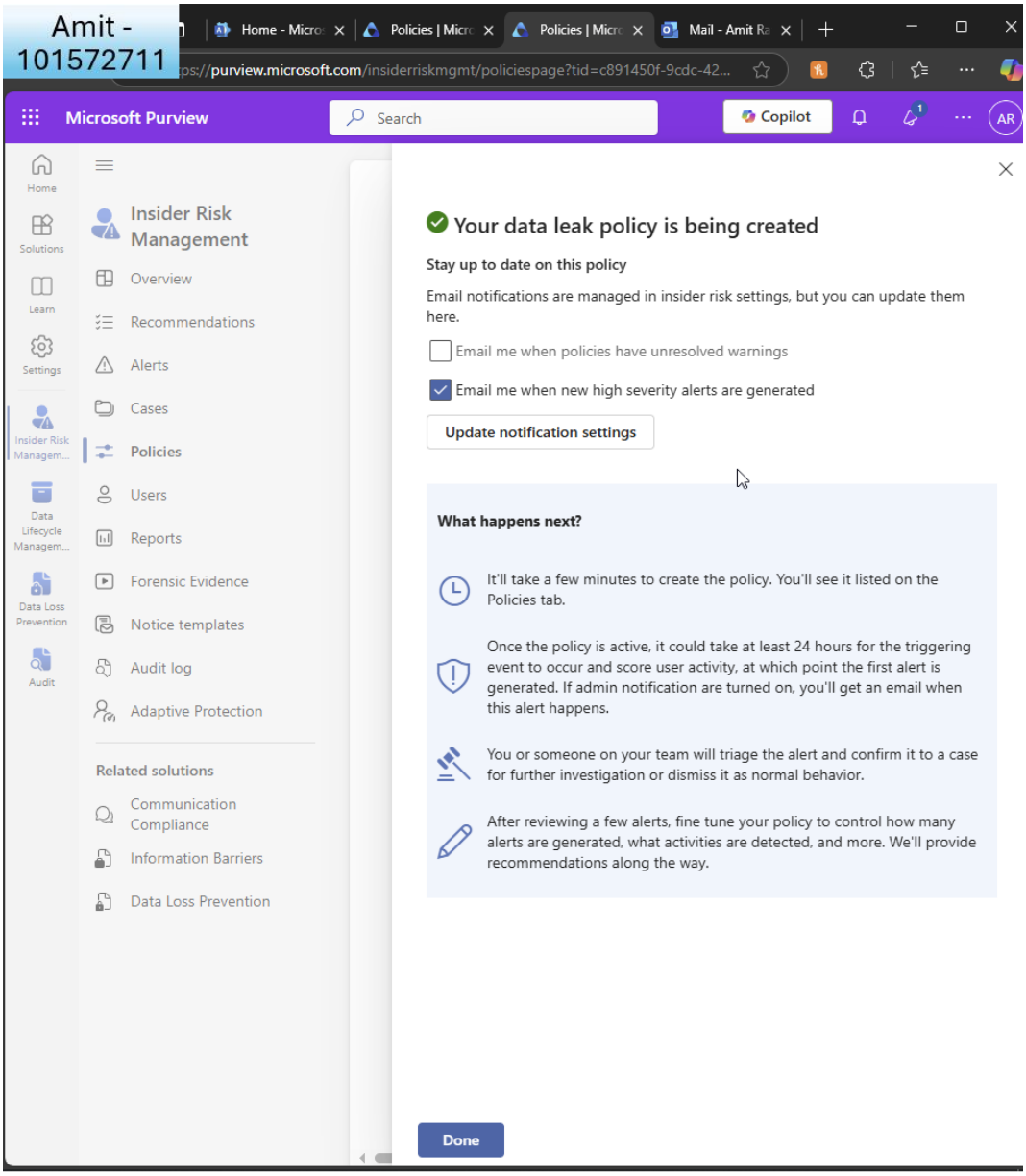
I go to 'policies'

Student Name: ……. Term: ……..
Student ID: ……..



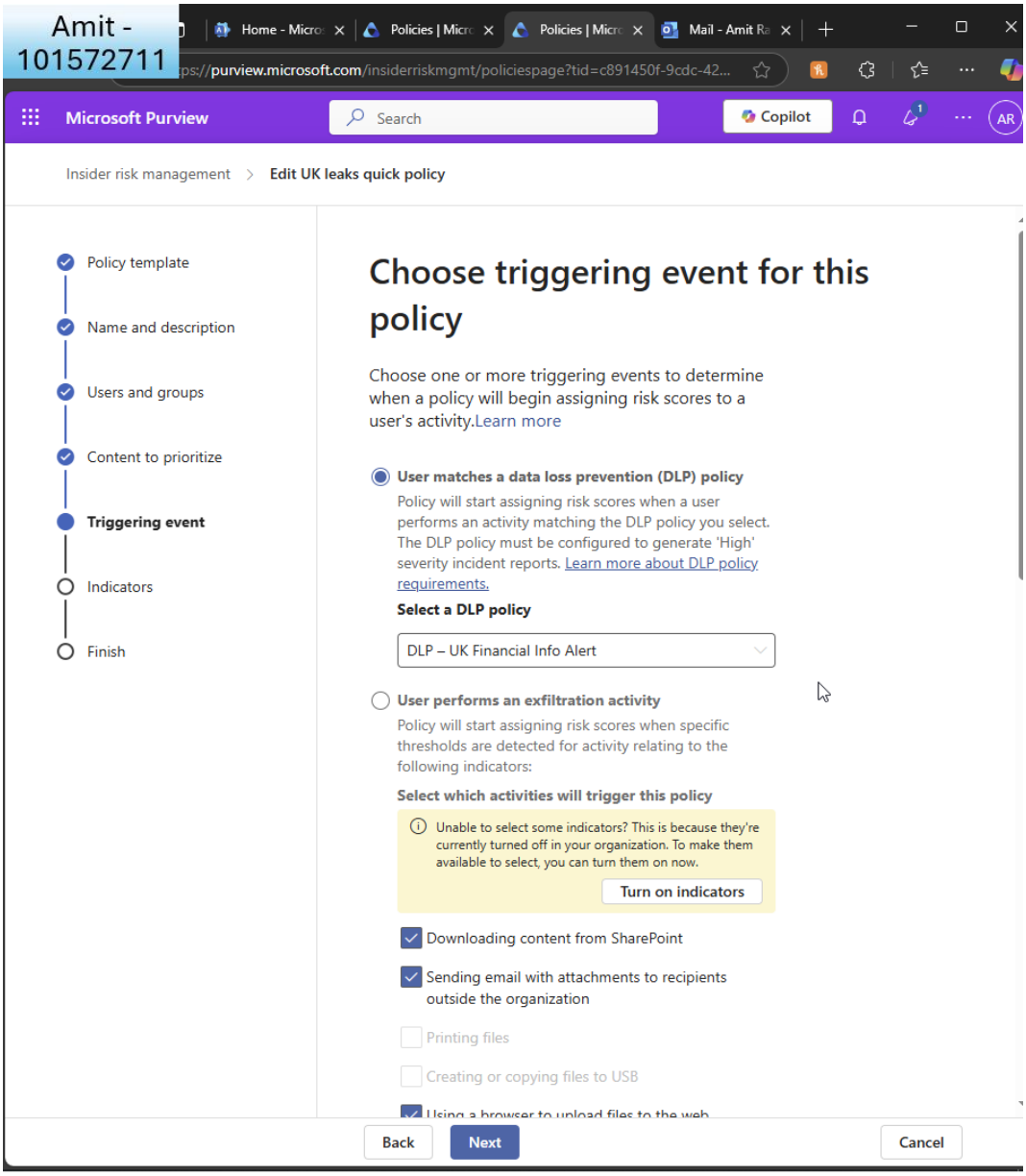
I create a data leak policy (quick) create

Student Name: ……. Term: ……..
Student ID: ……..



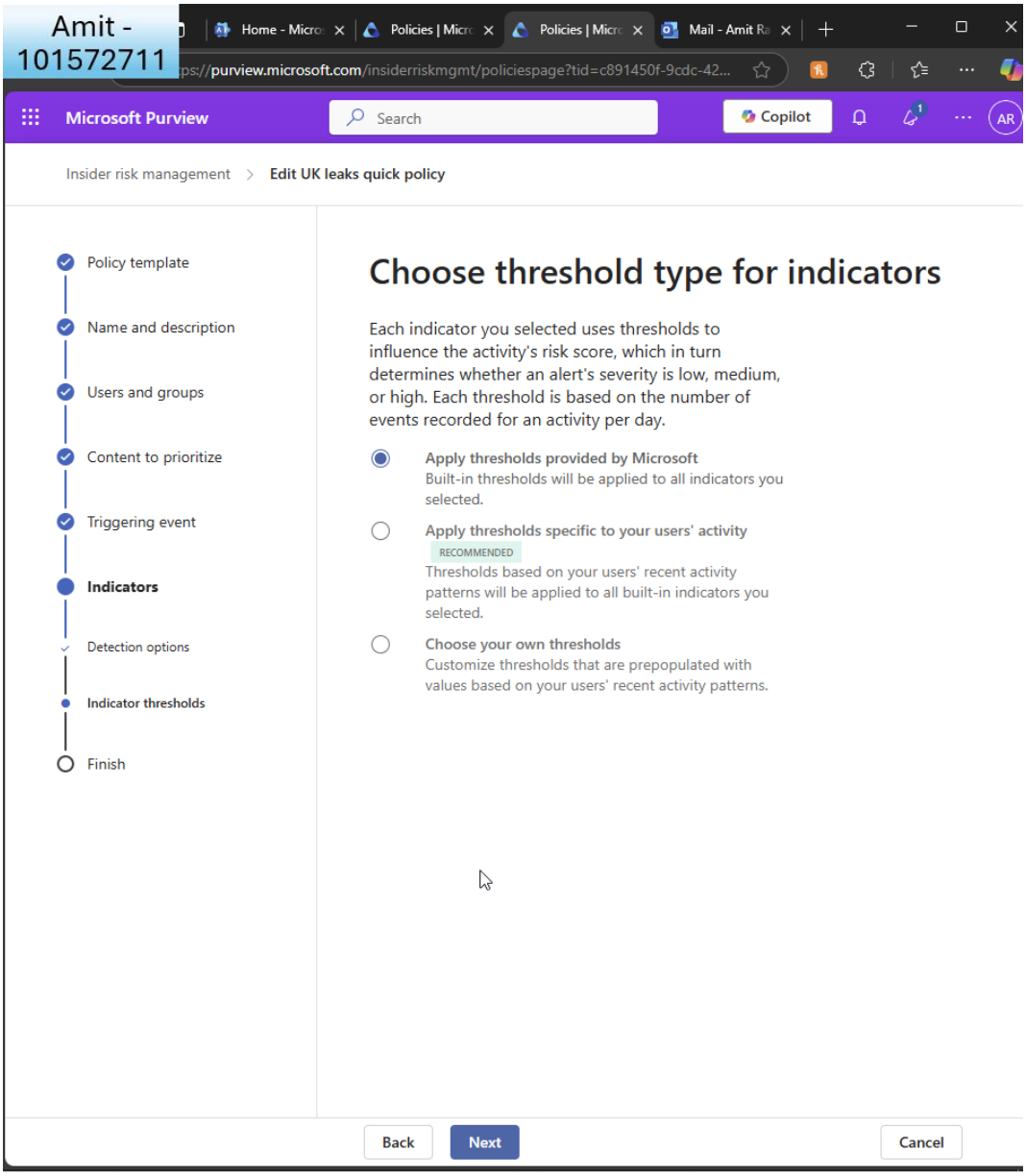
I see the confirmation

Student Name: ……. Term: ……..
Student ID: ……..



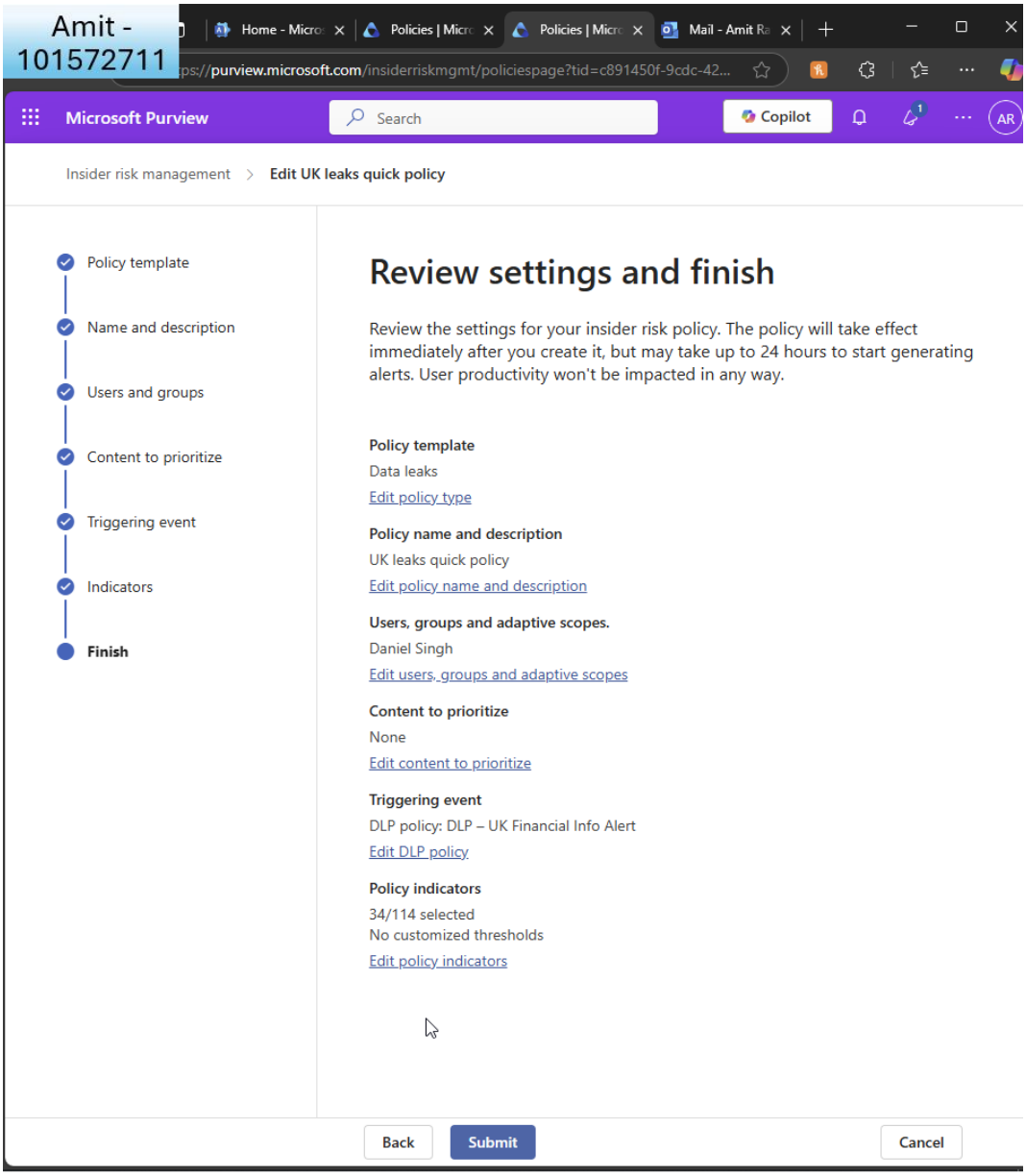
IRM said I need to choose a triggering event so I choose to run it when matched to my credit card DLP policy

Student Name: ……. Term: ……..
Student ID: ……..



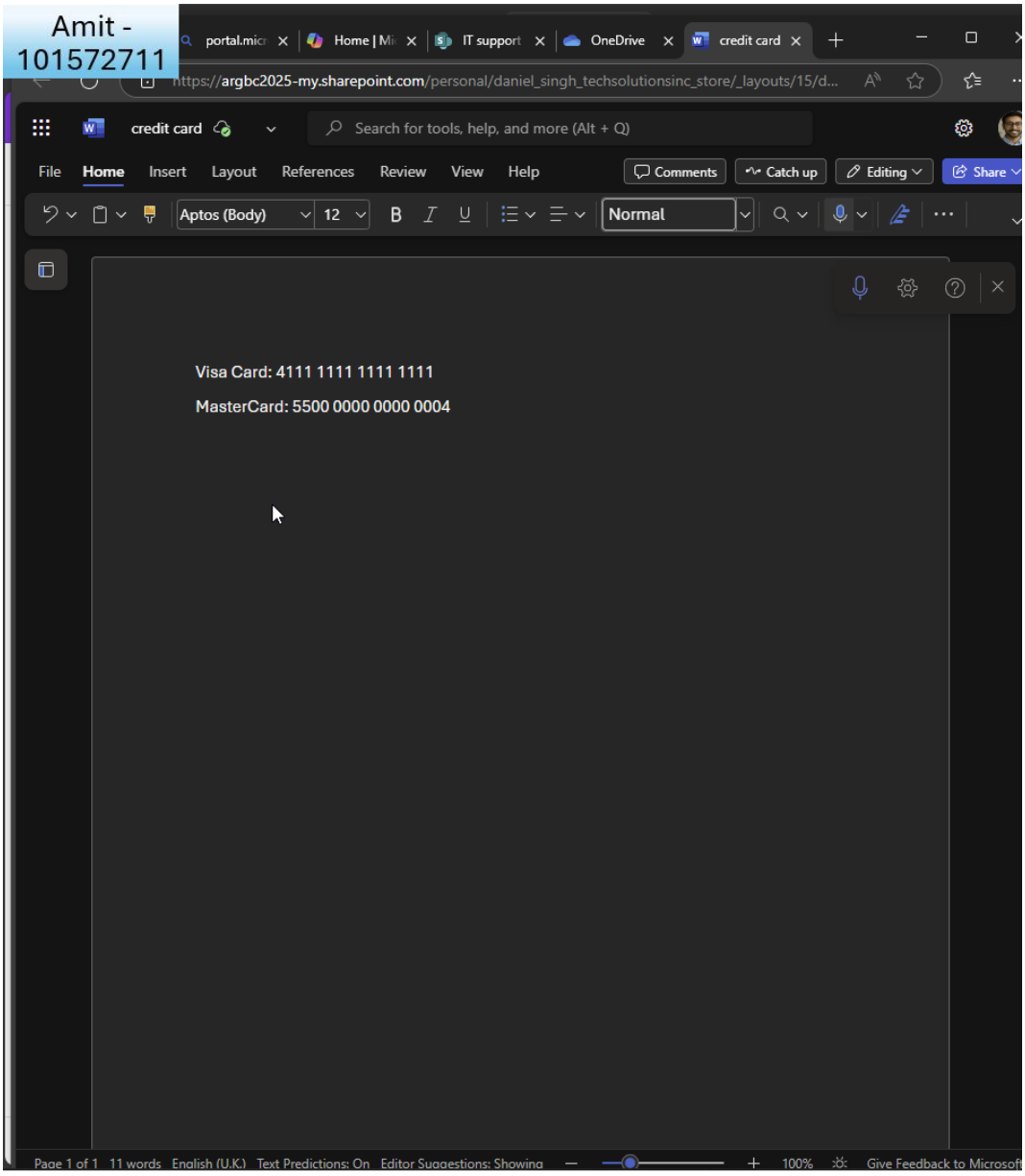
I choose default thresholds by MS

Student Name: ……. Term: ……..
Student ID: ……..



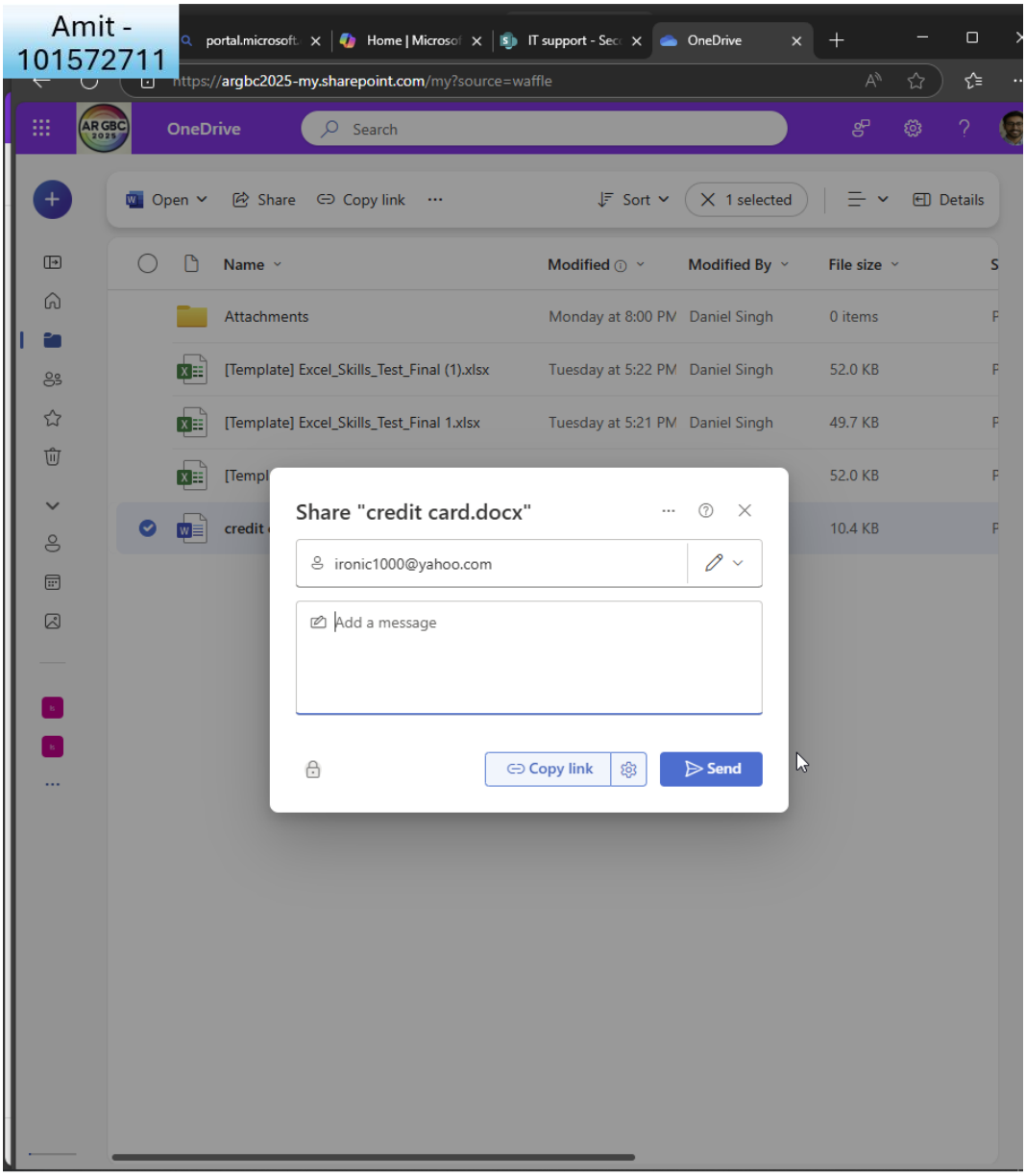
I review and finish

Student Name: ……. Term: ……..
Student ID: ……..



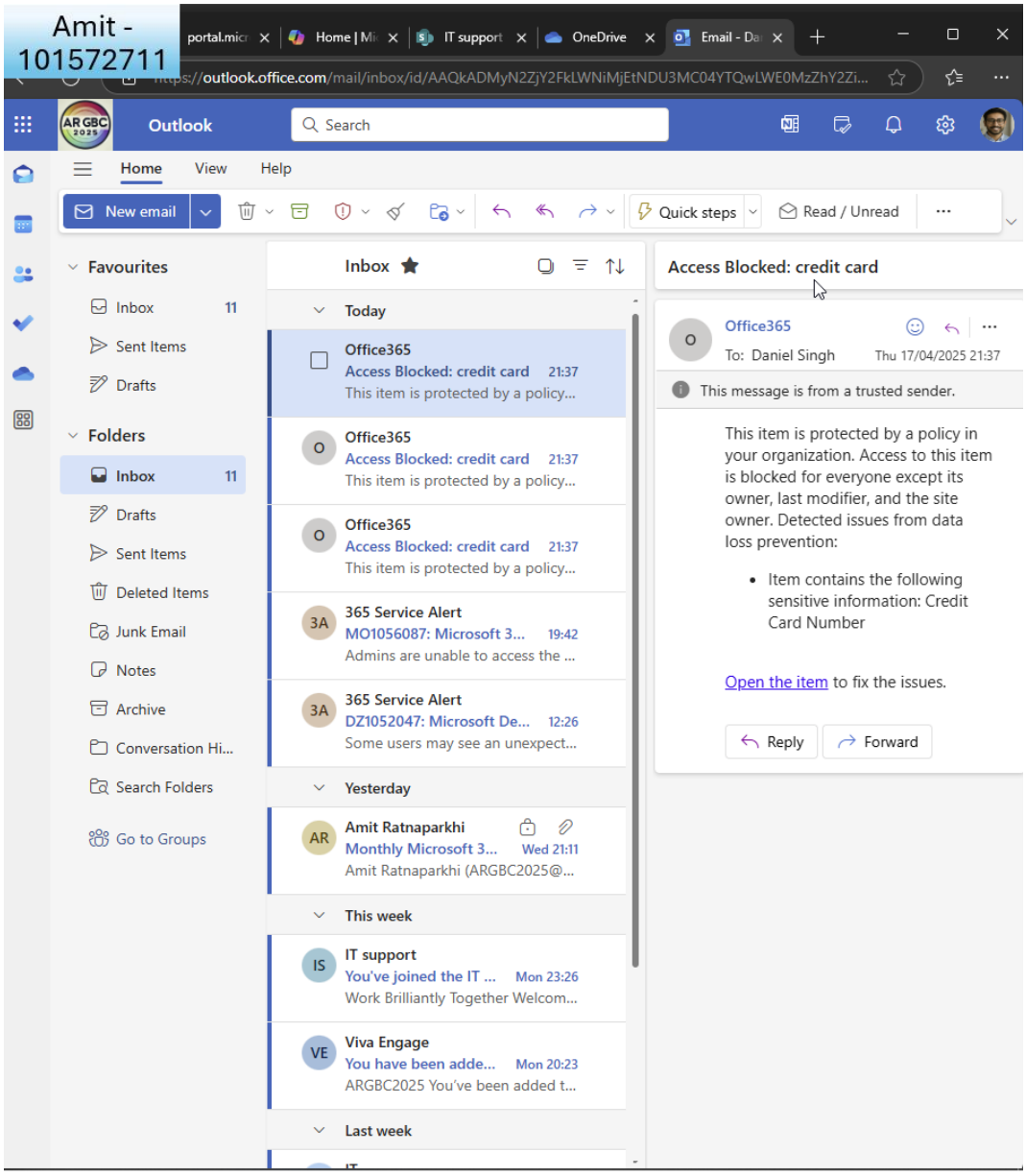
I create a 'dummy' credit card file as user 'Daniel'

Student Name: ……. Term: ……..
Student ID: ……..



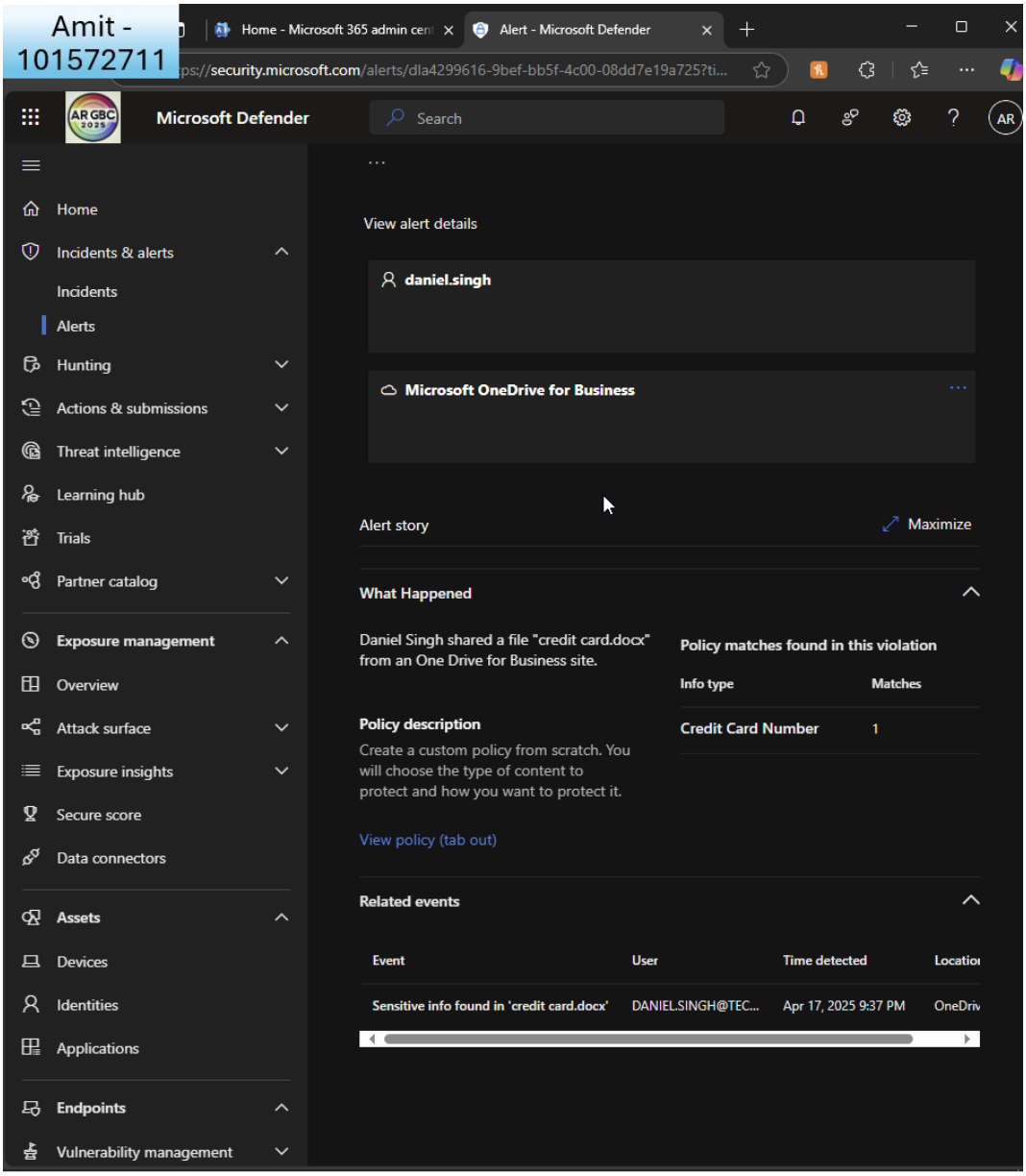
I share it externally

Student Name: ……. Term: ……..
Student ID: ……..



I receive a notification as Daniel

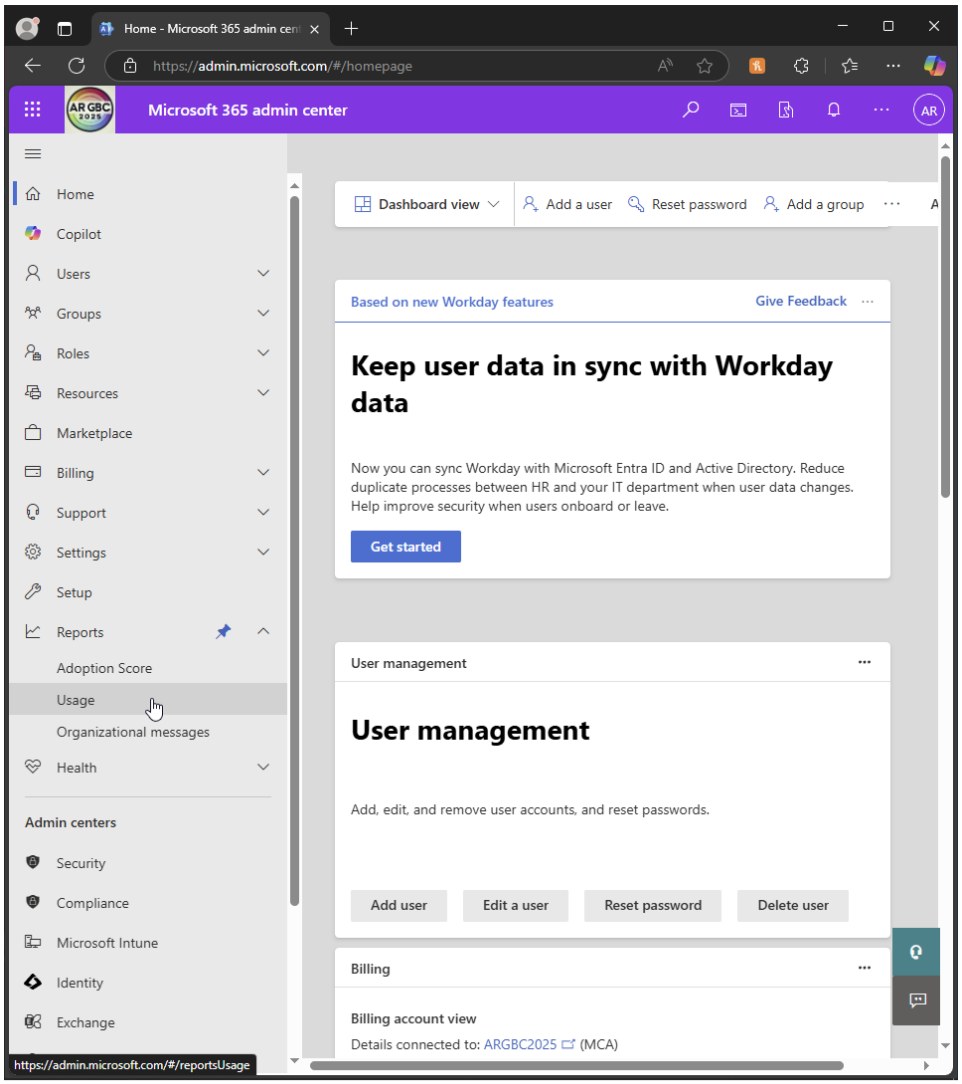
Student Name: ……. Term: ……..
Student ID: ……..



And I can see the alert in Defender

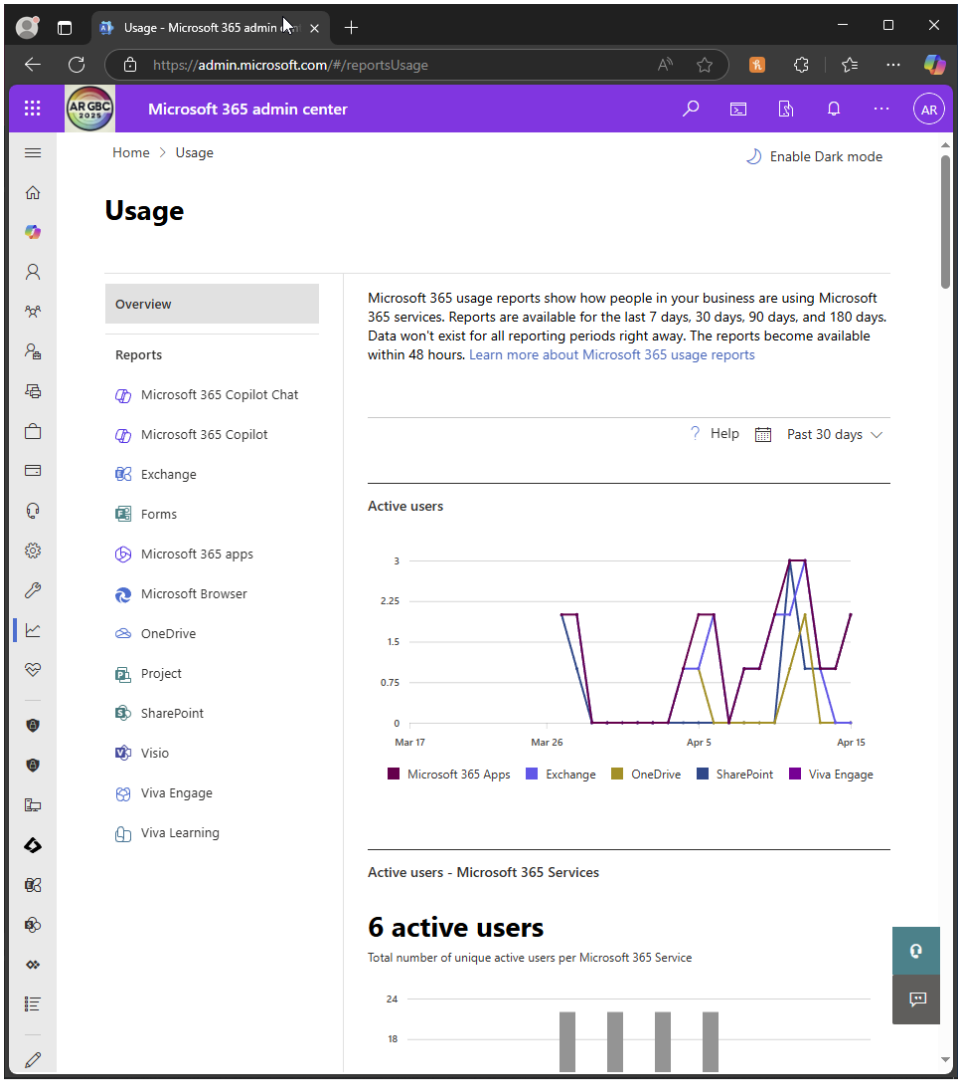
Student Name: ……. Term: ……..
Student ID: ……..

3. **Generate Usage Reports**:
    - Use the Microsoft 365 admin center to generate reports on user activity, email usage, and SharePoint site usage.



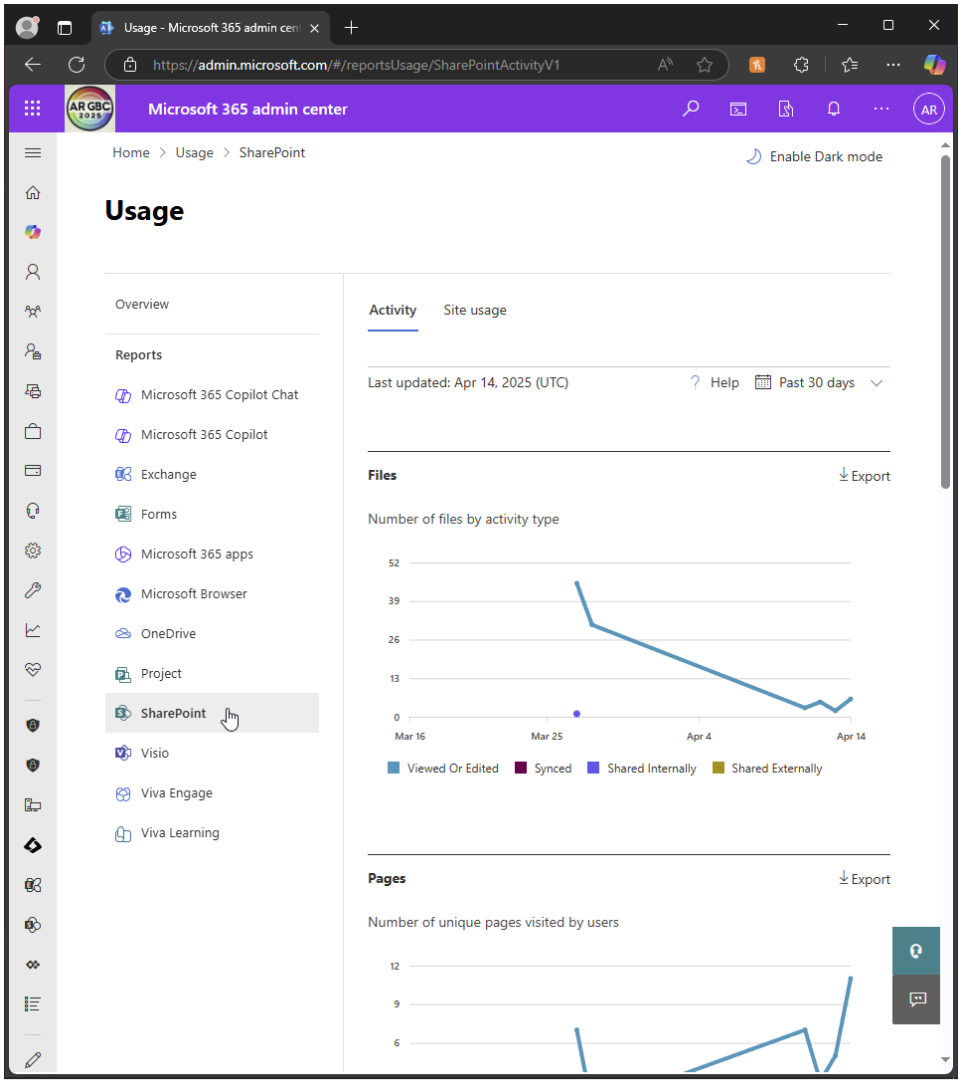
In admin centre, I go to ’reports - usage’

Student Name: ……. Term: ……..
Student ID: ……..



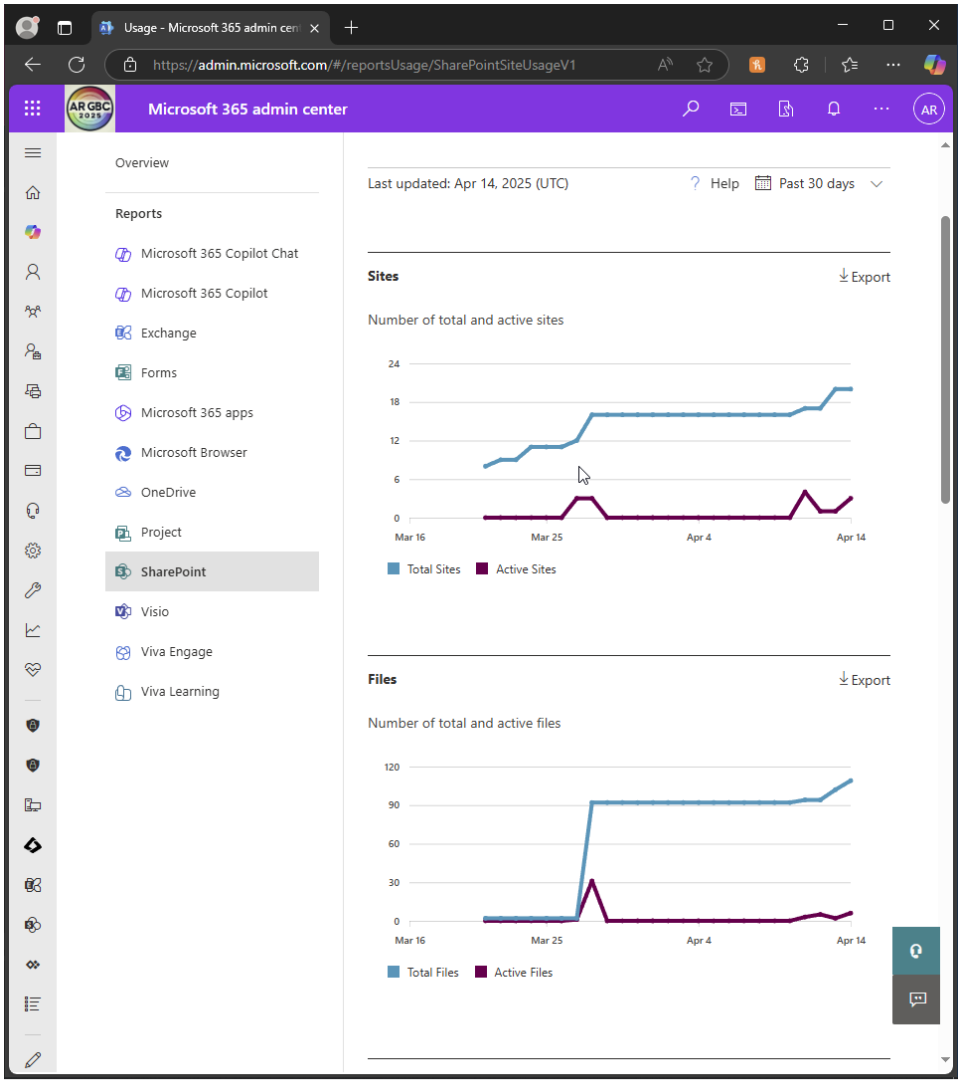
I can see reports such as active users

Student Name: ……. Term: ……..
Student ID: ……..



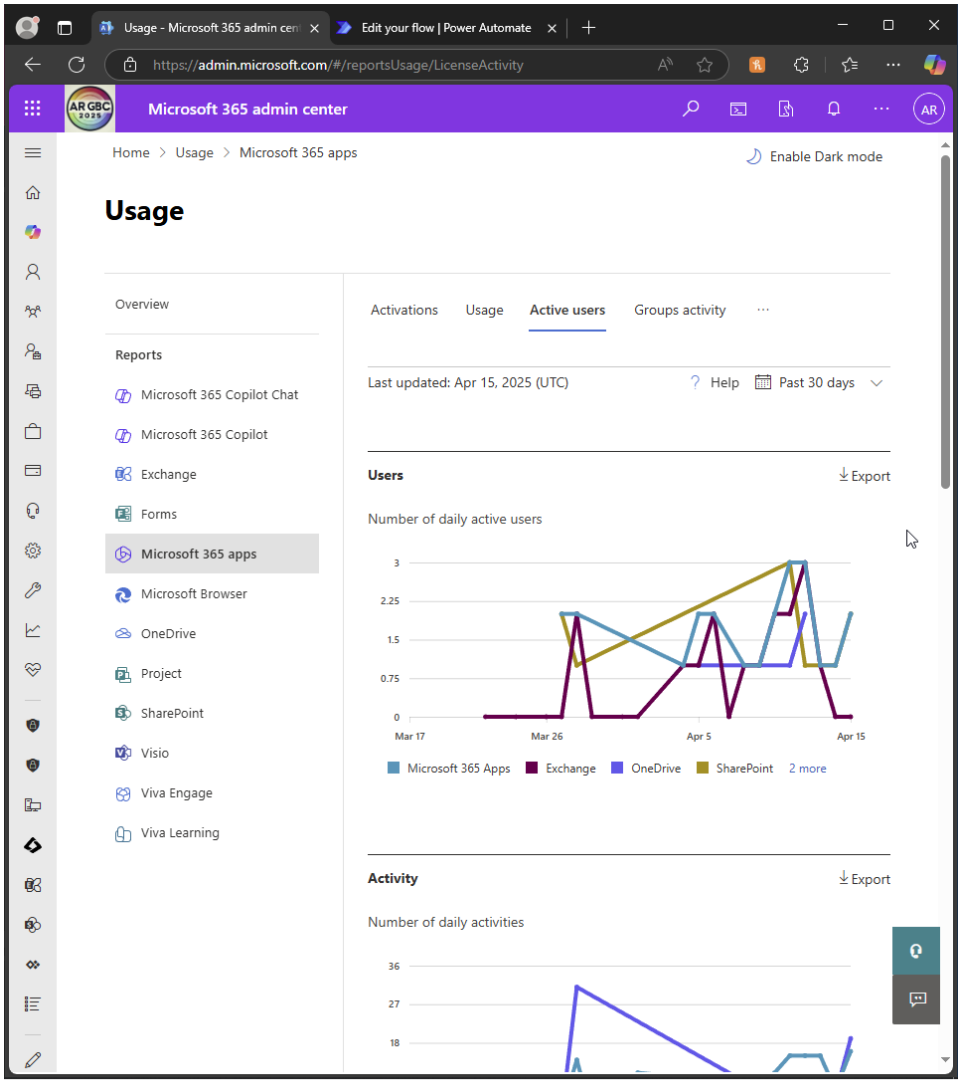
Sharepoint activity i.e. files

Student Name: ……. Term: ……..
Student ID: ……..



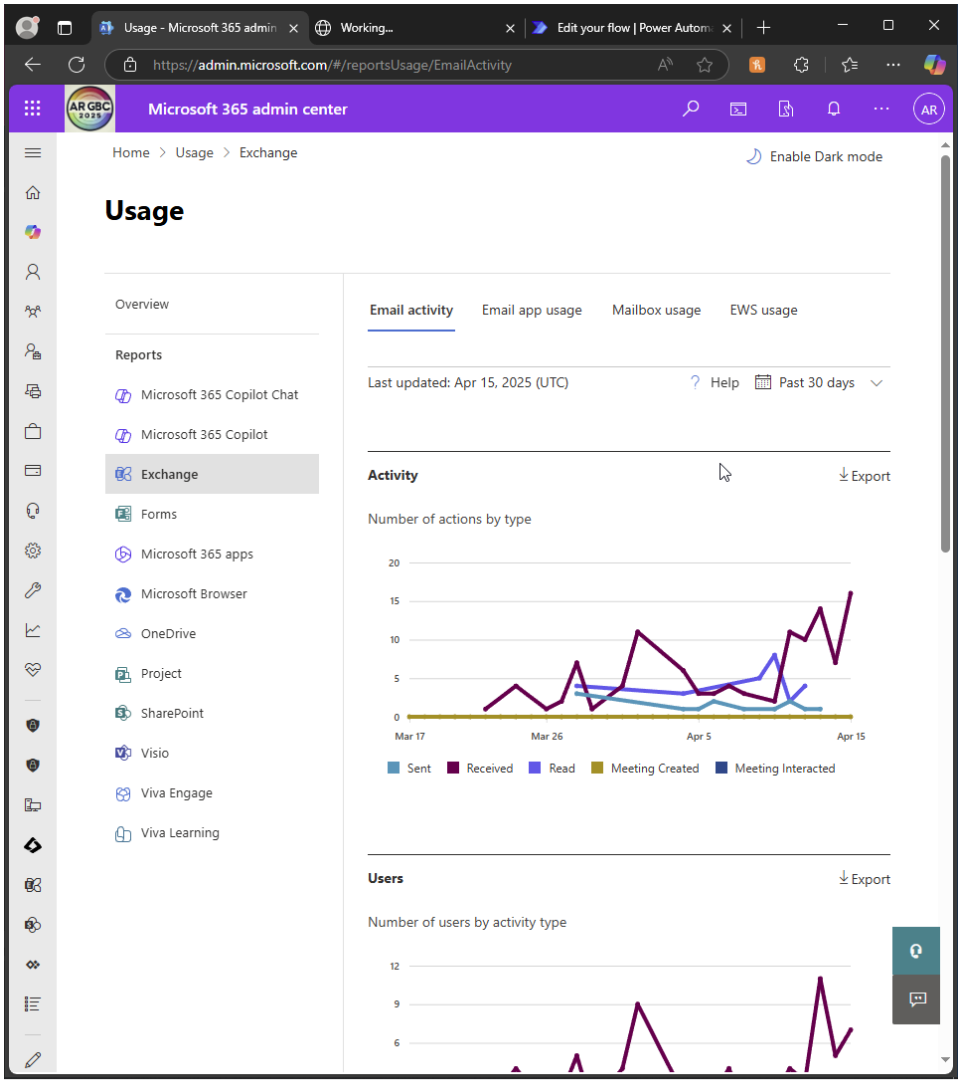
Sharepoint active sites

Student Name: ……. Term: …….
Student ID: …….



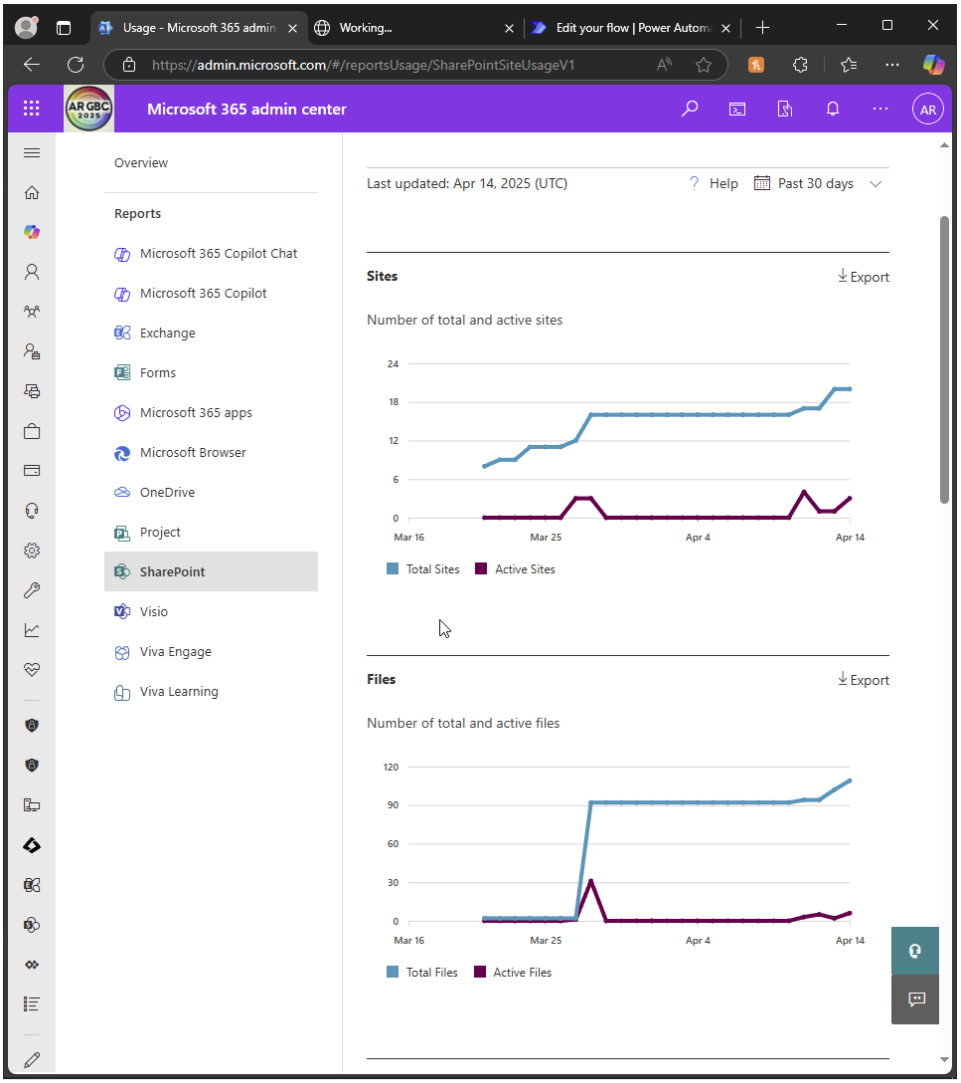
Active users

Student Name: ……. Term: ……..
Student ID: ……..



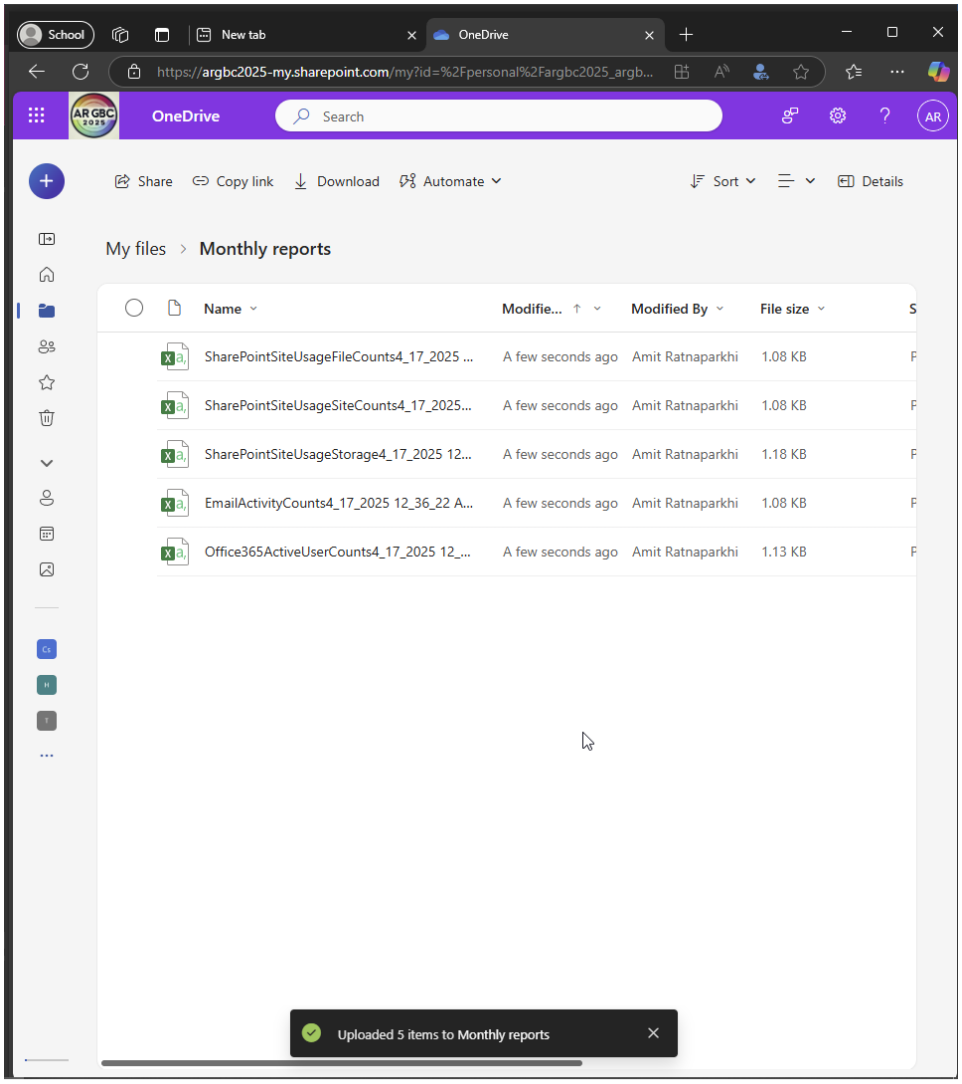
Email activity

Student Name: ……. Term: …….
Student ID: …….



Sharepoint sites and files. Click export to export all of them as CSV files

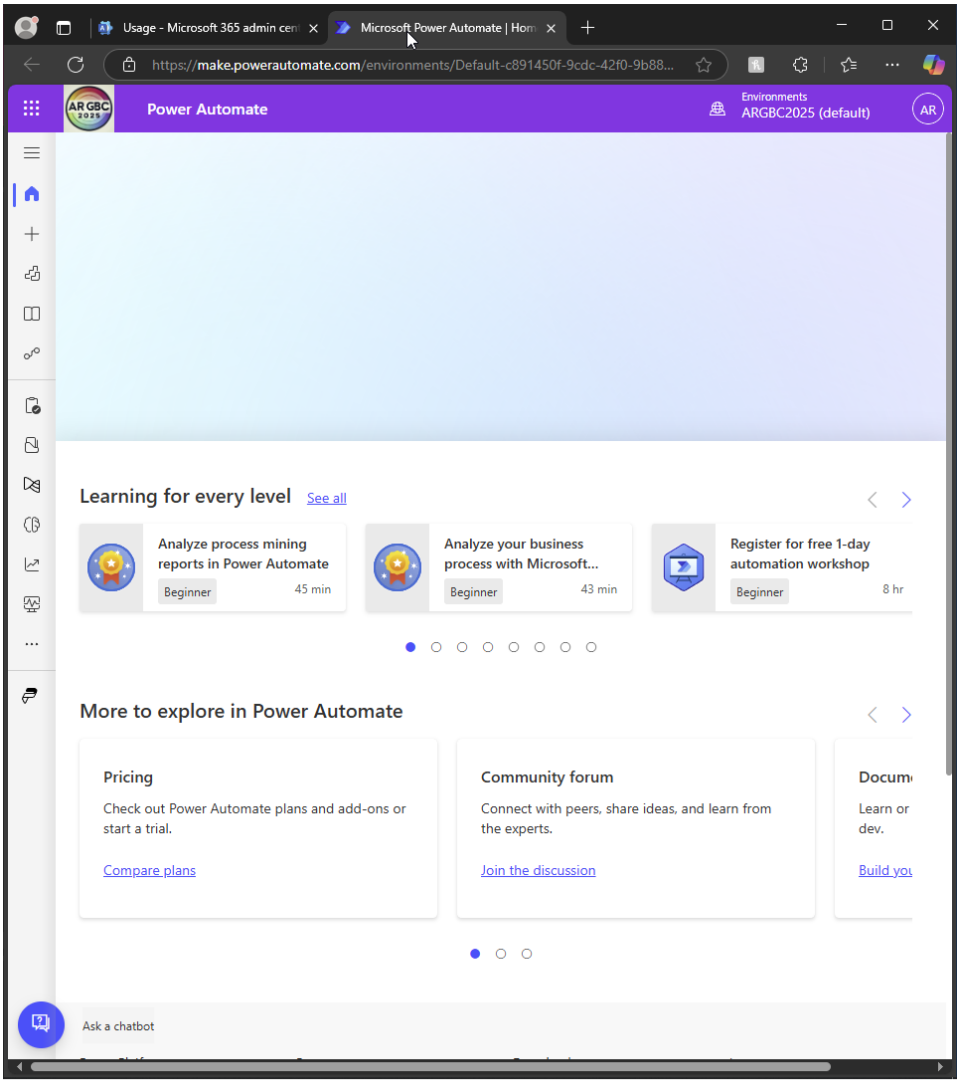
Student Name: ……. Term: ……..
Student ID: ……..



I upload them to onedrive 'monthly reports' folder

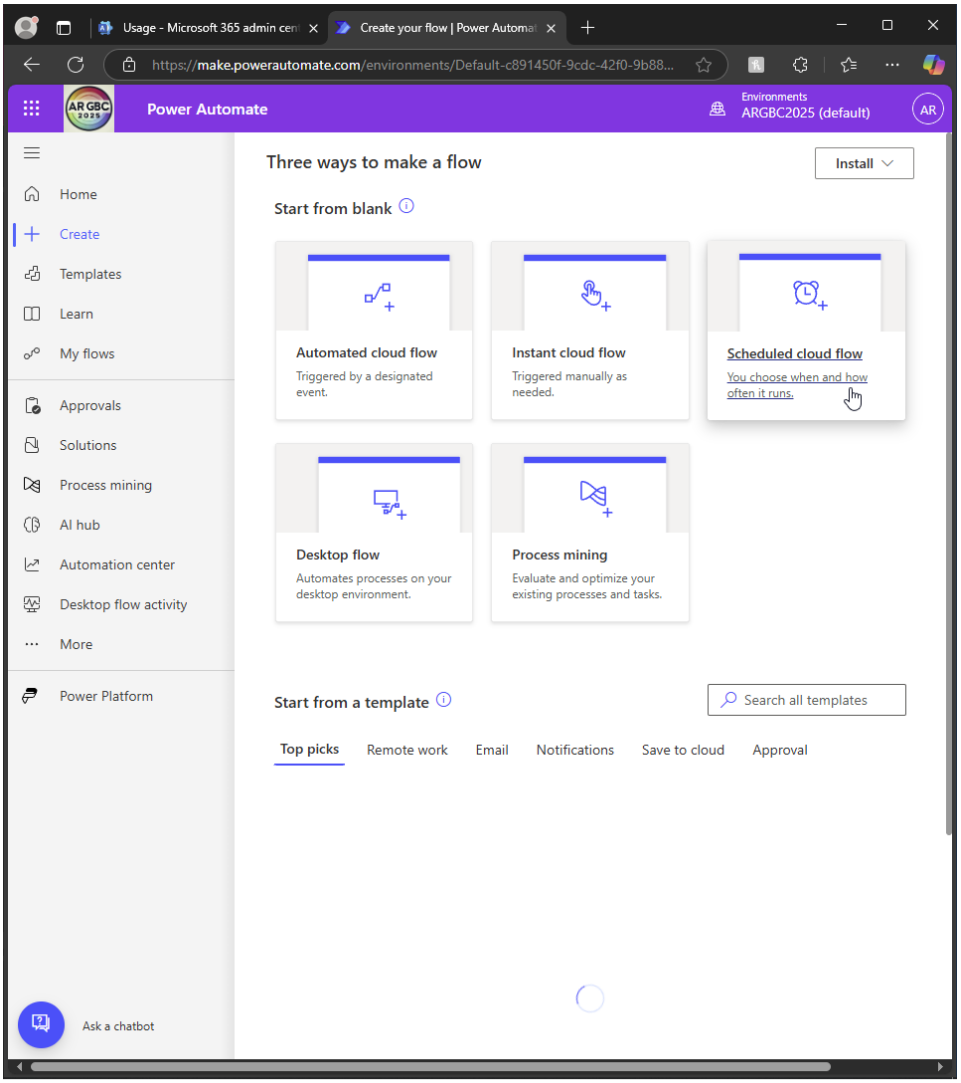
- Schedule monthly reports to be sent to IT administrators and department heads.(Optional, you can use Power Automate)

Student Name: ……. Term: ……..
Student ID: ……..



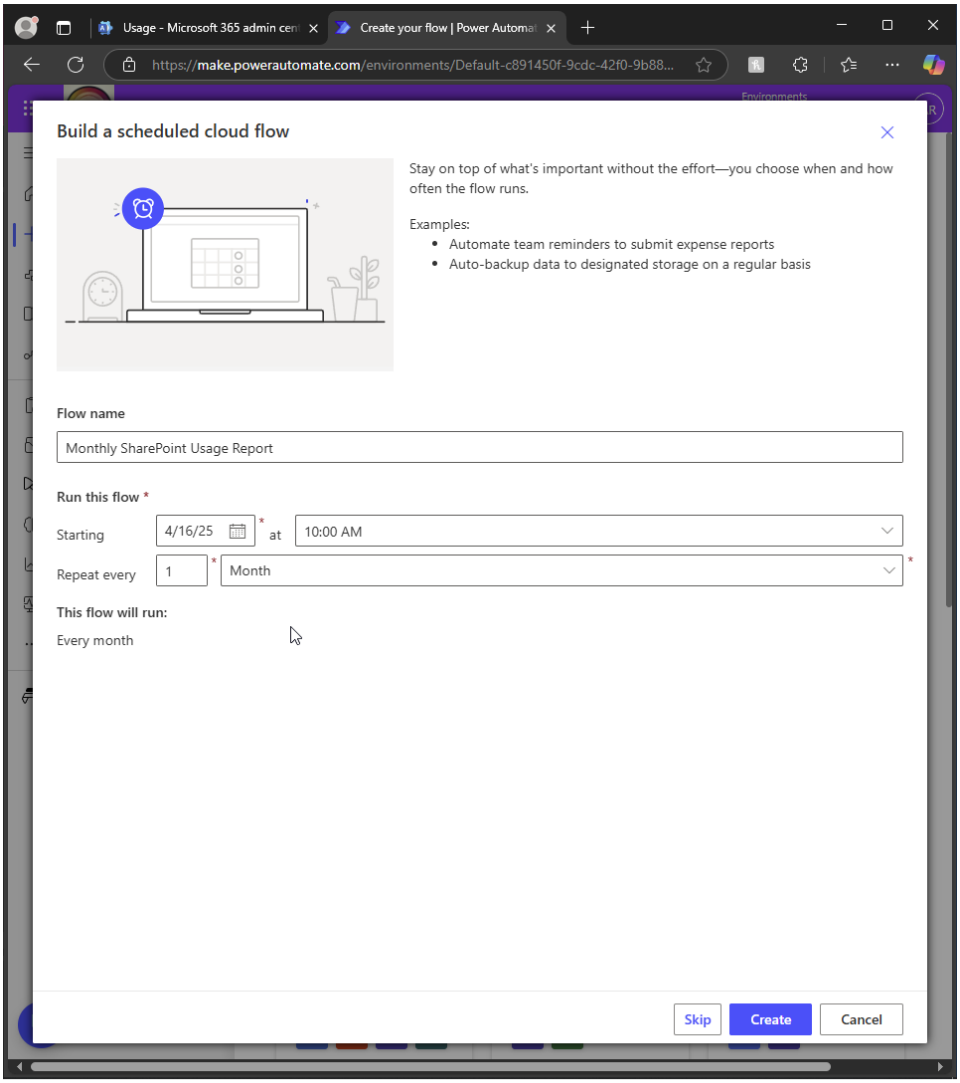
I choose to use Power Automate so I open it up

Student Name: ……. Term: ……..
Student ID: ……..



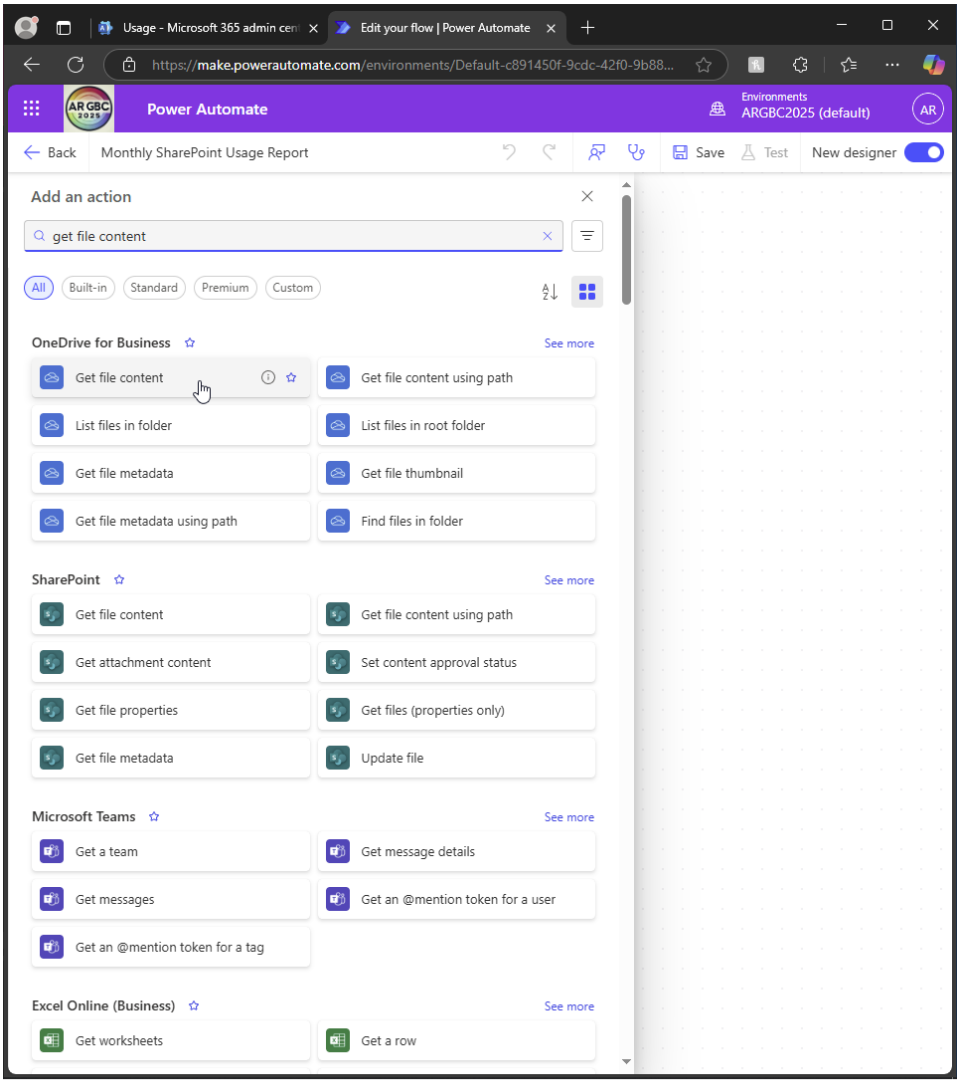
I click ’create’

Student Name: ……. Term: ……..
Student ID: ……..



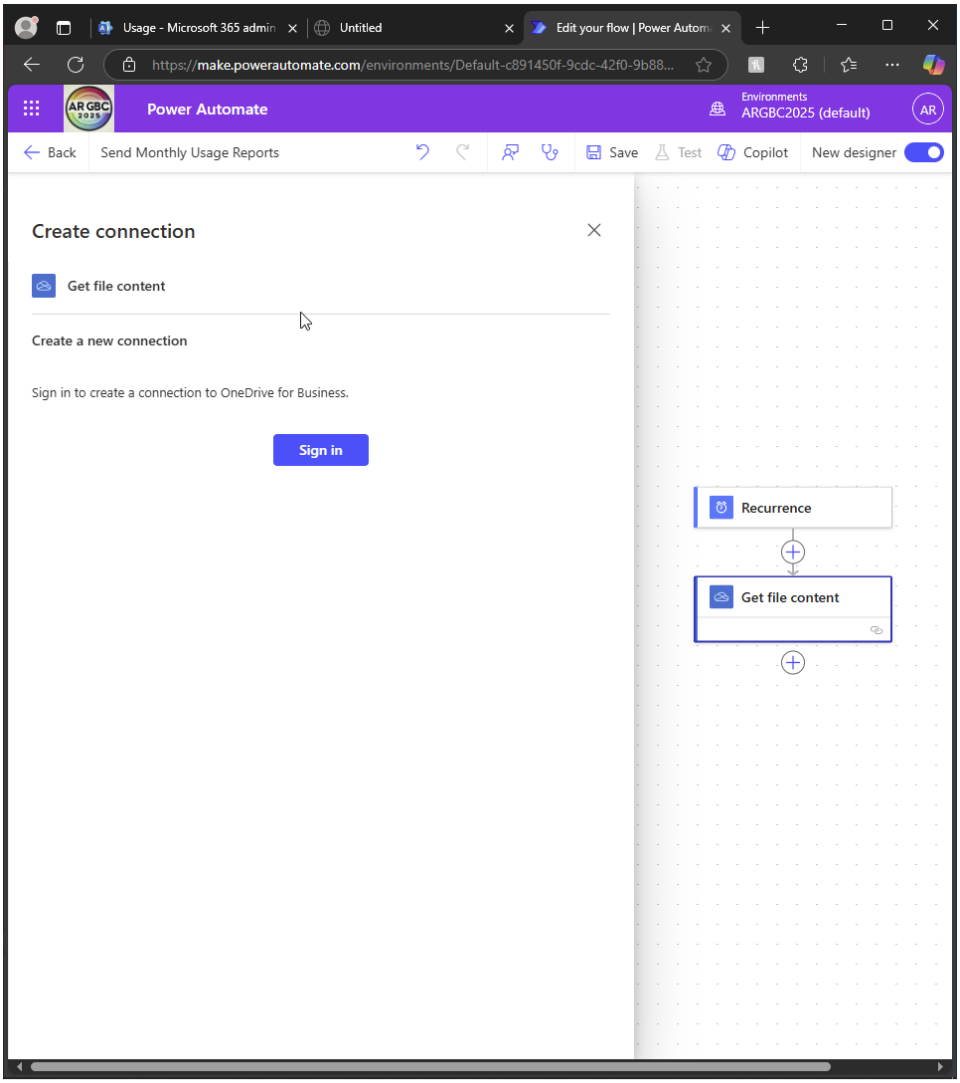
I name my flow and make it monthly

Student Name: ……. Term: ……..
Student ID: ……..



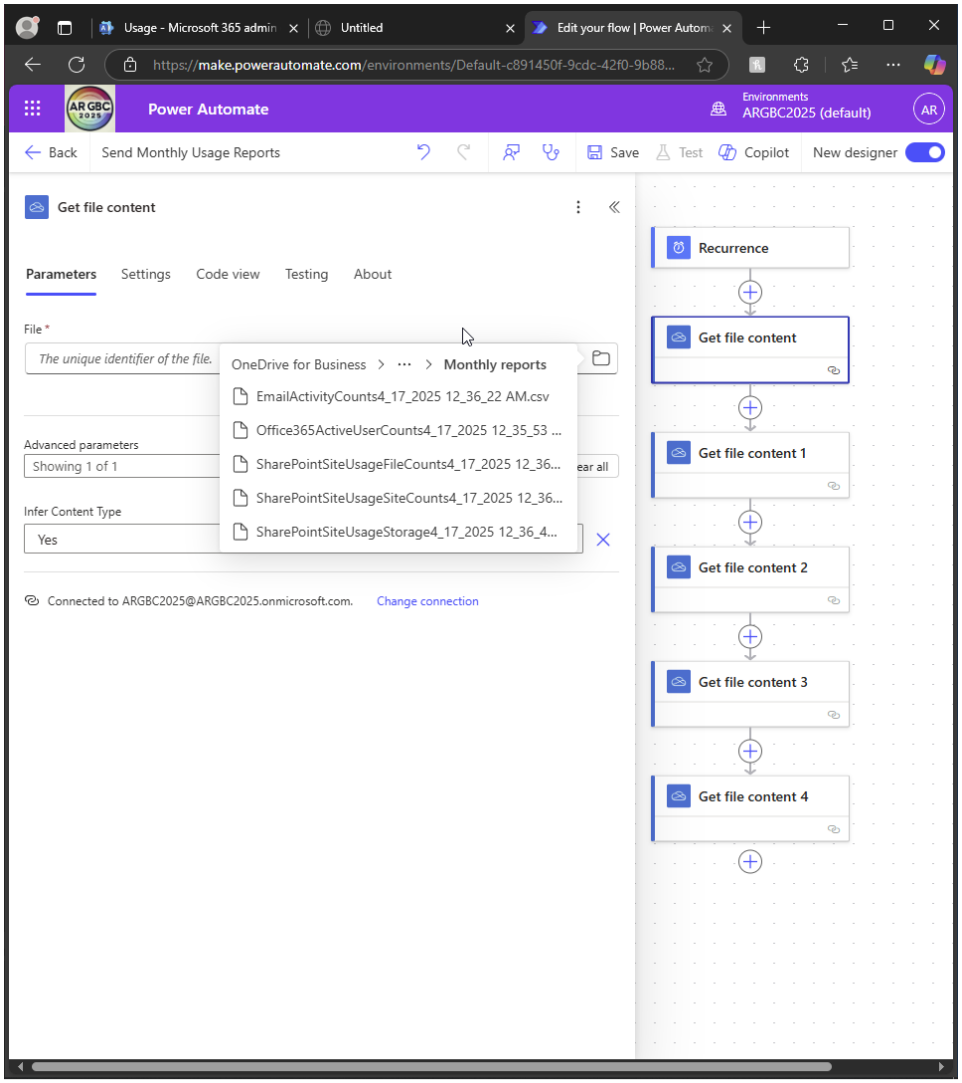
I choose to get file content from onedrive (the place I stored the CSVs)

Student Name: ……. Term: ……..
Student ID: ……..



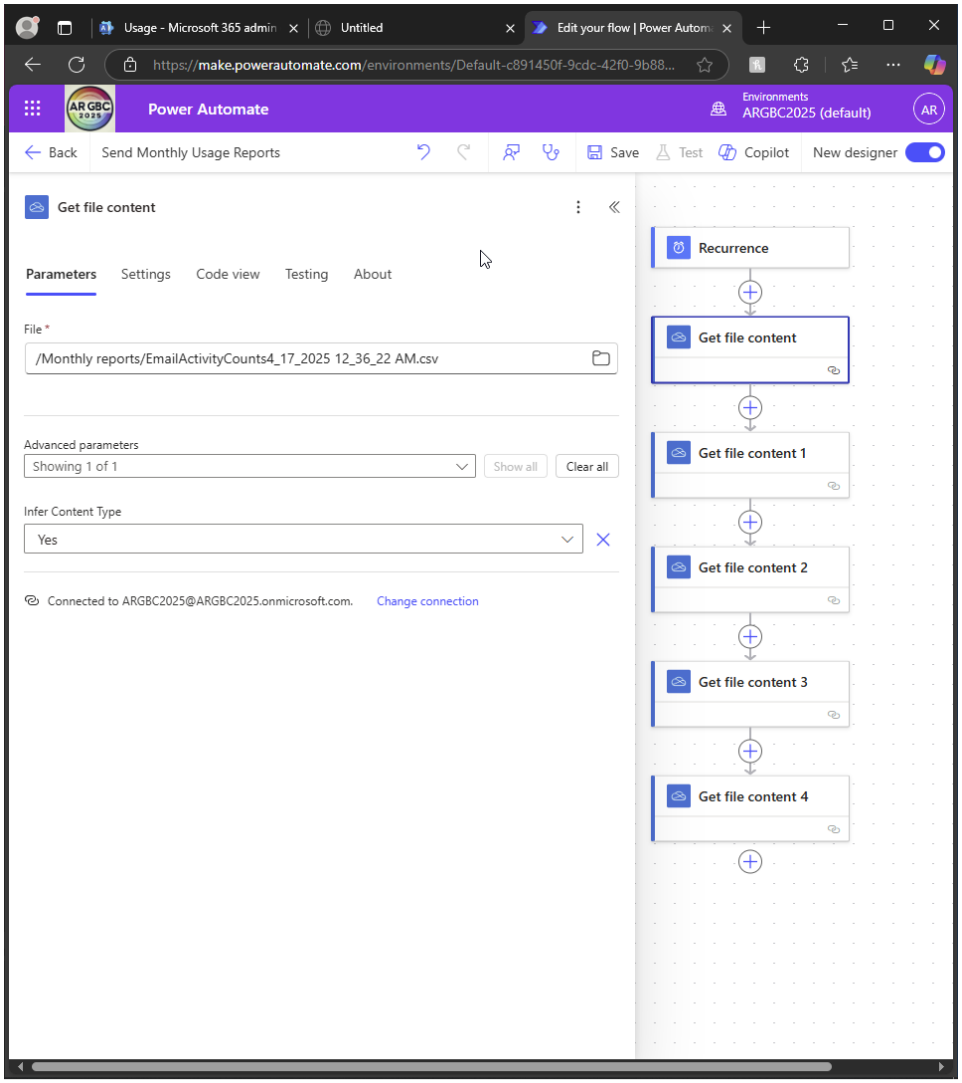
I create the connection with ondrive

Student Name: ……. Term: ……..
Student ID: ……..



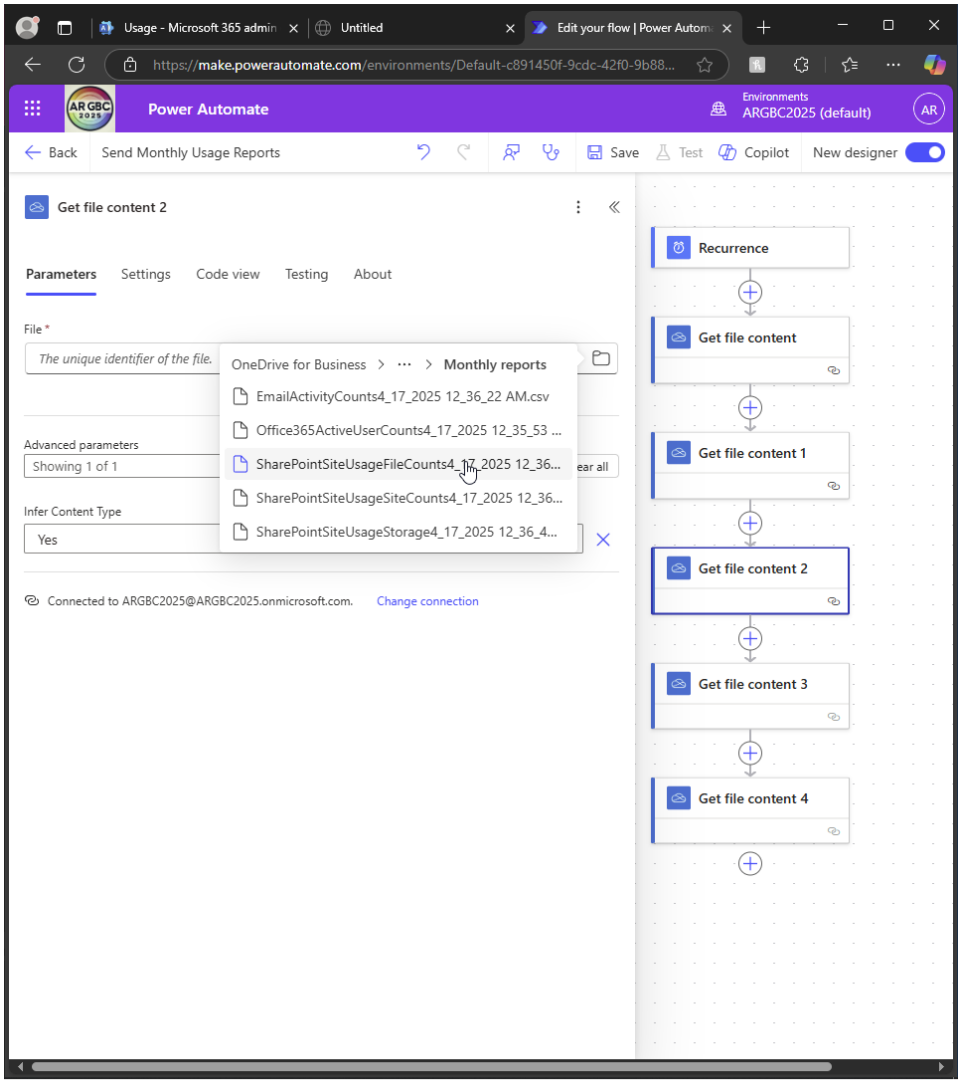
I repeat the process of getting file content so it gets content from all 5 CSV files

Student Name: ……. Term: …….
Student ID: …….



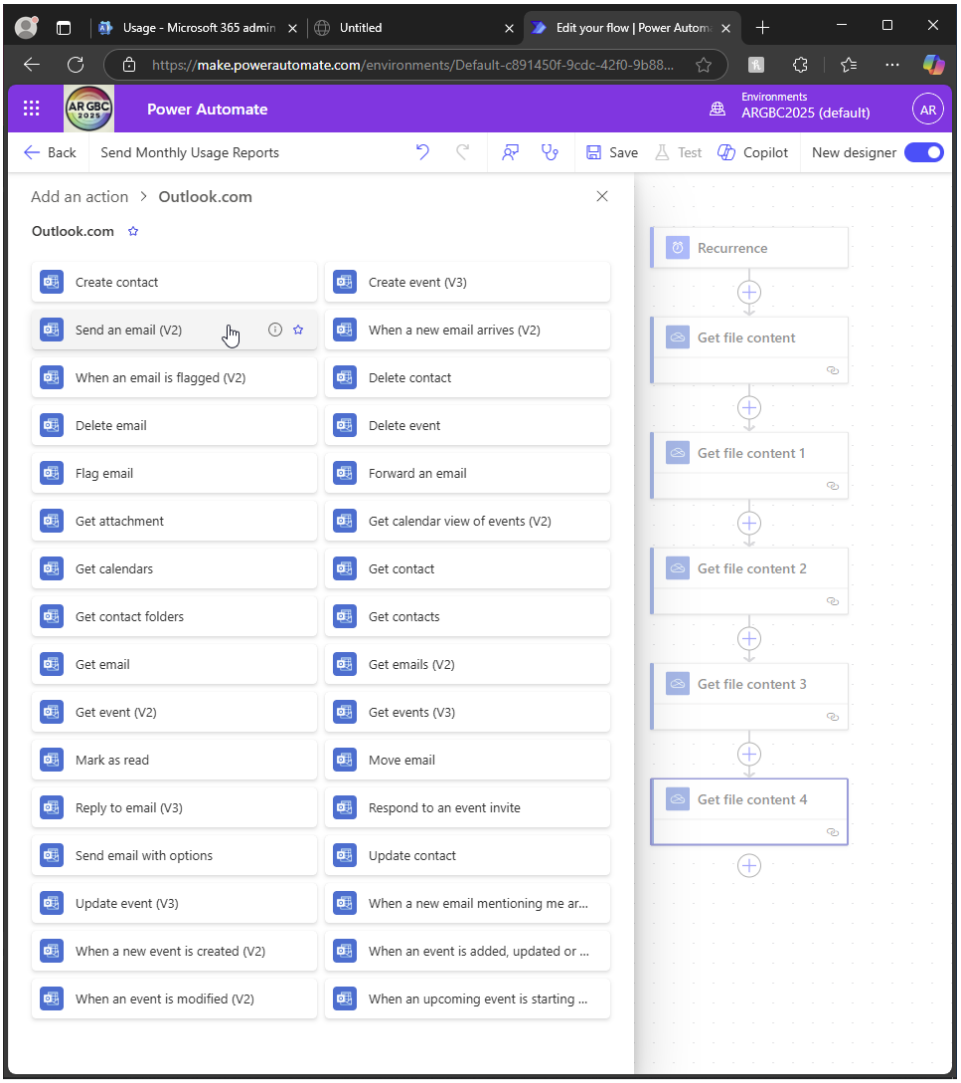
I specify the file

Student Name: ……. Term: ……..
Student ID: ……..



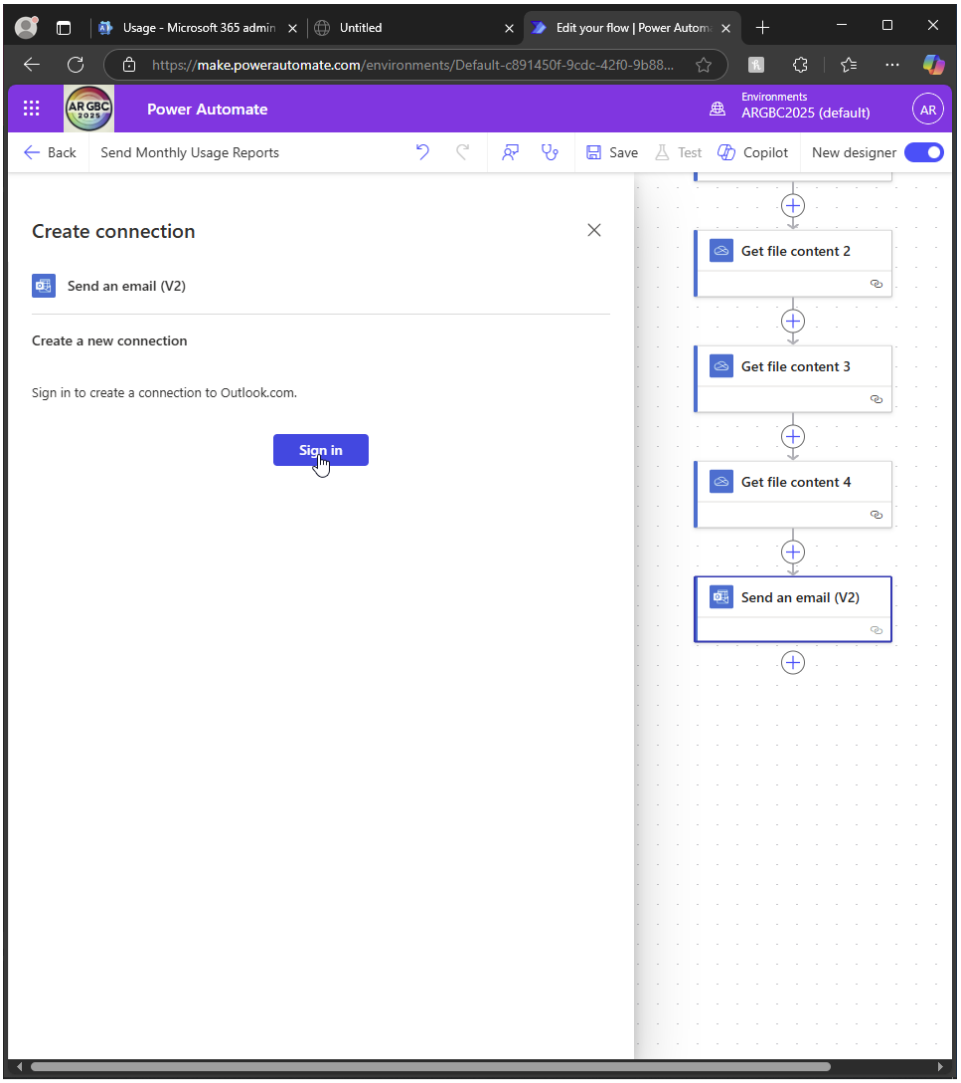
And repeat for each file content flow box

Student Name: ……. Term: ……..
Student ID: ……..



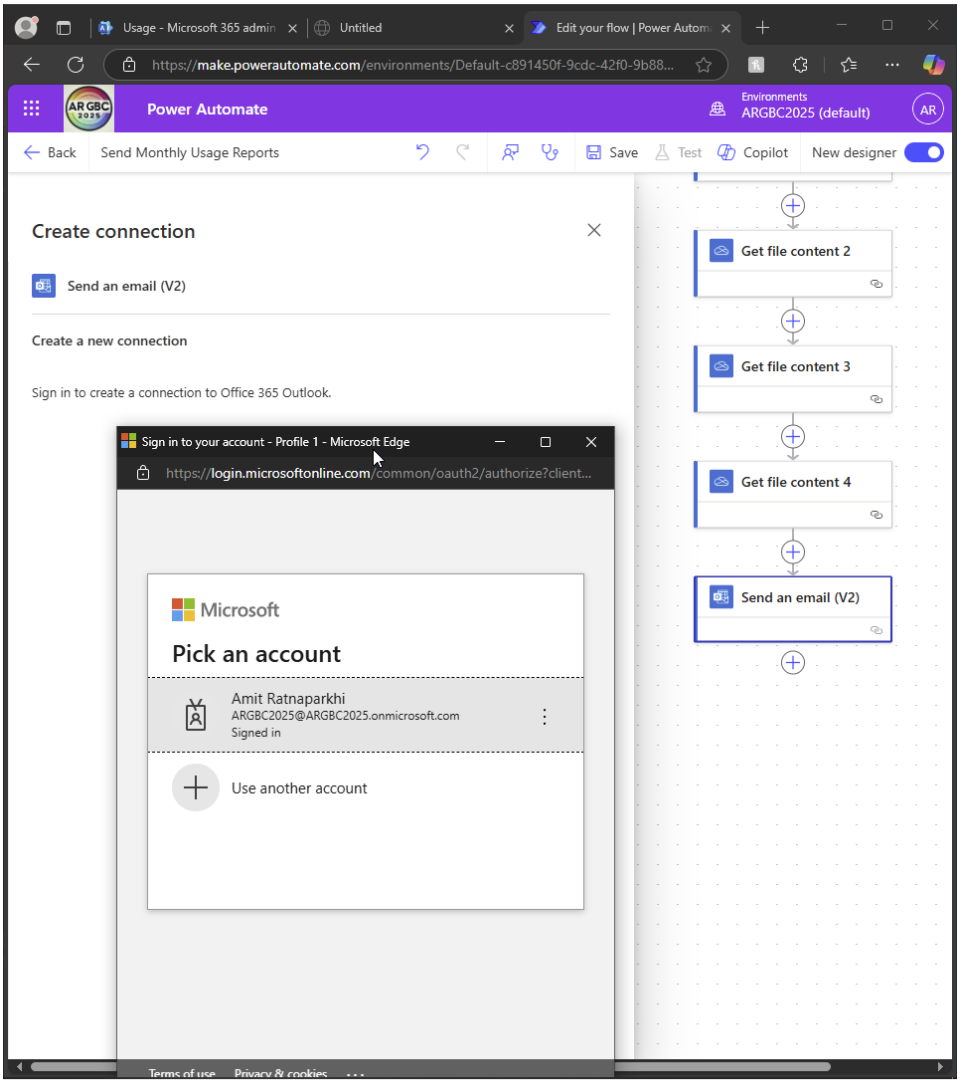
I add an action after ’get file content 4’ flow box to send an email

Student Name: ……. Term: ……..
Student ID: ……..



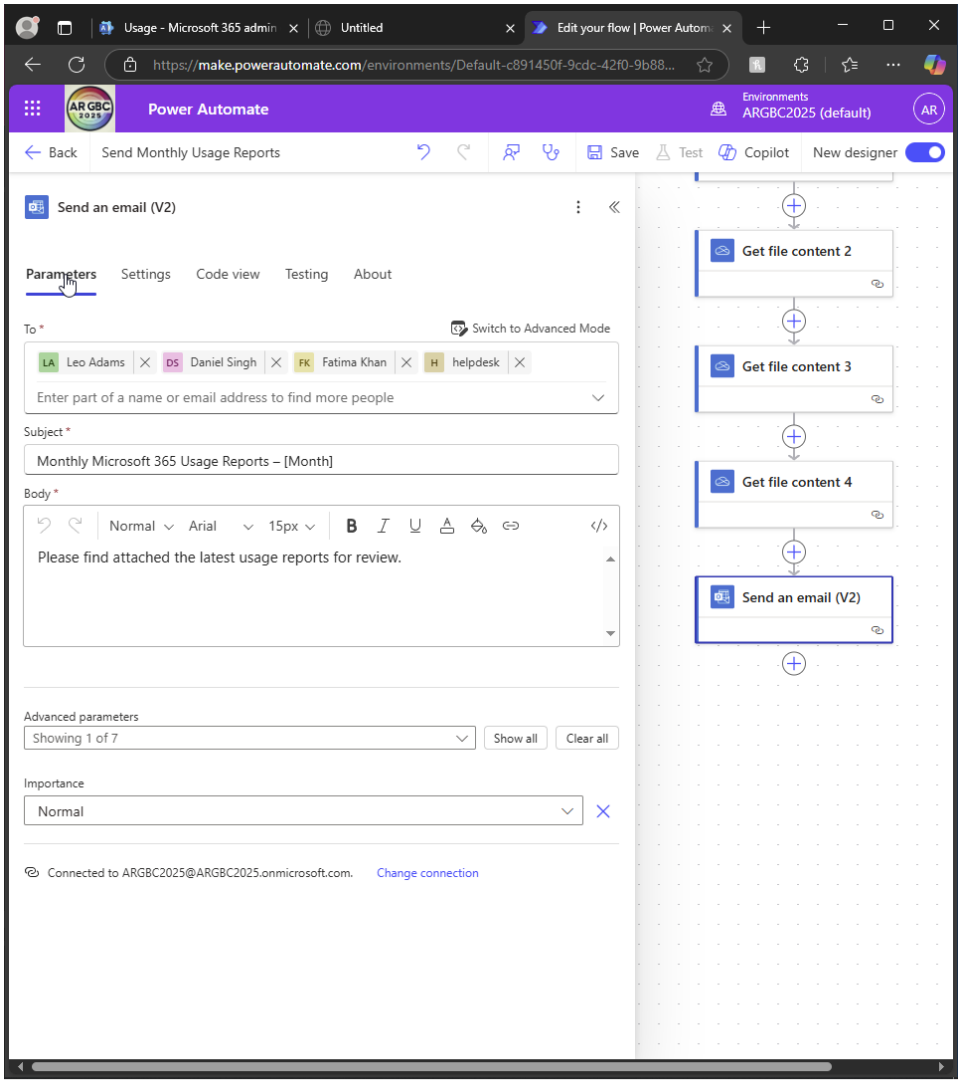
I create the connection to Outlook

Student Name: ……. Term: …….
Student ID: …….



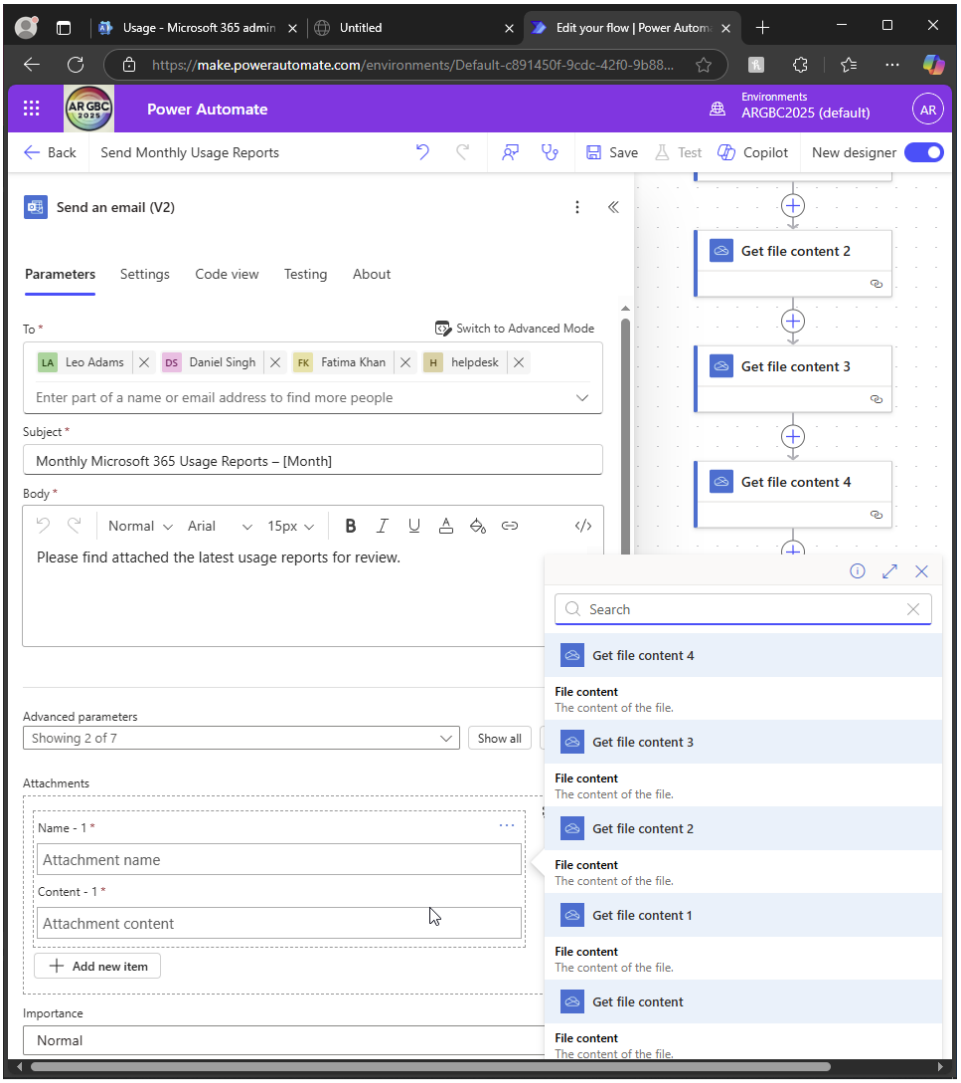
I sign in as GA

Student Name: ……. Term: ……..
Student ID: ……..



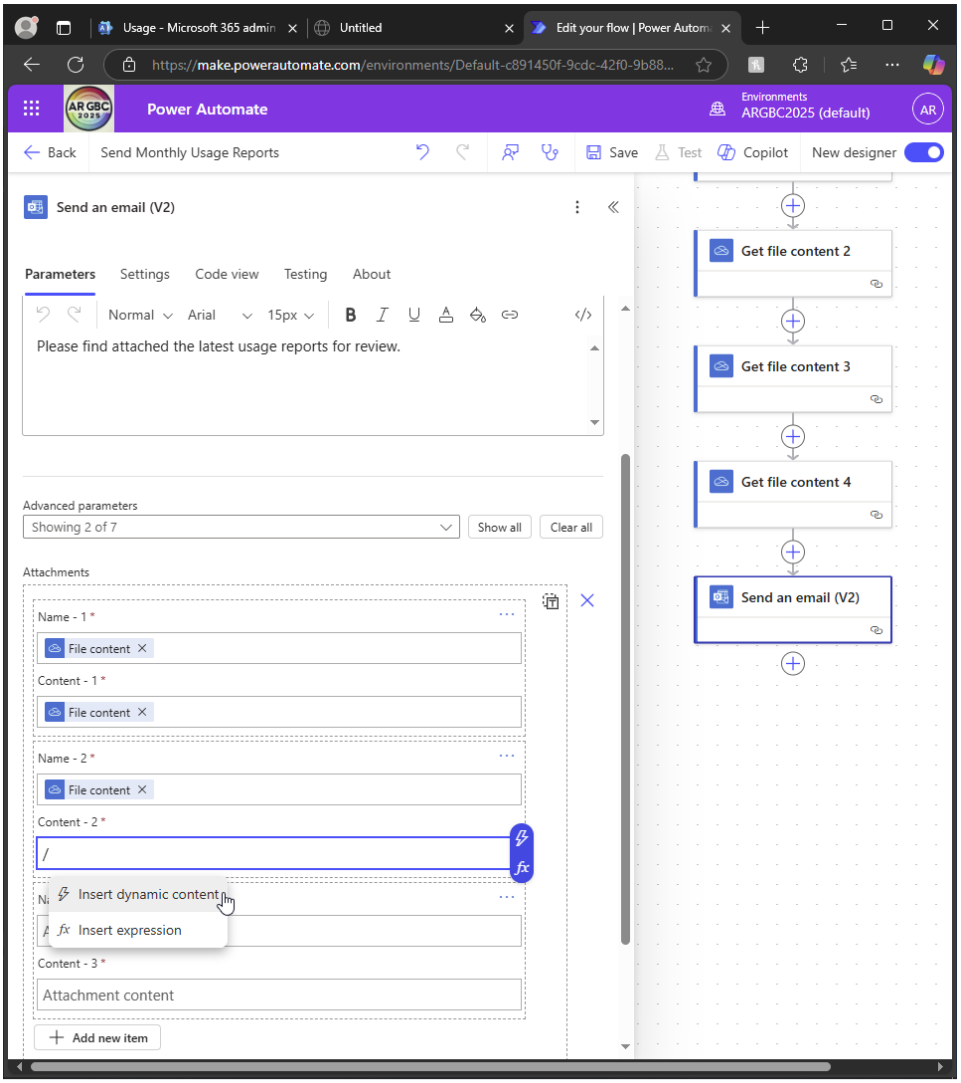
I choose to send the mail to IT departments and department heads

Student Name: ……. Term: …….
Student ID: …….



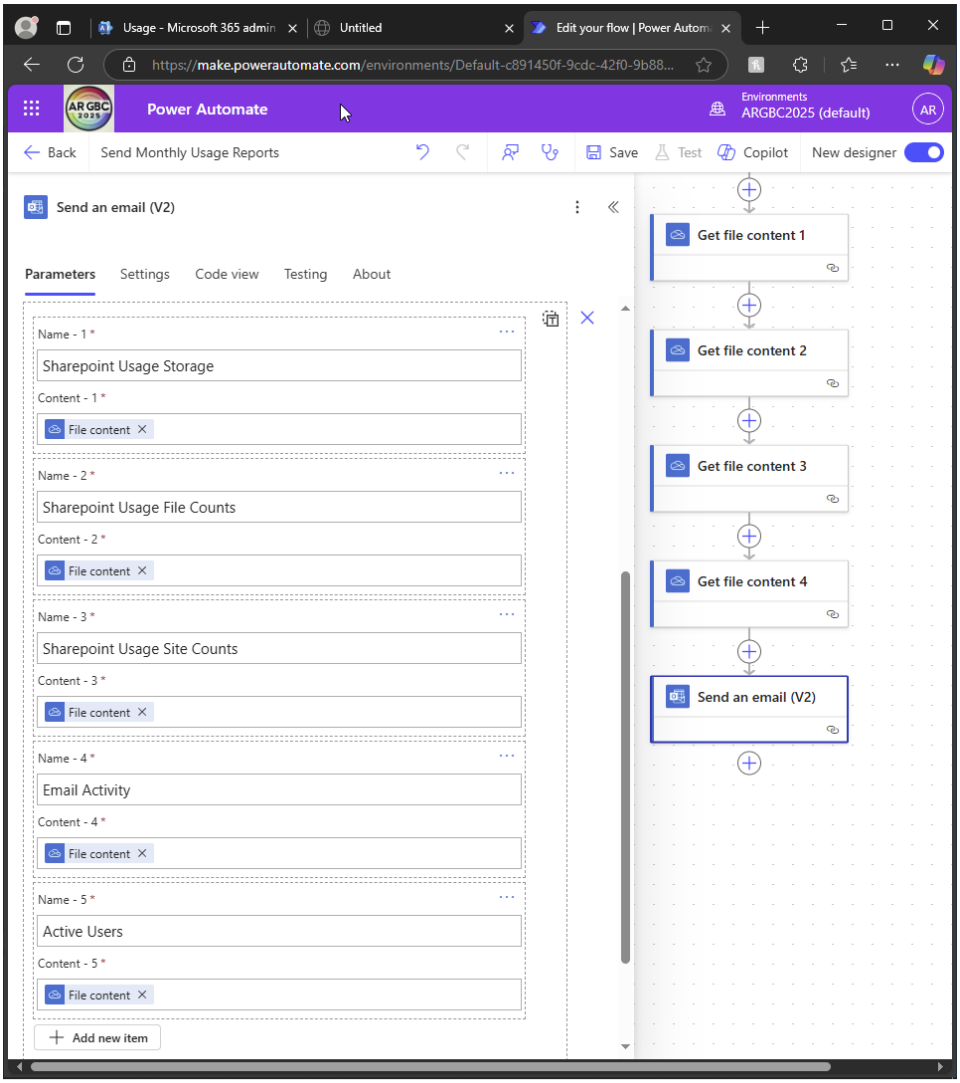
I dynamically attach each file contents

Student Name: ……. Term: ……..
Student ID: ……..



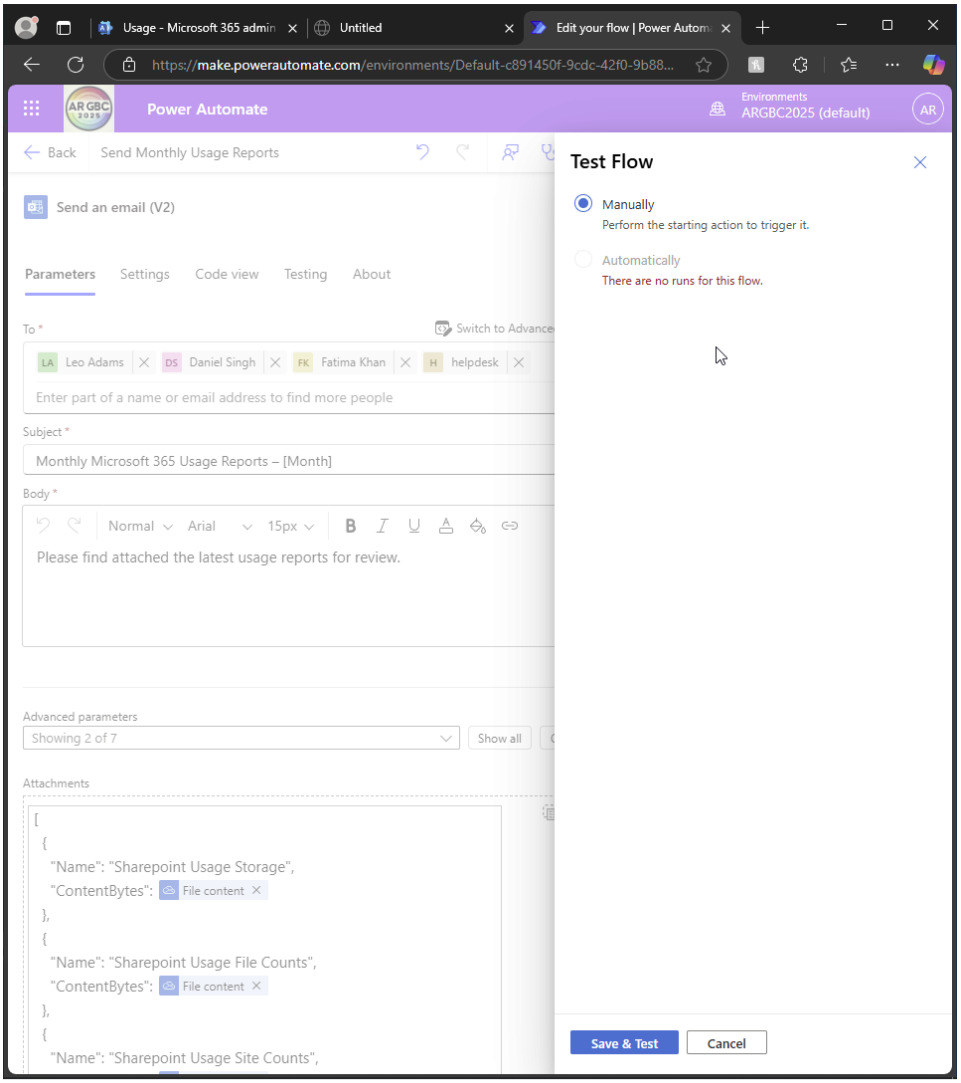
5 times, for each CSV

Student Name: ……. Term: ……..
Student ID: ……..



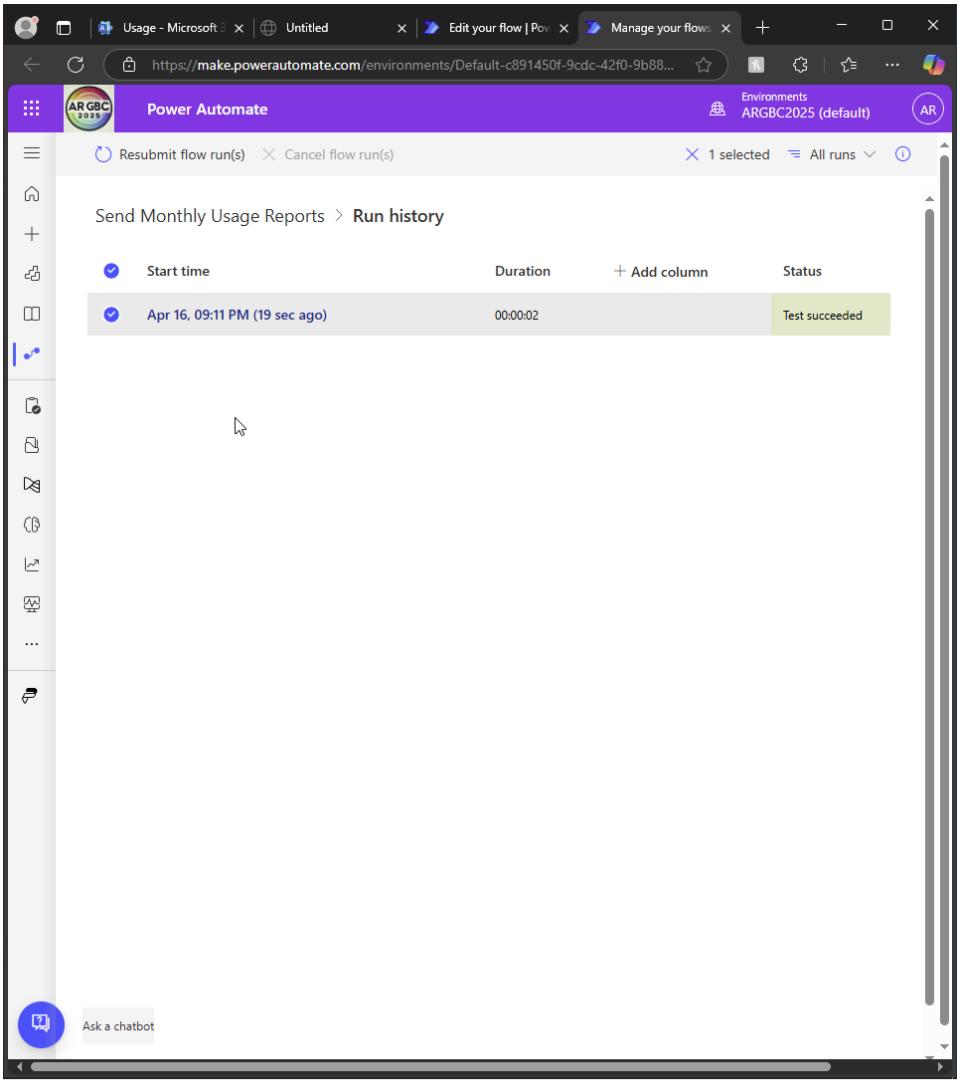
I give meaningful names to each file

Student Name: ……. Term: ……..
Student ID: ……..



I save it and test flow

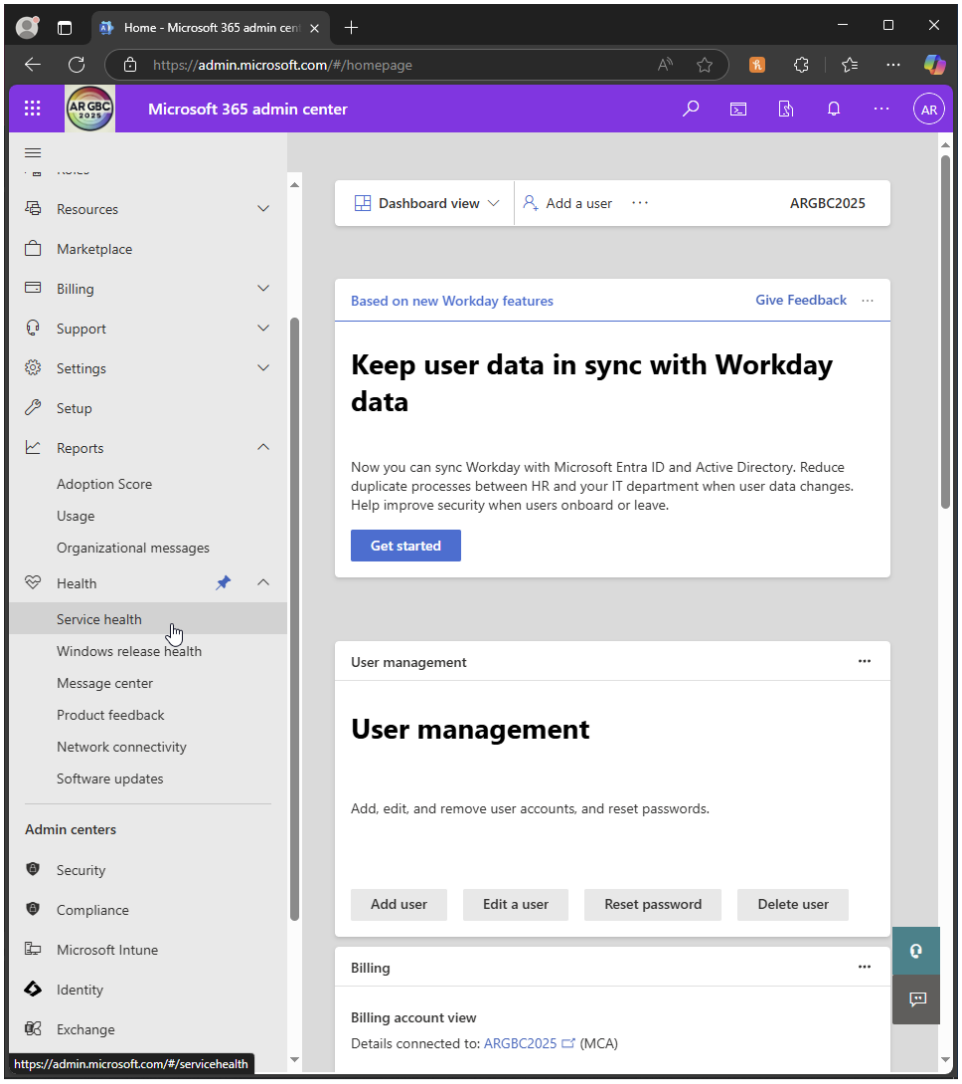
Student Name: ……. Term: ……..
Student ID: ……..



I confirm the test succeeded

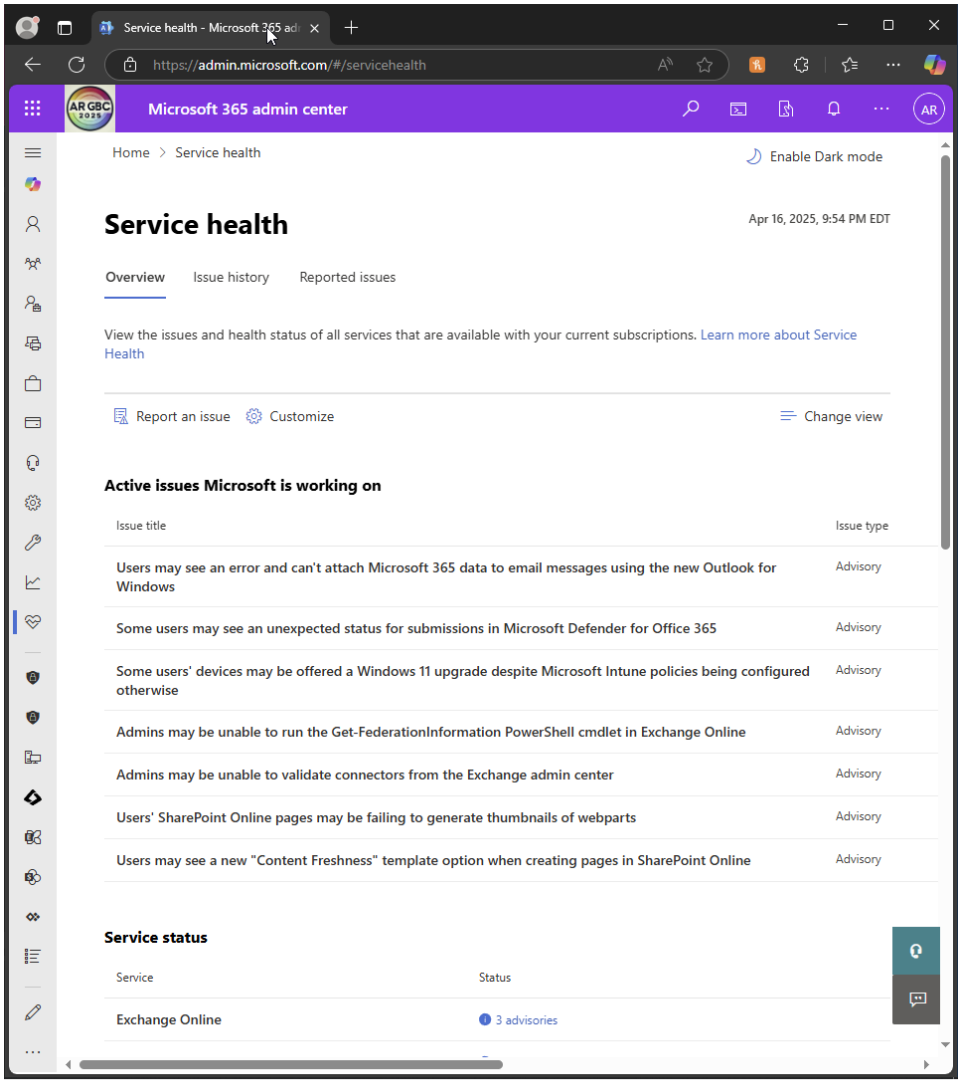
Student Name: ……. Term: ……..
Student ID: ……..

4. **Implement and Monitor Service Health**:
    - Set up service health alerts to notify administrators of any issues with Microsoft 365 services.



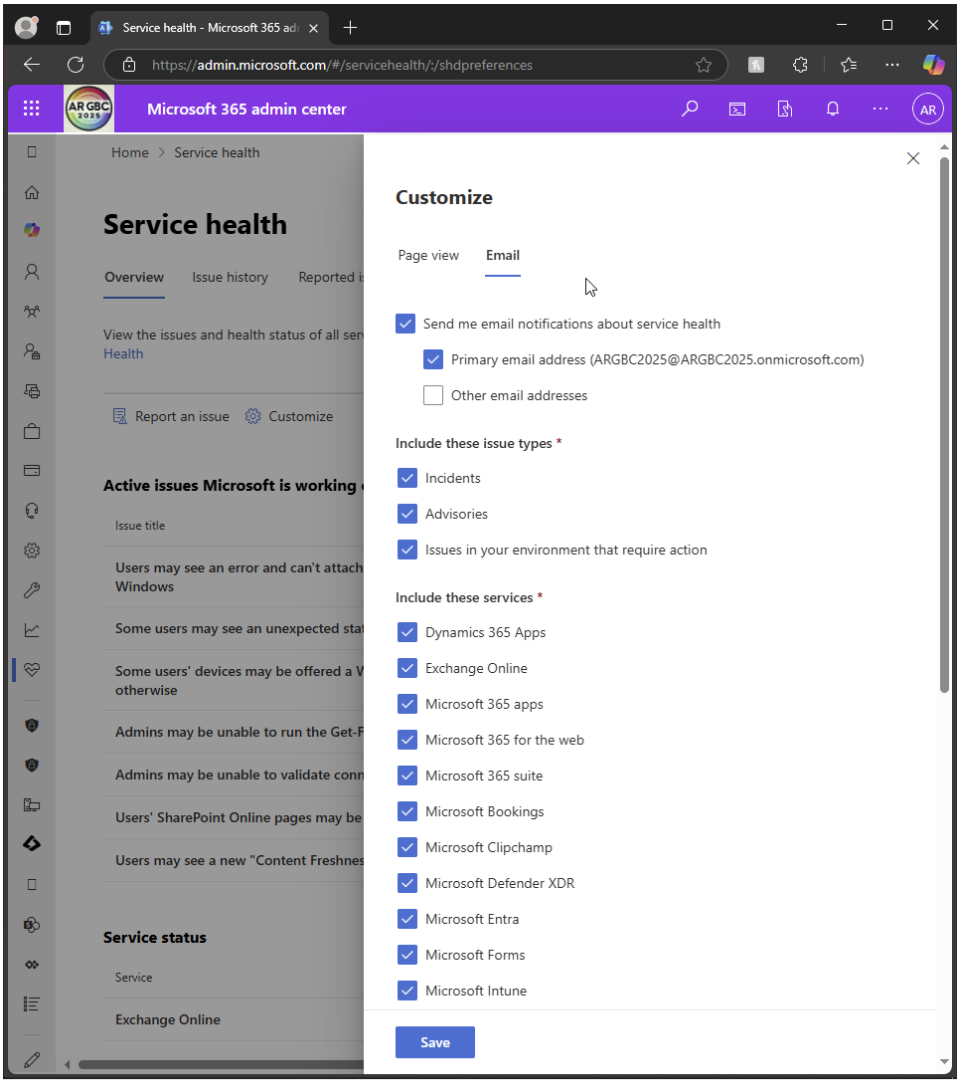
I go to admin centre - health - service health

Student Name: ……. Term: ……..
Student ID: ……..



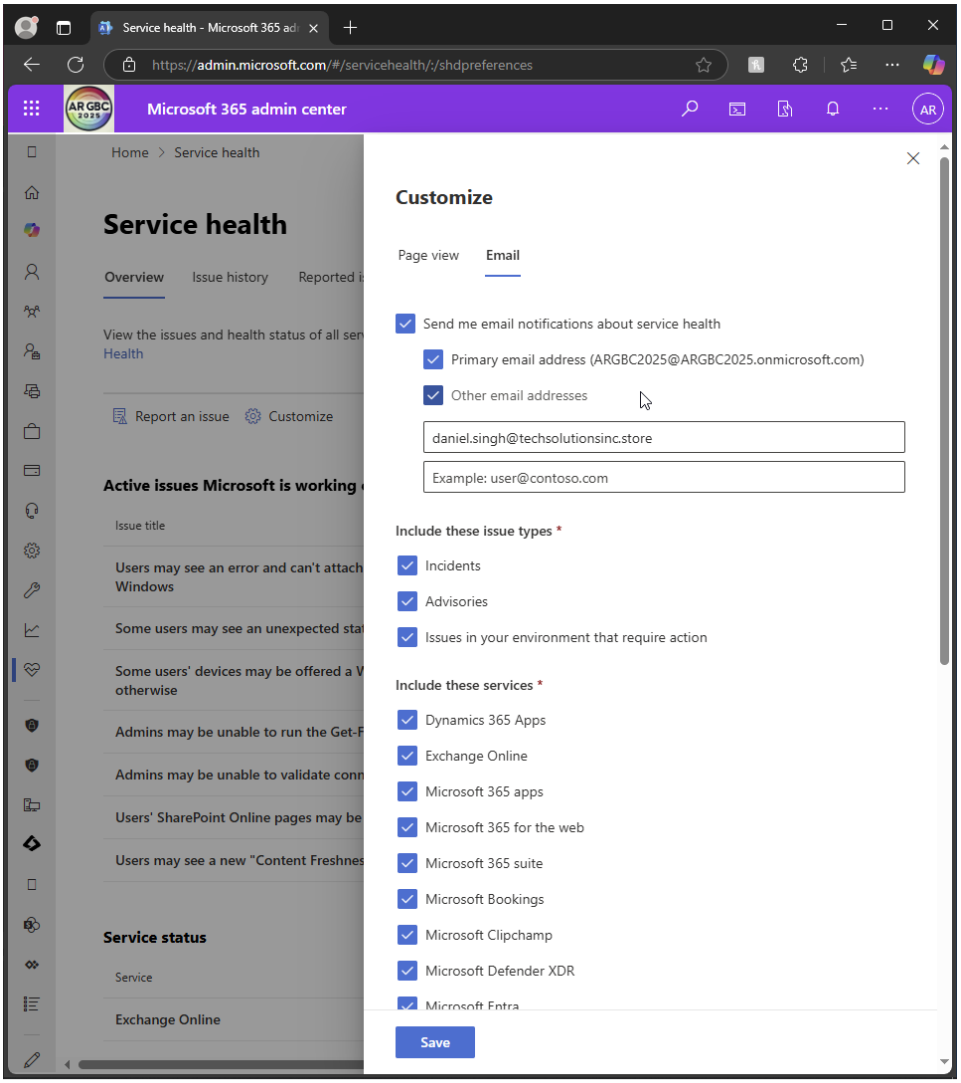
I check the dashboard

Student Name: ……. Term: ……..
Student ID: ……..



I click ’customise - email’ and ensure all services are ticked

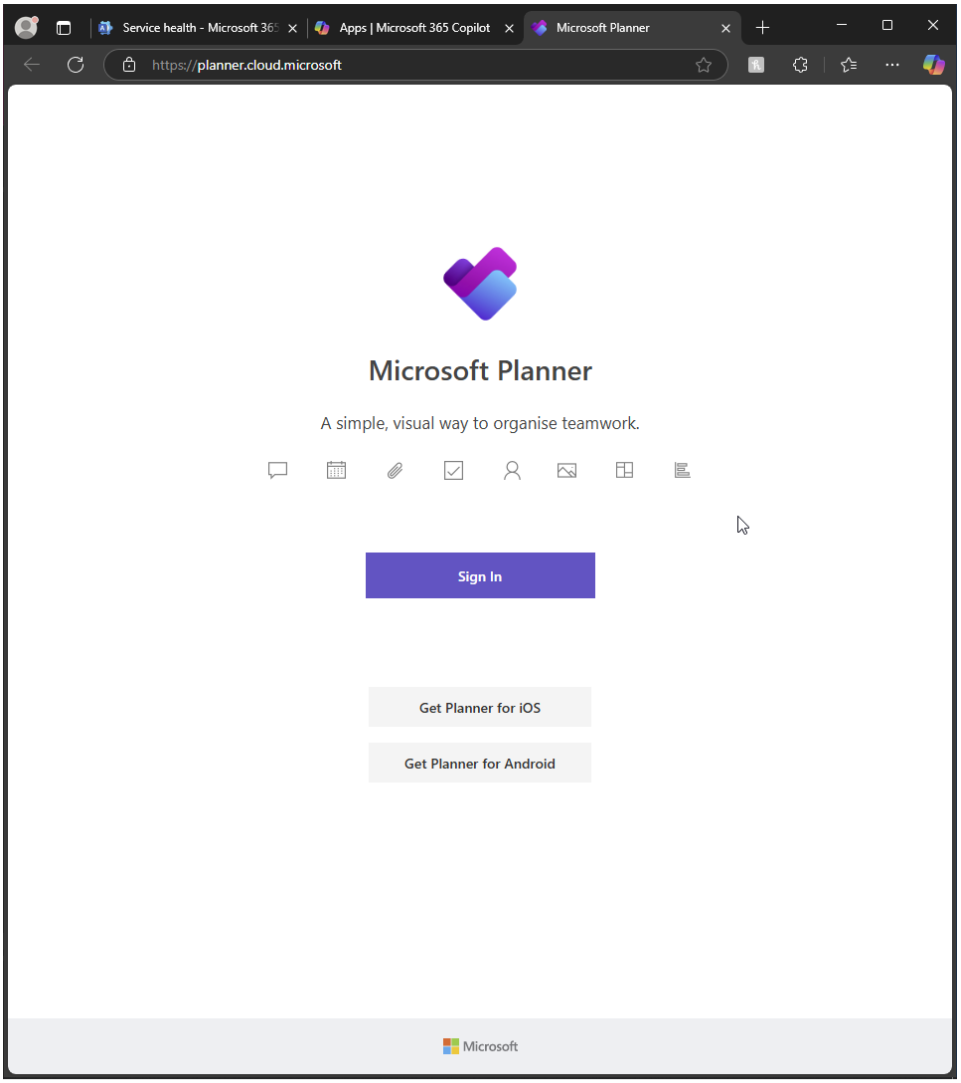
Student Name: ……. Term: ……..
Student ID: ……..



I ensure GA and IT head are recipients of the email

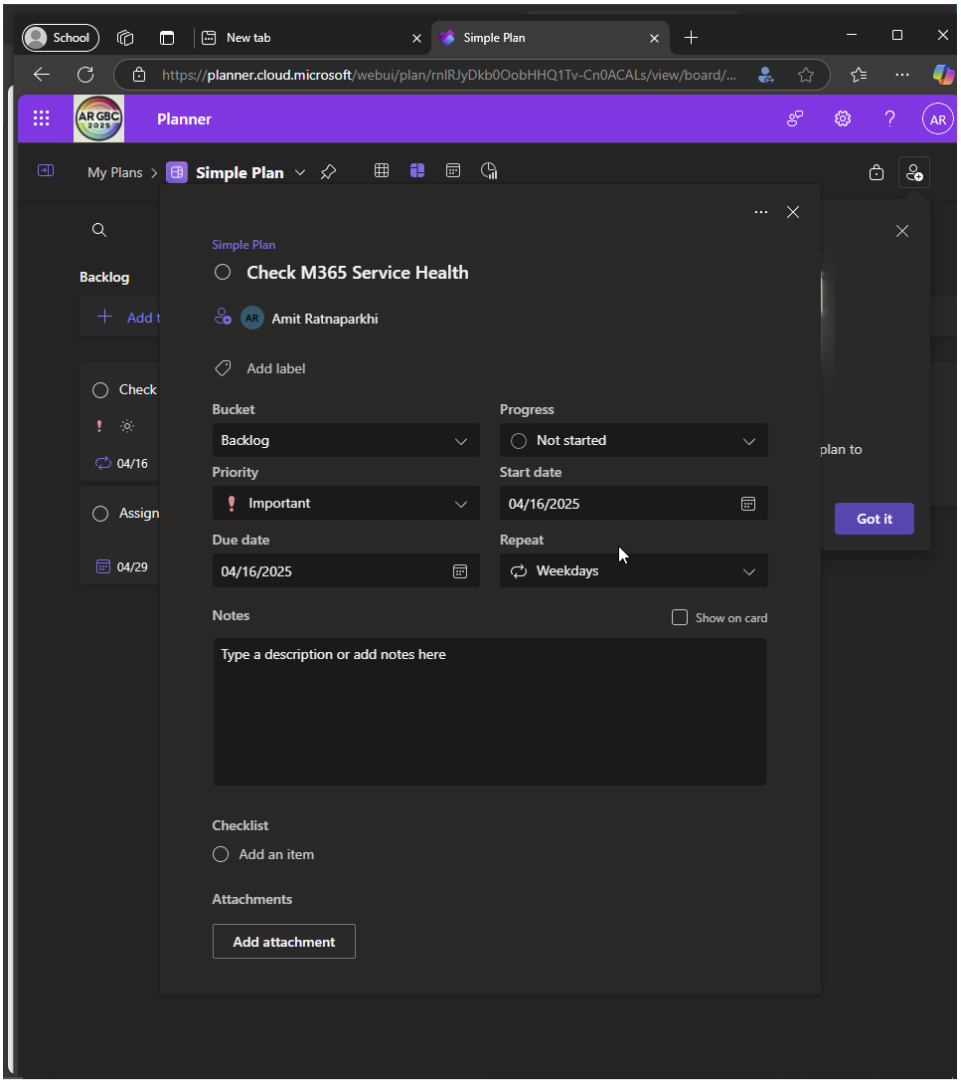
- Monitor the Service Health dashboard regularly to ensure all services are running smoothly.

Student Name: ……. Term: ……..
Student ID: ……..



I open MS Planner

Student Name: ……. Term: ……..
Student ID: ……..



I create a reoccurring task to remind me to check MS service health

~~~~~~

Student Name: …………….………….   Term: …………………………...
Student ID: ……………………………….

~~~~~~

Part B:

Wow! My task 4 felt like actually working as a real-life Microsoft 365 administrator and, at times, felt relentless! My starting point was to enable audit logs (again, because they had already been enabled from a previous task, but still had to exercise to do so for the task). I customised the audit log search to watch for SharePoint activity by Daniel Singh (IT admin), the account that had been configured to make file edits and deletes. The activity didn't display at first, so confusing! until I enabled the role of MS compliance administrator to myself. Strange to think that you need to add it to GA, you would think GA has access to everything! When the entries did display, it became fascinating to see how much insight Microsoft 365 offers into each action, each document, each click.

Creating alert policies to monitor for suspect activity was easy enough until I went to do so through DLP. That was red-herring! I had interpreted the assignment literally in attempting to catch mass deletions through a DLP rule — to be met with a brick wall of system errors (chatGPT was very wrong and I told her off!) Further probe, and I found that DLP does not accommodate such behavioural triggers such as volumes of deletion. Wasted time attempting to make it work, then changed tact and effectively did create the alert properly in the correct place in Microsoft Defender. To send out the notifications of the DLP policy breaches, used Insider Risk Management as allowed under the assignment. Even as Global Admin, however, I couldn't access without manually adding myself to the Insider Risk role group — something that can be explained by Microsoft. I can only assume that Purview is an entirely seperate module to MS365. Once in, sharing of data had to be activated, wait for analytics to be in action, and simulate a further mass deletion using 50 dummy files uploaded by Daniel. Re-ran the activity after the realisation that anything would ever be triggered unless Insider Risk Analytics had been manually switched to be in effect.

I realised at this point that I was confusing DLP with Defender alerts. I did some research and noticed that they don't have to be connected and the assignment was simply asking to trigger an alert for suspicious activity. So I went back to the drawing board! I started off with the idea that Defender and DLP alert settings are hand-in-hand. I could set up a DLP policy, which would natively send notifications out to Defender or Insider Risk. I spent hours trying to get them to talk with one another, with nothing seeming to happen.

I initially set up a custom alert for mass file removal, activating all of the indicators and modifying each of the settings I could. When I deleted the files from both recycle bins, though, nothing registered. Findings revealed that the Microsoft 365 connector wasn't even sending activity logs, even though it had previously appeared to be connected. I had to perform troubleshooting for that as well.

In the long run, I opted for a change of strategy. I switched the policy to single user mass download because it had a pre-configured template and was much easier to set up and as if my magic , it worked! It's been a learning curve, though, I can see that the greater the real-world exposure, the more second nature the setup of such policies will be, and the less intimidating.

I then built a few email, SharePoint, and user activity utilisation reports from the admin centre and exported them to OneDrive. A scheduled flow in Power Automate sent the reports to IT as well as department heads each month. Even here, there was a struggle! First using the incorrect Outlook connector and encountering authentication problems before discovering that you need to use the Office 365 connector. The final task was setting up a recurring alert as well as a reminder to glance at the dashboard from time to time. Which was easy (horray!) but even here, the “Preferences > Email” preference in previous versions is now anachronistic, and the alert setting is now under the “Customise” button. MS365 changes every minute! Overall, this task summarised everything that I’d thus far learned, but with the very real hiccups along the way.

If I were to improve Microsoft 365, first and foremost, its admin UI consistency would be the first to be gone. There's still so much in their own little pockets (Defender, Purview, Admin Center, Viva) that occasionally even the same feature is called something different based on what you're in. Giving Global Admins access to Insider Risk by default, or at least making it more obvious they're blocked, would be a no-brainer. The DLP interface really should inform you about what kinds of conditions they can work with, especially when users are trying to detect in-reality signals such as mass deletion.

For all of that, this was by far, the most helpful and realistic exercise. It didn’t simply tell me to click things — it had me act as an administrator, diagnose as an administrator, and actually create things that you might plausibly do in a real organisation, rather than a student.

~~~~~~

Student Name: …………………………. Term: …………………………..
Student ID: ………………………………..

~~~~~~

Deliverables:

- A detailed report documenting each step taken during the project, including screenshots and explanations.
- A summary of configurations and policies implemented, along with their rationale.
- A presentation to the class demonstrating the setup and explaining the choices made during the project.

Assessment Criteria:

- Completeness and accuracy of the tasks performed.
- Understanding and application of Microsoft 365 features and best practices.
- Quality of documentation and presentation.
- Ability to troubleshoot and resolve issues encountered during the project.

~~~~~~
Paste your screenshots here
~~~~~~